

UNIVERSITI POLY-TECH MALAYSIA

CYBERSAFE LEARNING HUB

MUHAMMAD IMRAN BIN MOHD HANIFAH

**BACHELOR OF INFORMATION
TECHNOLOGY (HONS) IN CYBER
SECURITY**

UNIVERSITI POLY-TECH MALAYSIA
Faculty of Computing & Multimedia

CYBERSAFE LEARNING HUB

MUHAMMAD IMRAN BIN MOHD HANIFAH
AM2408016649

FYP4124

DECEMBER 2025

Declaration of Originality

This project is all my own work and has not been copied in part or in whole from any other source except where duly acknowledged. As such, all use of previously published work (from books, journals, magazines, internet, etc.) has been acknowledged within the main report to an item in the References or Bibliography lists.

I also agree that an electronic copy of this project may be stored and used for the purposes of plagiarism prevention and detection.

Copyright Acknowledgement

I acknowledge that the copyright of this project and report belongs to Universiti Poly-Tech Malaysia.

Signed:



Date: 08/04/2026



Office Stamp

Abstract

The rapid expansion of digital technology has led to a significant increase in cybersecurity threats, yet awareness and understanding of these threats among university students remain critically low. Many students lack the foundational knowledge required to recognise and respond to common cyber risks such as phishing, malware, and weak password practices, making them vulnerable to attacks in both academic and personal digital environments. This project addresses this gap through the development of the CyberSafe Learning Hub, a web-based cybersecurity education platform designed to deliver structured, interactive, and gamified learning experiences to students.

The system was developed using the Laravel 12 framework with PHP 8.2, Livewire and Volt for reactive components, Bootstrap 5.3 for responsive design, and MySQL 8.0 as the database management system. The platform is deployed on a DigitalOcean cloud server using Docker containers managed through the Coolify self-hosting platform, ensuring reliable and scalable production performance.

Three core objectives guided the development of the system. The first objective was to improve cybersecurity awareness among students through structured lesson content. The second objective was to provide interactive and engaging education through multiple-choice quizzes with immediate feedback and an integrated AI-powered cybersecurity chatbot, built using the Groq API with the Meta Llama 3.3 70B Versatile model, which assists students with concept clarification during assessments. The third objective was to motivate students to apply cybersecurity knowledge through a gamification system featuring points, module-specific badges, a competitive leaderboard, and downloadable PDF certificates awarded upon category completion.

The system was evaluated through comprehensive testing covering non-functional, functional, and acceptance testing phases. All 18 non-functional test cases and 35 functional test cases across unit, integration, and system testing levels passed successfully. Client Acceptance Testing conducted with a lecturer at Kolej Teknologi Antarabangsa Cybernetics (KTAC) yielded a 100% acceptance rate across all 15 interview questions. User Acceptance Testing involving 54 student respondents recorded 100% positive responses across all evaluation criteria. The results confirm that the CyberSafe Learning Hub successfully meets all stated objectives and provides an effective, engaging, and secure platform for cybersecurity education.

Table of Contents

1	INTRODUCTION.....	17
1.1	Introduction	17
1.2	Project Background.....	17
1.3	Problem Statement.....	19
1.3.1	Low Cybersecurity Awareness Among Students	19
1.3.2	Limited Access to Interactive Cybersecurity Education	19
1.3.3	Lack of Motivation to Practice Cybersecurity Skills	19
1.4	Project Objectives	19
1.4.1	To Improve Cybersecurity Awareness Among Students	20
1.4.2	To Provide Interactive and Engaging Cybersecurity Education	20
1.4.3	To Motivate Students to Apply Cybersecurity Skills in Practice	20
1.5	Scope and Target User.....	20
1.5.1	Project Scope	20
1.5.2	Product Scope	21
1.5.3	Target User.....	21
1.6	Overview of This Report.....	22
2	LITERATURE REVIEW.....	23
2.1	Introduction	23
2.2	Investigation	23
2.2.1	Gamification in Cybersecurity Awareness	24
2.2.2	Mechanism of Gamified Learning.....	25
2.2.3	Case Studies of Gamification in Higher Education	26
2.2.4	Existing Tools and Platforms.....	26
2.2.5	Challenges and Limitations of Gamification in Cybersecurity Awareness	28
2.2.6	Investigation Summary Table.....	30
2.3	Related Works.....	31
2.3.1	TryHackMe	31
2.3.2	Cybrary.....	34
2.3.3	HackTheBox Academy	38
2.4	Comparison	41
2.5	Discussion	42
2.6	Conclusion.....	43
3	METHODOLOGY.....	44
3.1	Introduction	44
3.2	Agile Methodology.....	44
3.3	Phases in Agile Methodology	45
3.3.1	Phase 1: Planning.....	45
3.3.2	Phase 2: Design	46
3.3.3	Phase 3: Development.....	46
3.3.4	Phase 4: Testing.....	46
3.3.5	Phase 5: Deployment and Review	46
3.4	Requirement.....	47

3.4.1	Data Gathering Techniques	47
3.4.1.1	Questionnaire	47
3.4.1.2	Interview	47
3.4.2	Functional Requirement.....	48
3.4.3	Non-Functional Requirement	49
3.4.4	System Requirement	49
3.4.4.1	Hardware Requirement	49
3.4.4.2	Software Requirement	51
3.5	Analysis.....	54
3.5.1	Data Gathering Analysis	54
3.5.1.1	Questionnaire Analysis	55
3.5.1.2	Interview Analysis	66
3.5.2	Use Case Model	69
3.5.3	Flowchart	71
3.5.3.1	Student Flowchart	71
3.5.3.2	Admin Flowchart	73
3.6	Conclusion.....	74
4	DESIGN & IMPLEMENTATION.....	75
4.1	Introduction	75
4.2	Interface Design.....	75
4.2.1	Admin	77
4.2.2	Students	81
4.2.3	Mobile View (Student).....	85
4.3	Database Design.....	91
4.3.1	Data Dictionary	91
4.3.2	Data Flow Diagram (DFD)	104
4.3.3	Entity Relational Diagram (ERD).....	105
4.4	Security System Framework.....	107
4.4.1	Security Framework Diagram.....	107
4.5	Implementation Introduction	108
4.6	Execution Platform	108
4.6.1	Development Platform	109
4.6.2	Hosting Platform	110
4.7	Implementation Tools.....	111
4.7.1	Software	111
4.7.1.1	Visual Studio Code	111
4.7.1.2	Laravel 12 Framework	112
4.7.1.3	Livewire	112
4.7.1.4	Bootstrap 5	113
4.7.1.5	MySQL 8.0	113
4.7.1.6	Nginx	113
4.7.1.7	Docker	114
4.7.1.8	DigitalOcean	115
4.7.1.9	Coolify	116
4.7.1.10	Vite	116
4.7.1.11	Laravel Socialite	117
4.7.1.12	Groq AI	117
4.7.1.13	phpMyAdmin	118

4.7.1.14	<i>Composer</i>	118
4.7.1.15	<i>Github</i>	119
4.7.2	Programming Language	120
4.7.2.1	<i>PHP</i>	120
4.7.2.2	<i>JavaScript</i>	121
4.7.2.3	<i>HTML5</i>	122
4.7.2.4	<i>CSS</i>	122
4.8	System Interface	123
4.8.1	Landing Page (Public).....	123
4.8.2	Login Page	124
4.8.3	Register Page	125
4.8.4	Google OAuth Login	126
4.8.5	Student Dashboard.....	127
4.8.6	Module Listing (Student View)	128
4.8.7	Module Detail with Lesson List (Student View).....	129
4.8.8	Lesson Content View (Student View).....	130
4.8.9	Quiz Interface (Student View)	131
4.8.10	Quiz Result	132
4.8.11	AI Chatbot (Quiz Page).....	133
4.8.12	Badges Page (Student View)	134
4.8.13	Certificates Page (Student View)	135
4.8.14	Certificate Detail View (Student View).....	136
4.8.15	User Manual (Student View)	137
4.8.16	Admin Dashboard	138
4.8.17	Admin Category Management	139
4.8.18	Admin Create / Edit Category	140
4.8.19	Admin Module Management	140
4.8.20	Admin Create / Edit Module	141
4.8.21	Admin Lesson Management	142
4.8.22	Admin Lesson Content Editor	142
4.8.23	Admin Quiz Management	143
4.8.24	Admin Quiz Question Management	144
4.8.25	Admin Analytics Dashboard	144
4.8.26	Admin Student Analytics Drill-Down.....	145
4.8.27	Admin User Management	145
4.9	Significant Functions	146
4.9.1	Significant Functions.....	146
4.9.1.1	<i>Google OAuth 2.0 Authentication</i>	147
4.9.1.2	<i>Quiz Scoring and Validation</i>	148
4.9.1.3	<i>AI Chatbot Integration</i>	148
4.9.2	Security Elements.....	149
4.9.2.1	<i>Role-Based Access Control (RBAC) Middleware</i>	149
4.9.2.2	<i>Password Hashing and Data Protection</i>	150
4.9.2.3	<i>CSRF Protection</i>	150
4.9.2.4	<i>Owner-Only Resource Access</i>	151
4.10	Conclusion	152
5	FINDING	153
5.1	Introduction	153
5.2	Testing	153

5.3 Non-Functional Testing.....	155
5.3.1 Performance Testing.....	155
5.3.2 Security Testing.....	156
5.3.3 Usability Testing	157
5.3.4 Reliability Testing.....	158
5.4 Functional Testing.....	158
5.4.1 Unit Testing	158
5.4.2 Integration Testing	160
5.4.3 System Testing	162
5.5 Acceptance Testing.....	164
5.5.1 Client Acceptance Testing	164
5.5.2 User Acceptance Testing	168
5.6 Conclusion.....	178
6 CONCLUSION	179
6.1 Introduction	179
6.2 Project Schedule	179
6.2.1 Work Breakdown Structure	180
6.2.2 Gantt Chart.....	180
6.3 Risk Management.....	183
6.4 Achievement.....	185
6.4.1 To Improve Cybersecurity Awareness Among Students	185
6.4.2 To Provide Interactive and Engaging Cybersecurity Education	186
6.4.3 To Motivate Students to Apply Cybersecurity Skills in Practice	187
6.5 Constraint and Limitation	188
6.5.1 Limited Cybersecurity Topic Coverage	188
6.5.2 No Real-Time Collaboration or Discussion.....	188
6.5.3 English-Only Content.....	188
6.5.4 Manual Content Management.....	189
6.5.5 Dependency on Third-Party AI API	189
6.6 Future Work and Recommendation	189
6.6.1 Expand Cybersecurity Content	189
6.6.2 Multilingual Support	189
6.6.3 Live Discussion and Peer Interaction	190
6.6.4 Adaptive Learning Pathways.....	190
6.6.5 Bulk Content Import.....	190
6.6.6 Mobile Application.....	190
6.6.7 Advanced Analytics and Reporting	190
6.6.8 Gamification Enhancements	191
6.7 Conclusion.....	191
Appendix A – Questionnaire & Interview Questions	192
Appendix B – User Manual.....	203
Appendix C – Turnitin Result.....	250
Appendix D – Log Book	256
References	262

List of Figures

Figure 2.1: Example of gamified awareness module interface (Razack & Saad, 2024).....	24
Figure 2.2: TryHackMe interface with progress badges	27
Figure 2.3: HackTheBox Academy challenge map	27
Figure 2.4: Cybrary learning roadmap dashboard	28
Figure 2.5: TryHackMe Dashboard	31
Figure 2.6: TryHackMe Learning Path Page	32
Figure 2.7: TryHackMe Challenge Room Interface	32
Figure 2.8: TryHackMe Leaderboard Interface	33
Figure 2.9: TryHackMe Completed Room Example	33
Figure 2.10: Cybrary Dashboard Page	35
Figure 2.11: Cybrary Course Catalog and Career Paths	35
Figure 2.12: Cybrary Course Module Page.....	36
Figure 2.13: Cybrary Learning Progress Dashboard	36
Figure 2.14: Cybrary Certification Preparation Page	37
Figure 2.15: HackTheBox Academy Dashboard Page.....	38
Figure 2.16: HackTheBox Academy Lab Interface Page	38
Figure 2.17: HackTheBox Academy Completion Badge Page.....	39
Figure 2.18: HackTheBox Academy Certificate Page	39
Figure 2.19: HackTheBox Academy Exams Page	40
Figure 3.1: Agile Methodology Diagram (Popa et al., 2021)	45
Figure 3.2: Lenovo IdeaPad Gaming 3	50
Figure 3.3: Visual Studio Code Logo	51
Figure 3.4: Laravel 12 Logo	51
Figure 3.5: MySQL Logo	52
Figure 3.6: Bootstrap Logo	52
Figure 3.7: Google OAuth Logo	53
Figure 3.8: PHPUnit Logo	53
Figure 3.9: XAMPP Logo	54
Figure 3.10: Age of Respondents	56
Figure 3.11: Gender of Respondents.....	56
Figure 3.12: Program of Study.....	57
Figure 3.13: Frequency of Internet Use	57
Figure 3.14: Level of Cybersecurity Knowledge.....	58
Figure 3.15: Experience of Cybersecurity Incidents.....	58
Figure 3.16: Participation in Cybersecurity Awareness Program	59
Figure 3.17: Importance of Cybersecurity Awareness	59
Figure 3.18: Confidence in Protecting Personal Data	60
Figure 3.19: Preferred Learning Methods for Cybersecurity	60
Figure 3.20: Frequency of Applying Safe Online Practices.....	61
Figure 3.21: Awareness of Security Practices	61
Figure 3.22: Interest in Using Cybersecurity Learning Platforms	62
Figure 3.23: Importance of User Authentication.....	62
Figure 3.24: Motivation Through Gamification	63
Figure 3.25: Preferred Features in the CyberSafe Learning Hub.....	63
Figure 3.26: Usefulness of Progress Tracking	64
Figure 3.27: Importance of Platform Loading Speed.....	64
Figure 3.28: System Usability and Interface Design	65
Figure 3.29: Importance of Data Security and Encryption.....	65
Figure 3.30: Interview session with Mr.Syaheedullah	66

Figure 3.31: Use Case Diagram for CyberSafe Learning Hub	69
Figure 3.32: User (Student) Flowchart of CyberSafe Learning Hub	71
Figure 3.33: User (Administrator/Lecturer) Flowchart of CyberSafe Learning Hub	73
Figure 4.1: Landing Page	75
Figure 4.2: Login Page	76
Figure 4.3: Register Page	76
Figure 4.4: Admin Dashboard Page	77
Figure 4.5: Manage Module Page	78
Figure 4.6: Manage Lessons Page	78
Figure 4.7: Manage Quizzes Page	79
Figure 4.8: Student Analytics Page	79
Figure 4.9: Manage Users Page	80
Figure 4.10: Student Dashboard Page	81
Figure 4.11: View Module Page	82
Figure 4.12: View Lesson Page	82
Figure 4.13: Lesson Learning Page	83
Figure 4.14: Quiz Page	83
Figure 4.15: Quiz Result Page	84
Figure 4.16: Student Dashboard Page (Mobile View)	85
Figure 4.17: View Module Page (Mobile View)	86
Figure 4.18: View Lesson Page (Mobile View)	87
Figure 4.19: Lesson Learning Page (Mobile View)	88
Figure 4.20: Quiz Page (Mobile View)	89
Figure 4.21: Quiz Result Page (Mobile View)	90
Figure 4.22: Data Flow Diagram (DFD)	104
Figure 4.23: Entity Relationship Diagram (ERD)	105
Figure 4.24: Security Framework Diagram (SFD)	107
Figure 4.25: Windows 11 Pro	109
Figure 4.26: Ubuntu 24.04 LTS	110
Figure 4.27: Visual Studio Code Interface	111
Figure 4.28: Docker Interface	114
Figure 4.29: DigitalOcean Interface	115
Figure 4.30: Coolify Interface	116
Figure 4.31: Groq AI – Llama 3.3 Interface	117
Figure 4.32: phpMyAdmin Interface	118
Figure 4.33: GitHub Interface	119
Figure 4.34: PHP Code Snippet – Quiz Result Controller (QuizAttemptController.php)	120
Figure 4.35: JavaScript Code Snippet – Quiz Timer (show.blade.php)	121
Figure 4.36: HTML5 Code Snippet – Quiz Question Template (show.blade.php)	122
Figure 4.37: CSS Code Snippet – Chat Widget Styling (show.blade.php)	123
Figure 4.38: CyberSafe Learning Hub Landing Page (Desktop View)	123
Figure 4.39: CyberSafe Learning Hub Landing Page (Mobile View)	124
Figure 4.40: Login Page (Desktop View)	124
Figure 4.41: Login Page (Mobile View)	125
Figure 4.42: Register Page (Desktop View)	125
Figure 4.43: Register Page (Mobile View)	126
Figure 4.44: Google OAuth 2.0 Authentication Screen (Desktop View)	126
Figure 4.45: Google OAuth 2.0 Authentication Screen (Mobile View)	127
Figure 4.46: Student Dashboard (Desktop View)	127
Figure 4.47: Student Dashboard (Mobile View)	128
Figure 4.48: Student Module Listing Page (Desktop View)	128
Figure 4.49: Student Module Listing Page (Mobile View)	129

Figure 4.50: Module Detail Page with Lesson List (Desktop View)	129
Figure 4.51: Module Detail Page with Lesson List (Mobile View)	130
Figure 4.52: Lesson Content View (Desktop View)	130
Figure 4.53: Lesson Content View (Mobile View)	131
Figure 4.54: Quiz Interface (Desktop View)	131
Figure 4.55: Quiz Interface (Mobile View)	132
Figure 4.56: Quiz Result Page (Desktop View).....	132
Figure 4.57: Quiz Result Page (Mobile View)	133
Figure 4.58: AI Chatbot – Cybersecurity Tutor Assistant (Desktop View)	133
Figure 4.59: AI Chatbot – Cybersecurity Tutor Assistant (Mobile View)	134
Figure 4.60: Student Badges Page (Desktop View)	134
Figure 4.61: Student Badges Page (Mobile View)	135
Figure 4.62: Student Certificates Page (Desktop View)	135
Figure 4.63: Student Certificates Page (Mobile View)	136
Figure 4.64: Certificate Detail View (Desktop View)	136
Figure 4.65: Certificate Detail View (Mobile View)	137
Figure 4.66: Student User Manual Page (Desktop View)	137
Figure 4.67: Student User Manual Page (Mobile View)	138
Figure 4.68: Admin Dashboard	138
Figure 4.69: Admin Category Management	139
Figure 4.70: Admin Category Create / Edit Form	140
Figure 4.71: Admin Module Management	140
Figure 4.72: Admin Module Create / Edit Form	141
Figure 4.73: Admin Lesson Management	142
Figure 4.74: Admin Lesson Content Editor	142
Figure 4.75: Admin Quiz Management	143
Figure 4.76: Admin Quiz Detail and Question Management	144
Figure 4.77: Admin Analytics Dashboard	144
Figure 4.78: Admin Student Analytics – Individual Student View	145
Figure 4.79: Admin User Management	145
Figure 4.80: Code Snippet – Google OAuth 2.0 Callback (GoogleController.php)	147
Figure 4.81: Code Snippet – Quiz Submission and Validation (QuizAttemptController.php) ..	148
Figure 4.82: Code Snippet – AI Chatbot System Prompt (ChatbotController.php)	148
Figure 4.83: Code Snippet – Role-Based Access Control Middleware (RoleMiddleware.php) ..	149
Figure 4.84: Code Snippet – Password Hashing and Hidden Fields (User.php)	150
Figure 4.85: Code Snippet – CSRF Protection in Blade Form (show.blade.php)	150
Figure 4.86: Code Snippet – Owner-Only Access Control (QuizAttemptController.php)	151
Figure 5.1: Client Acceptance Testing Session with Mr.Syaheedullah bin Yahya	165
Figure 5.2: Q1 – Age Range of Respondents	168
Figure 5.3: Q2 – Gender of Respondents	169
Figure 5.4: Q3 – Registration & Login	169
Figure 5.5: Q4 – Navigation & Usability	170
Figure 5.6: Q5 – Cybersecurity Awareness (Lesson Structure)	170
Figure 5.7: Q6 – Cybersecurity Awareness (Content Clarity)	171
Figure 5.8: Q7 – Cybersecurity Awareness (Learning Outcome)	171
Figure 5.9: Q8 – Interactive Education (Quiz Design)	172
Figure 5.10: Q9 – Interactive Education (Visual Elements)	173
Figure 5.11: Q10 – Interactive Education (Quiz Feedback)	173
Figure 5.12: Q11 – Motivation & Gamification (Points System)	174
Figure 5.13: Q12 – Motivation & Gamification (Badge System)	174
Figure 5.14: Q13 – Motivation & Gamification (Progress Tracking)	175
Figure 5.15: Q14 – Functional Requirements (Lesson & Quiz Access)	175

Figure 5.16: Q15 – Functional Requirements (Progress Recording)	176
Figure 5.17: Q16 – Non-Functional Requirements (Performance).....	177
Figure 5.18: Q17 – Non-Functional Requirements (Security)	177
Figure 6.1: Work Breakdown Structure of the CyberSafe Learning Hub Project	180
Figure 6.2: Gantt Chart of the CyberSafe Learning Hub Project Timeline	181

List of Tables

Table 2.1: Investigation Summary Table	30
Table 2.2: Comparison of Existing Project	41
Table 3.1: Functional Requirement Table	48
Table 3.2: Non-Functional Requirements Table	49
Table 3.3: Hardware Requirements Table	50
Table 3.4: Analysis of Interview Questions	67
Table 4.1: Users Table.....	91
Table 4.2: Roles Table.....	92
Table 4.3: User Roles (Pivot) Table	92
Table 4.4: Categories Table	93
Table 4.5: Modules Table	93
Table 4.6: Lessons Table.....	94
Table 4.7: Lesson Contents Table	95
Table 4.8: Lesson Comments Table	96
Table 4.9: Quizzes Table	96
Table 4.10: Questions Table.....	97
Table 4.11: Answers Table	97
Table 4.12: Quiz Attempts Table	98
Table 4.13: Quiz Answers Table.....	99
Table 4.14: Student Progress Table	99
Table 4.15: Badges Table.....	100
Table 4.16: User Badges Table	101
Table 4.17: Certificates Table	101
Table 4.18: User Certificates Table	102
Table 4.19: Achievement Notifications Table	103
Table 5.1: Testing Overview	154
Table 5.2: Performance Testing.....	155
Table 5.3: Security Testing	156
Table 5.4: Usability Testing.....	157
Table 5.5: Reliability Testing	158
Table 5.6: Unit Testing.....	159
Table 5.7: Integration Testing	160
Table 5.8: System Testing	162
Table 5.9: Client Acceptance Testing – Interview Response Summary.....	165
Table 6.1: Project Task Timeline and Duration	181
Table 6.2: Project Risk Management.....	183

Acknowledgements

Alhamdulillah, all praise and thanks to Allah SWT for granting the strength, patience, and guidance to complete this Final Year Project successfully. This accomplishment would not have been possible without the support, encouragement, and contributions of many individuals, and sincere gratitude is extended to all of them.

Deepest appreciation is given to beloved parents for their endless prayers, unwavering encouragement, and unconditional support throughout this journey. Their love and sacrifice have been the greatest source of motivation.

Special thanks and heartfelt gratitude are extended to the Final Year Project Supervisor, Madam Noraliza binti Azizan, for her invaluable guidance, constructive advice, patience, and dedication from the very beginning until the successful completion of this project. Her expertise and continuous encouragement played a significant role in shaping the direction and quality of this work.

Sincere appreciation is also given to the Final Year Project Coordinator, Madam Norfazlina binti Johar, for her efficient management of the FYP process, clear communication, and continuous support provided to all students throughout the programme.

Gratitude is extended to the Final Year Project Examiner, Ts. Ainul Hazmin bin A Hamid, for his thorough evaluation, professional feedback, and constructive comments that greatly contributed to improving the overall quality of this project.

Heartfelt thanks are also owed to the project client, Mr. Syaheedullah bin Yahya, a lecturer at Kolej Teknologi Antarabangsa Cybernetics (KTAC), for his trust, cooperation, and valuable input during the client acceptance testing session. His feedback and perspectives from an educator's standpoint were instrumental in validating the platform's effectiveness and relevance.

Appreciation also goes to all classmates and friends who willingly participated during the testing and evaluation phases, providing honest and useful responses that contributed to the success of the User Acceptance Testing.

Finally, thanks are extended to the institution, faculty, and all individuals who have directly or indirectly contributed to the completion of this project. May all efforts and contributions be rewarded with success, and may this project serve as a meaningful contribution to the fields of cybersecurity and education.

1 INTRODUCTION

1.1 Introduction

This chapter concludes the project by restating the project history and reasons for project initiation, the problem statement which identifies the critical elements of the problem which requires such a project, the project objectives and the project scope and target user. The chapter concludes with a brief overview of the rest of the report.

1.2 Project Background

In the 21st century, cybersecurity is a concern; digital technologies in education, work, and daily life have deeply rooted themselves. Among the heaviest users of these digital platforms are students engaging in online learning management systems, social media, cloud storage, and communication tools daily. However, this frequent usage does not equate to safe usage. Most students either lack awareness or discipline to follow cybersecurity best practices and thus expose themselves to cyber threats like phishing attacks, malware infection, poor password management, and unsafe online behaviors. According to studies conducted globally, young internet users often remain very confident about their digital skills, which contributes to their highly vulnerable position regarding cyber threats compared to more experienced users (Gabra et al., 2020).

This task is made more difficult because traditional cybersecurity training has fundamental limitations. Many awareness campaigns or lecture-based classes can impart theory, but many of these efforts are “dry as cardboard” and don’t engage students to change behaviours on a long-term basis. For instance, students know that they should use strong passwords but they reuse weak passwords because of their instant recall. This gap of knowing and doing exemplifies the necessity for education about cybersecurity awareness to be more interactive and engaging.

There are a few platforms out there that do this for CyberSafe Learning Hub, like TryHackMe, Cybrary and HackTheBox Academy. These resources range from virtual labs, to professional courses, to real-world simulations. But their major audience is IT undergraduate, working professionals or certification candidates. Consequently, the content can be extremely technical and expected former networking, programming or penetration testing tool knowledge. Though these platforms are great in professional progress, they do not cater for beginners or even non-IT students who need simple and easy-to-read and

age-appropriate resources. This opens a hole in the availability of security education tools, especially for IT-non related students in higher education.

Taking cognizance of this problem, Kolej Teknologi Antarabangsa Cybernetics (KTAC), a private institution of higher learning in Malaysia, has realised the need to incorporate cybersecurity awareness within its educational curriculum. KTAC realizes that cybersecurity learning is applicable not only to IT majors. All students across disciplines have interactions with digital systems such as turning in assignments, online banking and social networking and communication. With insufficient test and prepare, if their standoffishness throws them into phishing scams, thieving, identity theft, and other crimes in cyberspace.

The problem that motivated this project was the low level of awareness and few easily accessible tools for dealing with cyber security in colleges. Workshops or seminars, when held at all, are typically a onetime activity and provide no guarantee that any learning will be retained or behaviour modified. Thus, KTAC needs a sustainable and organized solution, which easily integrates with the learning experiences of students, thus making them to be involved in cybersecurity awareness activities rather than being mere recipients of information.

In order to fill this gap, the proposed project will develop CyberSafe Learning Hub, a web application designed for KTAC students. The platform will deliver lessons with interactive quizzes and gamified challenges on key cybersecurity topics like phishing awareness, password safety, and safe browsing. Through gamifying the content through points, badges and progression, student have been more motivated to complete the course and students should not only learn this key stuff but learn how it is applied in their digital lives. Lecturers will be able to take advantage of an academic admin dashboard which allows content creation and management, the ability to track a student's performance over time. Students are at the centre and lecturers in support, two beneficial aspects of the platform that will make it last within an educational setting.

Ultimately, this project intends to fill the void between pro-level cyber security training environments out there and the lack of beginner-friendly college-oriented systems. Through a focus on accessibility, interactivity and motivation, the CyberSafe Learning Hub will enable KTAC students to develop safer online behaviours, while leaving the College with a trusted long-term method for educating young people about digital literacy safely navigating threats.

1.3 Problem Statement

Students in general also continue to struggle with awareness of cyber security. Despite regular use of digital devices/tablets and online platforms, the vast majority of students fail to comprehend the risks involved or what actions can safeguard them. Current awareness campaigns are often too mechanistic; they warrant already a bit of understanding but not being yet so formalized and probably still more making people aware. This thereby results in a requirement for an environment that would make cybersecurity to be presented in less formal, interactive and more motivational way especially where such learners are not IT inclined.

1.3.1 Low Cybersecurity Awareness Among Students

In general, and particularly in Malaysia, students (university and colleges) are often not equipped with appropriate knowledge about cybersecurity threats like phishing, malware spread, unsafe online behavior which could be exploited. For example, studies involving Malaysian university students report similar findings, where many lack essential cybersecurity practices and rely heavily on risky online habits (Gabra et al., 2020).

1.3.2 Limited Access to Interactive Cybersecurity Education

College-based conventional awareness means tend to be boring and/or students just did not get it, resulting in low involvement or limited knowledge retained. Studies have found that passive methods of instruction lead to only a modest change in behavior, but the impact can be enhanced by interactive and experiential training approach on enhancing internet users' awareness (Ng & Kamsin, 2021).

1.3.3 Lack of Motivation to Practice Cybersecurity Skills

Without gamified or hands-on experiences, students are less likely to apply cybersecurity knowledge in real life, leaving them vulnerable to online threats. Research demonstrates that gamification methods (e.g., quizzes, badges and leader boards), notably increase motivation and engagement in cyber security curricula (Gwenhure & Rahayu, 2024).

1.4 Project Objectives

The primary focus of the project is to design a system that engages college students for improved cyber security awareness education. Rather than passive learning, the device incorporates interactive and gamified learning for improved knowledge retention and motivation.

1.4.1 To Improve Cybersecurity Awareness Among Students

This goal is about increasing students' awareness of basic cyber threats like phishing, malware and weak passwords. Through organized, age-specific coursework, students will not only gain an understanding of what these dangers are, but also how to be safe in the digital world. This recommendation will better prepare students to defend themselves on the virtual landscape, mind the gap between their knowledge and the level they need to know.

1.4.2 To Provide Interactive and Engaging Cybersecurity Education

This goal highlights the requirement to achieve more than rote learning, a teaching method of dubious influence on knowledge retention among students. The platform will include interactive elements such as brief quizzes, multiple-choice questions and visual collateral like infographics to foster an engaging learning process. By delivering straightforward, interactive lessons, students are engaged and more likely to pay attention, find the information useful, and use it in their digital lives.

1.4.3 To Motivate Students to Apply Cybersecurity Skills in Practice

This purpose is intended to engross students in learning cybersecurity and not give up through gamification. Students earn points by completing lessons and quizzes, see their progress represented in a nice infographic, and win badges for hitting milestones. It is through these simplistic elements of gamification that learning becomes a reward and fun, thereby promoting the continued use of learned material in daily digital activities.

1.5 Scope and Target User

This part of the project defines the scope and who will be affected by its use. By making the scope explicit, it helps to keep the project on track with what we can actually accomplish and prevents a reasonable idea from getting out of control. And if the target audience is determined, then it's clear for whom and how the system has been created.

1.5.1 Project Scope

The CyberSafe Learning Hub project is an initiative to develop a web-based platform that educates university students about key areas of cybersecurity awareness, including phishing, password security, and secure browsing. The platform will include organized modules, quizzes and gamification elements such as points, badges and progress to increase engagement, while a lecturer dashboard will facilitate lesson management and student participation.

The system will be designed in Laravel 12 framework for the backend and MySQL database while Bootstrap for responsive frontend. By the end of this article, we will demonstrate how Google OAuth API can be used for secure login and later we use PHPUnit to test if the components work as intended- that is any new update should not lead to bugs. Despite relying on proven tools like Laravel, MySQL, and Bootstrap, more work must be poured into mastering the more intricate features of Laravel; into including gamification features in the application; as well as adapting leading content from other trusted sources like NCSA, OWASP and scholarly journals. The purpose is strictly educational and awareness raising, without really going deep into advanced penetration testing or cyber security learning at a pro level.

1.5.2 Product Scope

The product vision underscores functional as well as non-functional elements of the CyberSafe Learning Hub. In terms of functionality, the platform provides simplified cyber security knowledge by the way of interactive lessons, quizzes and playful content on safe internet usage, password security and digital responsibility. Gamification elements like gamified points, badges and progress will be used to make it more engaging. A lecturer dashboard is also offered so that the lecturers can design lessons, allocate modules and check students' performance for utilizing learning outcomes.

Non-functional-wise, the system will focus in usability with a clean and intuitive interface that make easy to most students or lecturers to navigate around on the platform. Performance requirements to be able to run smoothly and respond quickly when loading lessons, quizzes, or dashboards even during normal use. Security concerns will be met with the use of secure login and handling of student data, while reliability will assure consistent system availability for classroom time and individual use. The platform will also assist in making accessibility available to ensure that there is inclusivity for a wide range of learners.

Though the platform does an all-round job in creating a general sense of awareness within cyber security, it doesn't have coverage for more advanced technical topics like pentesting, malware analysis or cert-based training. Instead, the emphasis is on developing an intelligent basis of cybersecurity in college student's everyday lives.

1.5.3 Target User

This project is aimed at users in Kolej Teknologi Antarabangsa Cybernetics; primarily college students, particularly non-IT students who are ignorant towards cybersecurity. These students are heavy users of digital devices, and network consumes hence making them susceptible to common cyber threats in the absence of proper education.

The platform is designed to teach them good cybersecurity habits they can use during their day-to-day digital pursuits by serving up digestible, easy-to-understand content. Lecturers besides students as secondary users will have access to a dashboard too, where they can author and monitor information of learning objects in their course. This duality in users permits the system to adequately support both teaching practices and learning events.

1.6 Overview of This Report

Chapter 1: Introduction

This chapter presents the background, problem statement, objectives, scope and target users of CyberSafe Learning Hub project. It is the base of the research and clarifies the need to inculcate cyber security awareness among students at Kolej Teknologi Antarabangsa Cybernetics.

Chapter 2: Literature Review

This chapter surveys literature, platforms, and approaches on cybersecurity awareness. It reviews the potentials of solutions like TryHackMe, Cybrary, and HackTheBox Academy and brings out their advantages as well as drawbacks. The description is intended to explore some deficiencies in existing methodologies, justify a need for a simpler and more gamified learning platform for college students.

Chapter 3: Methodology

In this chapter, we describe the approach used to create the CyberSafe Learning Hub. It teaches collecting, analyzing and translating user requirements to the system functionality. Surveys and interviews were used as data collection methods for students and lecturers to recognize user needs and expectations. The results from the study were interpreted to specify both functional and non-functional requirements for the system, on which the design of the system was based. Also, it complies requirements analysis and visual models like use case diagram and flow diagram to provide the understanding of how the system operates to serve its purpose.

2 LITERATURE REVIEW

2.1 Introduction

A literature review is a critical analysis of the studies, theories and practices conducted or used for the study area concerned. Its goal is to position the present project in a wider research context through identification of relevant pieces of work, description of main findings and gaps that have not been studied. In this way, the review provides a solid basis for the proposed investigation and shows how it relates to other scholarly conversations. Literature studies on online cyber security awareness, education gamification and existing systems or efforts to address them are conducted for this study. This section is dedicated to consolidating the literature and research projects in order to provide sound foundations for authors' research trajectory and prototyping of a gamified platform for university/college students.

2.2 Investigation

With students being exposed to more and more digital platforms where their data could be at risk, cybersecurity has become critical to higher education. Conventional cybersecurity training methods like lecturing or text-based modules cause loss of student's attention and are not engaging most, especially with non-IT students (Pramod et al., 2024). In the past few years, gamification has been acknowledged as a potential intervention to boost engagement, motivation, and retention through embedding game-like features into learning settings. There have been several studies that showed the effectiveness of learning games in terms of daily participation which fosters long-term behavioural modification by forcing students to apply their knowledge in simulated or interactive setting (Razack & Saad, 2024; Maluda et al., 2023).

The next subsections go deeper into the potential of gamification in cybersecurity training, from its definition and use for awareness raising, to an analysis of the mechanisms at work, case studies at university level, available tools and challenges around. These discussions will lay a grounding for the adaptation of gamification to address issues pertaining to university students, and validate the creation of a customised platform which is the CyberSafe Learning Hub.

2.2.1 Gamification in Cybersecurity Awareness

Gamification means the inclusion of game design elements in nongaming environments to enhance user experience and motivation. Within cybersecurity education, researchers have found gamification to enhance knowledge retention and promote security proactive behaviours (Pramod et al., 2024). Common features are challenges, levels, badges and storytelling in that they enable learners to work interactively with content as opposed to passively consuming learning. Indeed, a few institutions have started utilizing gamified modules with good student feedback in terms of enjoying and not fearing learning (Razack & Saad, 2024).

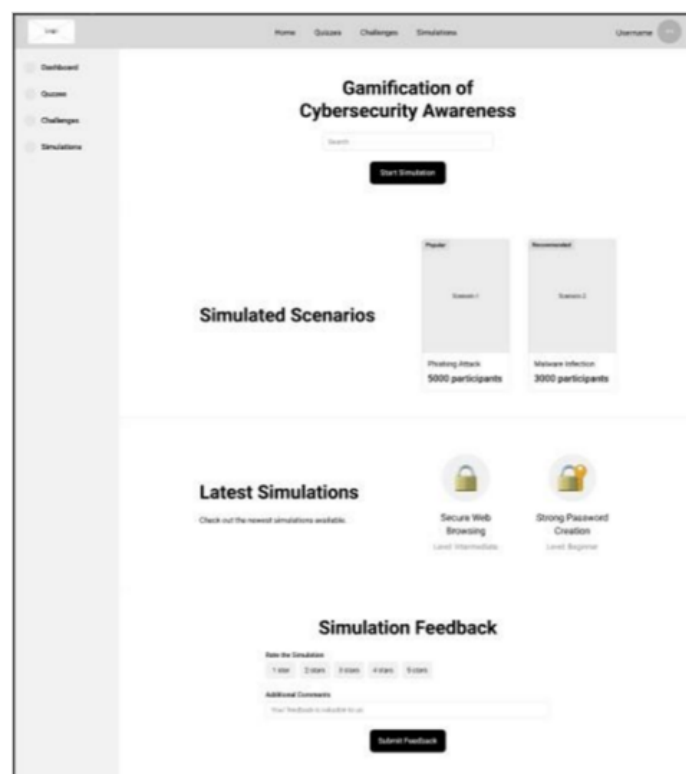


Figure 2.1: Example of gamified awareness module interface (Razack & Saad, 2024)

Figure 2.1 illustrates a sample interface of a gamified cybersecurity awareness module. The interface is a mix between visual narratives and interactive elements, such as quizzes, scoring structures and badges. The following is an overview of how the module combines these components to show how game play can enhance learning. The structure motivates learners to advance tiers, collect badges, and see a sense of accomplishment which reinforces motivation and long-term engagement.

This study has validated gamification as the primary engagement technique for CyberSafe Learning Hub. Previous research (Huotari & Hamari, 2019; Pramod et al., 2024)

shows that the addition of challenges, badges and storytelling enhances user motivation and learning. This is in line with a goal of the project to render cybersecurity learning more interactive and attractive than traditional means.

2.2.2 Mechanism of Gamified Learning

The gamification of cybersecurity is a three-part process involving content delivery, interactive engagement, and feedback. Content delivery works much like the same field, in which learners are presented with micro-lessons or scenarios that unfold. Hands-on practice can be used as collaborative quiz or simulation with role-playing. Feedback instruments, like scores or development profiles are useful for pupils to compare their growth and incentivize constant participation (Gwenhure et al., 2024). These methodologies were designed so that learners stay engaged and encouraged, while being reminded of effective cybersecurity habits.

The second stage is interactive participation, in which learners directly use their knowledge. These can come in the form of quizzes, simulated phishing attempts, riddles or role-playing games where students play defenders against cyber-attacks. Engagement is also enhanced when the learners are placed at the centre of action, involved rather than entertained.

The third stage is feedback, and reinforcement, which is important in maintaining motivation. And leaderboards, scorecards, achievement badges and progress dashboards give users instant feedback on their efficacy. Such feedback serves to strengthen correct behaviour and identify which areas are still in need of improvement, so that learners can continue working on the material. It has been shown that if feedback is instantaneous and transparent, students will tend to persevere and acquire a sense of accomplishment (Maluda et al., 2023).

These stages, in turn, form a self-reinforcing learning cycle that boosts awareness, builds retention and drives motivation. The mechanism explains why so many institutions of higher learning are now looking at gamification: It takes cybersecurity training from being a compliance-based chore to being an engaging, even fun experience that is in tune with the students' desire for interactive and goal-oriented learning.

Seeing as gamified learning incorporates content delivery, engagement and feedback it is important to structure how learning is designed within the CyberSafe Learning Hub. Insights from Gwenhure et al. (2024) and Maluda et al. (2023) support the addition of attributes like quizzes, phishing exercises or real-time progress dashboards to the platform. These elements

help to ensure that learners remain engaged and sustainably improve their cybersafety knowledge in the CyberSafe Learning Hub environment.

2.2.3 Case Studies of Gamification in Higher Education

Recent researches indicate the importance of gamification in higher education. Maluda et al. (2023) tested gaming and cybersecurity training for undergraduates, and discovered that when the sessions were gamified this significantly enhanced understanding and memory retention when compared against not gamified lectures. Similarly, Ambikapathy et al. (2024) Games and higher education in Malaysia Gamification is found to have an impact on the increased attendance rate and motivation of young generation learning at Malaysian universities based on their learning preference. A typical element of gamification platforms are leaderboards, which have been proved in previous works to induce competition and motivation between students (Maluda et al., 2023; Ambikapathy et al., 2024). While these studies are not directly related with the use of leaderboard, they emphasize the fact that competitive components sustain engagement and support long-term behaviour change.

Review of the case series described in Maluda et al. (2023) and Ambikapathy et al. (2024) prove that gamification can work on the educational context. These findings justify the inclusion of features such as leaderboards and progress tracking in the CyberSafe Learning Hub, which have been shown to increase engagement and motivation for university students.

2.2.4 Existing Tools and Platforms

There are already several sources that use gamification in cyber security education. For example, TryHackMe has the labs/games approach with points/levels/badges, but the content isn't beginner friendly and requires a lot of technical literacy. HackTheBox Academy offers an online environment based on virtual machines where students could solve penetration testing challenges gamified but it might be too difficult for university or college students that do not have a technical background. Cybrary, for example, offers organized cybersecurity courses that come with quizzes, hands-on labs and career-focused road maps. Cybrary is a bit more user-friendly compared to HackTheBox and predominantly emphasizes workforce training/professional certification rather than student-oriented awareness.

These constraints underscore a requirement for a dedicated platform that combines gamification with accessible, awareness-themed content targeted at university and college students.

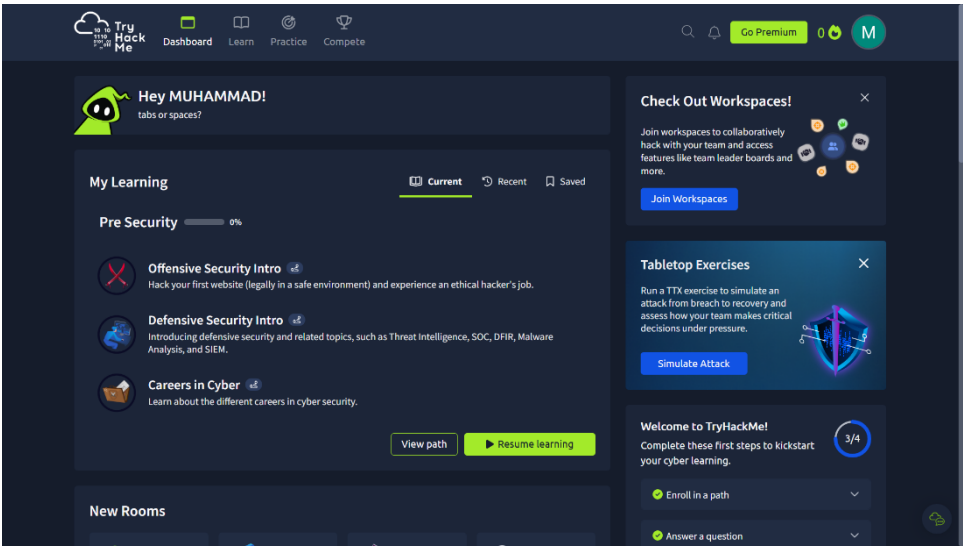


Figure 2.2: TryHackMe interface with progress badges

Figure 2.2 presents the interface of TryHackMe, one of the most widely recognized gamified cybersecurity learning platforms. It motivates users with progress badges, ranking systems and scenario-based challenges. Every badge signifies knowledge of a content area or accomplishment on some sort of challenge that students can feel proud to earn. But while this format is optimal for the more technically inclined, some potential barriers to entry may be found here with deeper concepts and hands-on penetration testing exercises.

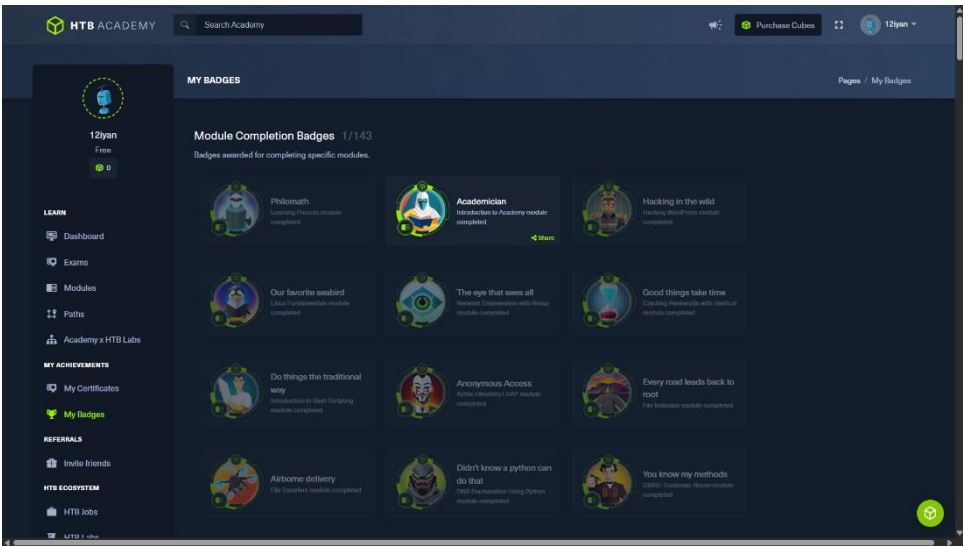


Figure 2.3: HackTheBox Academy challenge map

Figure 2.3 shows the challenge map interface of HackTheBox Academy, which offers penetration testing and cybersecurity skill-building exercises in a gamified format. Learners are able to connect environments for a variety of levels tied to on-the-job cybersecurity scenarios. Although this approach develops exploration and independence, this type of technological focus that can cater to the IT specialist or expert is not always necessarily accessible.

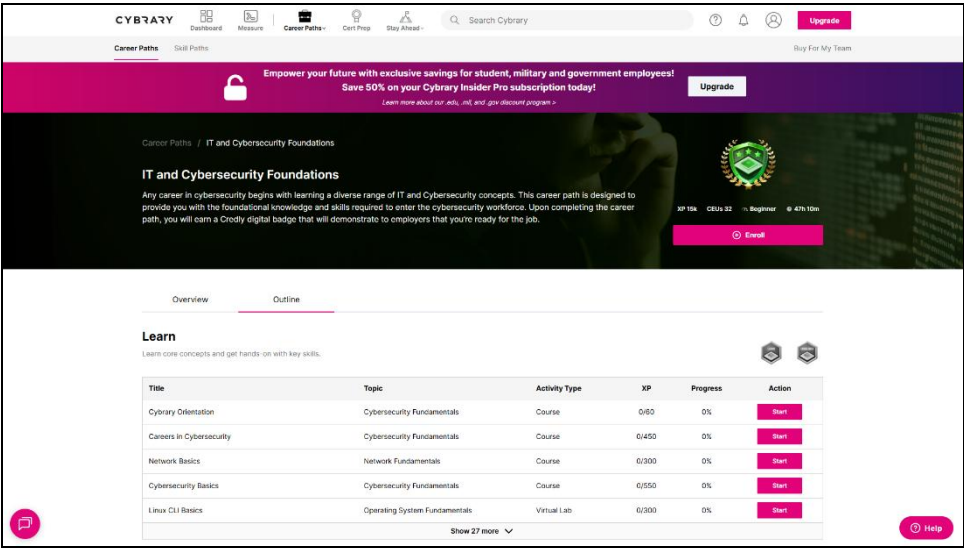


Figure 2.4: Cybrary learning roadmap dashboard

Figure 2.4 illustrates the learning roadmap dashboard from Cybrary, which provides structured course pathways, skill-tracking, and progress monitoring features. Cybrary, in contrast to TryHackMe and HackTheBox Academy, is more focused on career development, certifications and workforce training. Its roadmap guides learners in mapping out their path as per career requirements, so it is definitely a helpful resource for IT learners. But even though Cybrary’s easy-on-the-eye layout most certainly makes accessing the content easier, it may not be the ideal solution for university entrants that are at beginner level, and need more awareness raising, gamification-based training.

The analysis of existing gamified cybersecurity platforms like TryHackMe, HackTheBox Academy and Cybrary has shown that the current tools are aimed at advanced technical audience rather than beginners. Our research supports the focus of CyberSafe Learning Hub as a starter site and awareness-centered experience specifically for tertiary education students. The results validate the course’s choice to focus on low-level cyber security knowledge rather than more advanced penetration testing challenges.

2.2.5 Challenges and Limitations of Gamification in Cybersecurity Awareness

While gamification has been shown to have a great potential for promoting cyber security awareness, it also presents serious threats. A first-order limitation lies in the risk of over-focusing on extrinsic rewards such as points and badges which might make students concentrate on earning rewards rather than internalizing secure habits. This could detract from real learning to shallow competition.

Another major challenge is the prior knowledge of learners. Some works emphasize that participants usually have very different expertise when they start a gamified training. For instance, if the task is too easy, experienced learners can get relatively bored by feeling that the task is meaningless.

If on the other hand, the activities are too challenging, students may become discouraged and eventually tune out. In both scenarios, the efficacy of gamified learning is degraded. This highlights the importance of precise balancing of difficulty, skill scaffolding, and adaptive learning paths in order to keep all learners engaged and benefiting from the training.

Additionally, contextual adaptation remains a limitation. Strategies that prove successful in corporate environments, such as competitive leaderboards, may not translate effectively into higher education settings where collaboration and inclusivity are more important (Gwenhure et al., 2024). Poorly designed gamified systems can unintentionally exclude learners or discourage participation if they do not align with the educational culture or learners' motivations.

These challenges underline the importance of designing gamified systems that are simple, inclusive, and tailored to the learners' expertise and environment. A balanced approach that integrates both intrinsic motivation (curiosity, mastery, problem-solving) and extrinsic rewards can maximize effectiveness and foster long-term behavioural change in cybersecurity awareness.

Investigating challenges such as overreliance on extrinsic rewards, differences in learner skill levels, and contextual adaptation issues (Gwenhure et al., 2024) provides valuable guidance for improving the design of the CyberSafe Learning Hub. These insights justify incorporating adaptive difficulty levels, inclusive design principles, and a balance between intrinsic and extrinsic motivation. By addressing these limitations, the CyberSafe Learning Hub aims to create a more engaging, fair, and educational gamified learning experience for all users.

2.2.6 Investigation Summary Table

Table 2.1: Investigation Summary Table

Year	Title / Author	Aim	Findings
2023	Evaluating the Effectiveness of Gamification to Increase Cybersecurity Awareness among Students — Maluda et al.	To evaluate the impact of gamification on cybersecurity awareness among students.	Gamification significantly improved awareness and engagement, showing higher retention compared to traditional teaching methods.
2024	Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students — Razack & Saad	To design an interactive gamified platform for cybersecurity education.	Students reported better motivation and learning outcomes, with increased interest in cybersecurity practices.
2024	Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review — Gwenthure & Rahayu	To review existing studies on gamification for non-IT professionals.	Gamification is effective in improving awareness but challenges remain in sustaining engagement and measuring behavioral change.
2021	Assessing the Effects of Gamification on Enhancing Information Security Awareness — Wu et al.	To assess the impact of gamified approaches on information security awareness.	Gamified training increased awareness and improved compliance behavior compared to non-gamified training.
2022	Game-based Learning Platform to Enhance Cybersecurity Education — Khan	To introduce a game-based learning platform for cybersecurity education.	Students showed higher knowledge retention and found the learning experience more enjoyable.
2025	A Case Study in Gamification for a Cybersecurity Education Program: A Game for Cryptography — Huitema & Wong	To develop and test a gamified cryptography learning tool.	The game improved students' understanding of cryptography concepts and fostered active participation.
2024	Gamification for Cybersecurity Education in Malaysian Universities: A Case Study — Ambikapathy et al.	To explore the effectiveness of gamification in local higher education	Reported increased participation and motivation among students, highlighting cultural and contextual relevance.
2024	Gamification in Cybersecurity Education: A State-of-the-Art Review and Research Agenda – Pramod et al.	To examine existing gamification approaches in cybersecurity education and outline future research needs.	The review highlights key game elements used, common benefits, existing challenges, and areas for further development in cybersecurity education.

2.3 Related Works

Cybersecurity training platforms like TryHackMe, Cybrary, and HackTheBox Academy have gained immense popularity for teaching the concepts of cybersecurity using gamification as well as simulations and structured learning. As much as these platforms are successful, the learning assumes that the user has technician-professional level of understanding, which does not cater well to the general university and college student population. The next subsections of this chapter discuss the platforms' methodologies, the interfaces, the strengths, and the limits of each, including relevant figures.

2.3.1 TryHackMe

TryHackMe is a gamified cybersecurity training platform designed for both beginners and advanced learners. Its content is organized into “rooms” and “learning paths” consisting of reading with guided materials, interactive activities, and lab work. Users of the platform get motivated with elements of gamification, such as points, badges, and leaderboards.

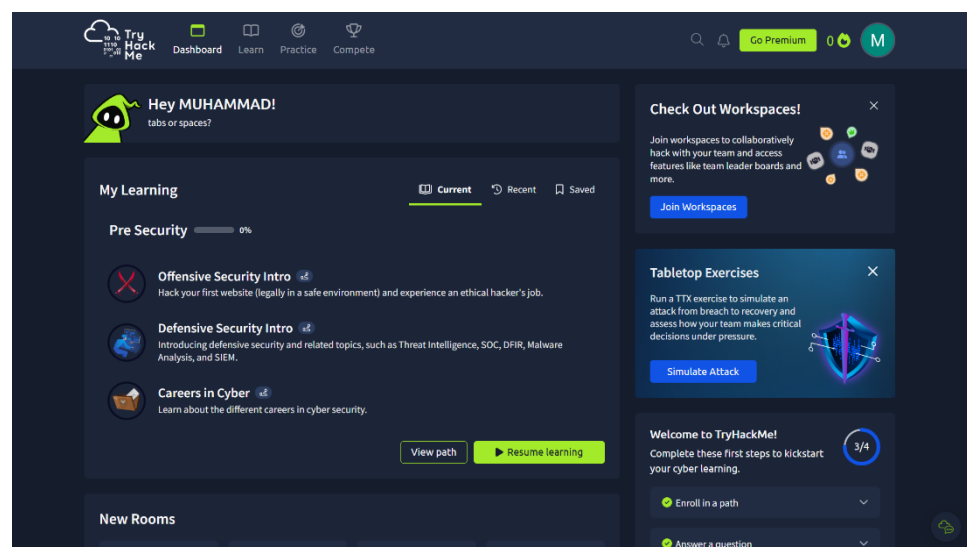


Figure 2.5: TryHackMe Dashboard

As illustrated in Figure 2.5, the TryHackMe dashboard is where users can track their progress and other metrics such as earned badges, streaks, and leaderboard ranks. This demonstrates the ability of the platform to provide elements of gamification intended to provide a sense of achievement and competition.

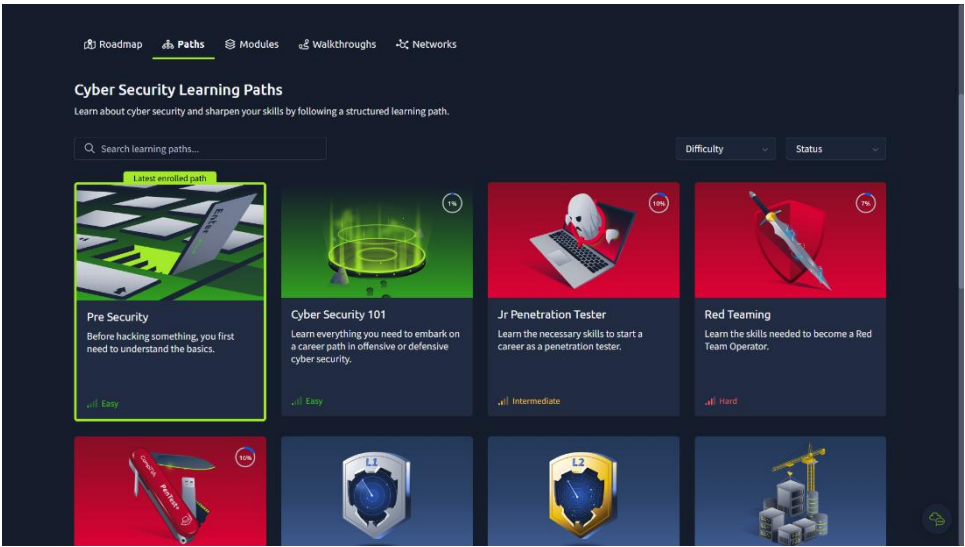


Figure 2.6: TryHackMe Learning Path Page

Figure 2.6 illustrates the Learning Path page that shows a list of rooms based on levels or categories. This illustrates how the system organizes progression of knowledge. It teaches students step-by-step, from surface to deep knowledge.

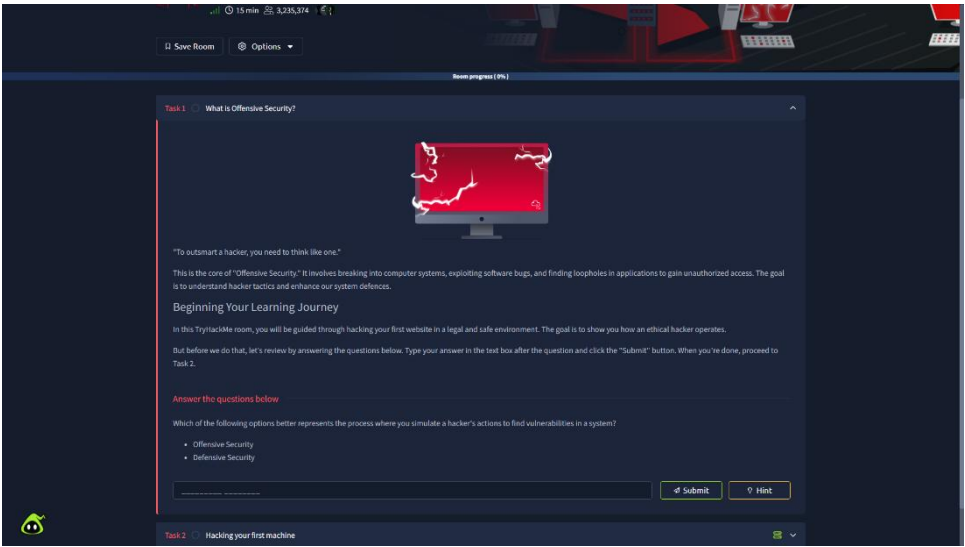


Figure 2.7: TryHackMe Challenge Room Interface

An example of a Challenge Room interface is shown in Figure 2.7, where instructions are presented on one face and there may be an embedded terminal or exercise space on the other side. We think this is a great example of how both theory and practice appear to be integrated which presents the opportunity for learners apply their knowledge in real time.

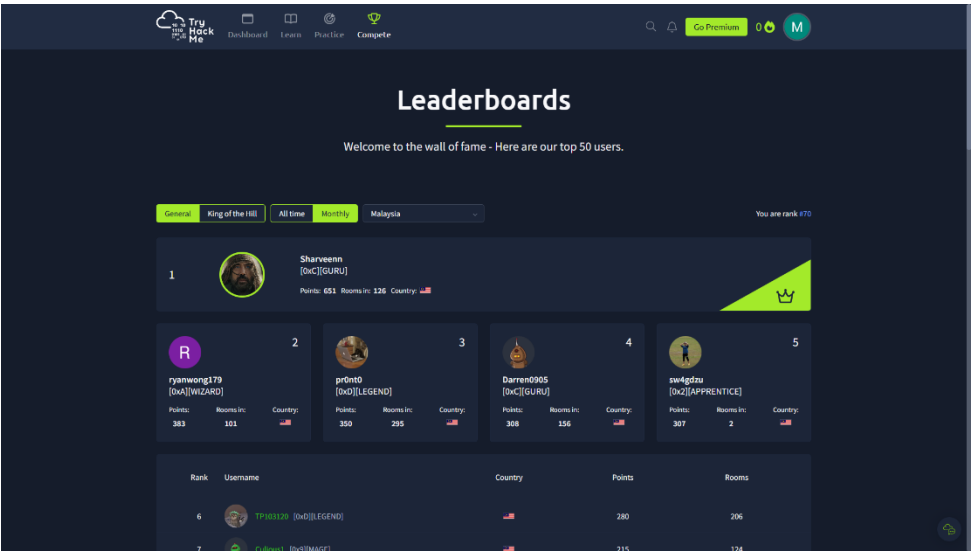


Figure 2.8: TryHackMe Leaderboard Interface

The TryHackMe's leaderboard section screenshot is shown in Figure 2.8, where users are awarded points through completing the challenges that are being displayed as toppers of the table. This competitive nature serves to increase extrinsic motivation in the learners and to keep them coming back for more.

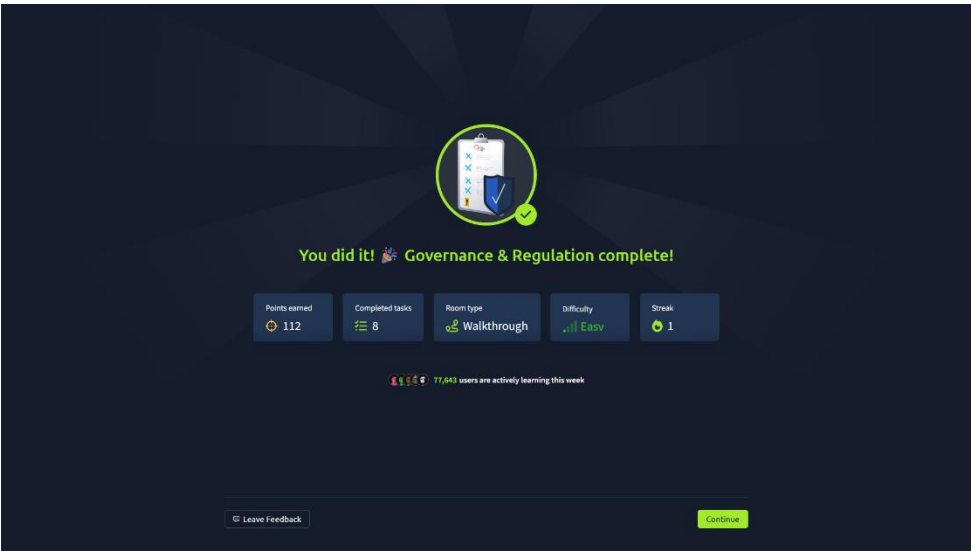


Figure 2.9: TryHackMe Completed Room Example

Figure 2.9 shows the completion summary page of a TryHackMe room known as "Governance & Regulation." The interface shows points earned, number of tasks finished, room type and difficulty and learning streak. This solidifies the game principle of feedback and recognition that learners can see their great effort in their easy-to-read progress report.

The user starts by selecting a room or a path. Starting with a brief concept overview, rooms deliver tasks that require learners to interact with sandbox.sh environments, such as executing commands, or taking advantage of a misconfigured service. Learners submit flags or badges, as evidence of progress; they instantly earn feedback to accompany reward points. These points are aggregated into badges and ranking levels which can be viewed in the dashboard, to keep learners motivated.

TryHackMe really shines in realistic simulation with its large collection of practical rooms which mirror real-world security setups and situations. These learning labs are particularly important for practical skill development, specifically in areas such as vulnerability identification, exploit techniques and secure system configurations all of which complement theoretical knowledge through hands-on use. This is in line with prior work where the platform's gamified aspects like points, badges, ranks have also helped maintain learner motivation through providing an incentive for continued engagement and effort. But when it comes to awareness training like among non-technical university or college students, the depth and complexity of the platform can be intimidating. A lot of the exercises take for granted knowledge of basic command-line utilities, networking material and penetration testing techniques which might exclude some less IT literate learners. On the other hand, even if technical capabilities are reinforced through offensive and defensive challenges, the platform does not directly provide simplified awareness packages like phishing recognition, password hygiene or safe web browsing which would be essential for everyday cybersecurity behaviour. In summary, TryHackMe is efficacy in up-scaling skill acquisition for budding cybersecurity professionals - albeit with a large amount of modification to the tool for it to be used as an awareness mechanism within global higher education.

2.3.2 Cybrary

Cybrary is a platform that provides structured, “course style” training in ever-expanding topics ranging from ethical hacking, to cloud security, critical incident response (cyber crisis management), network defense and threat intelligence. It focuses on comprehensive content coverage through a combination of video, readings, quizzes and optional labs.

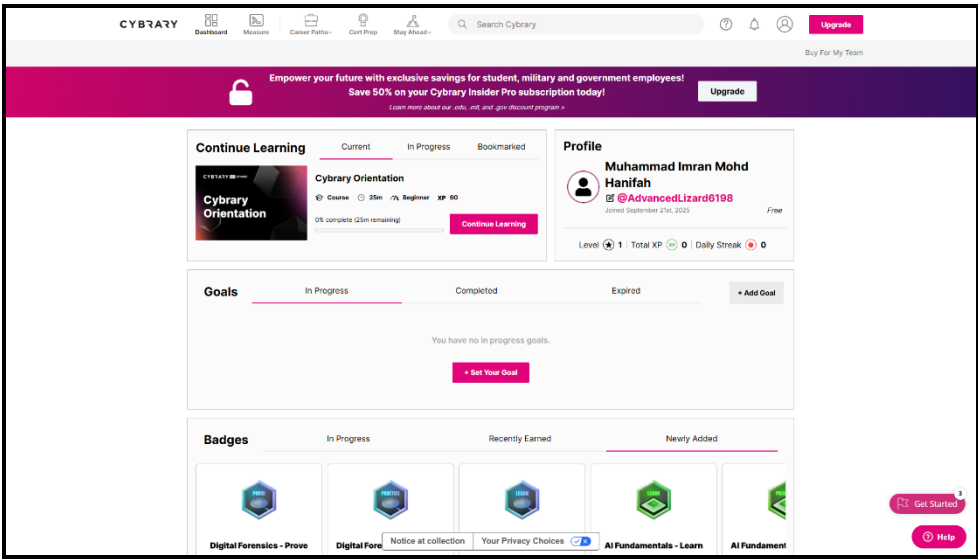


Figure 2.10: Cybrary Dashboard Page

Figure 2.10 shows the Cybrary dashboard through which users can monitor their learning progress, continue courses and develop course recommendations in line with user objectives. By visually displaying progress, achievements and next activities of learning paths this personalised way of learning promotes a continuous involvement.

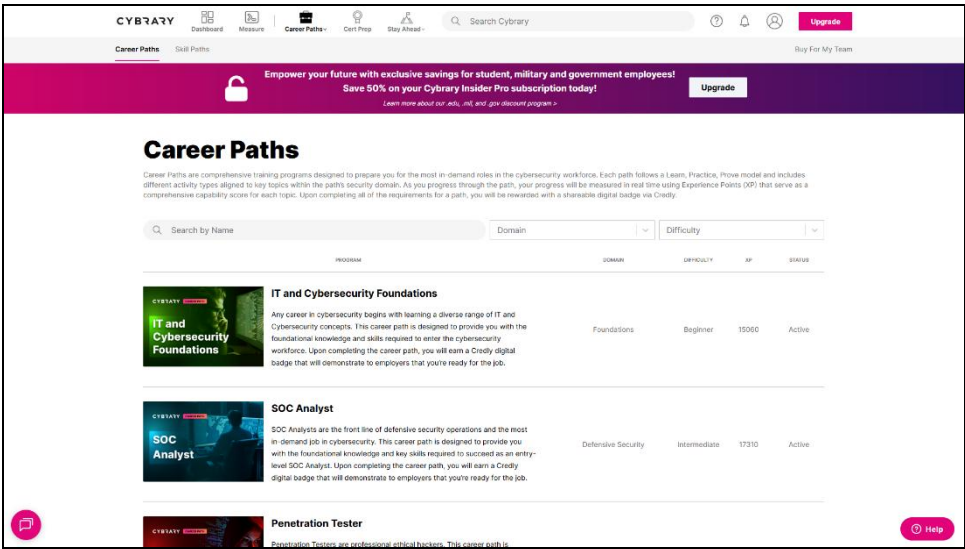


Figure 2.11: Cybrary Course Catalog and Career Paths

In Figure 2.11, a snapshot of the Cybrary course catalog and career paths is provided in which learners may follow a structured path such as SOC analyst or PenTester. This function places Cybrary among the platforms providing content that also steers its learners towards targeted professional roles in cybersecurity.

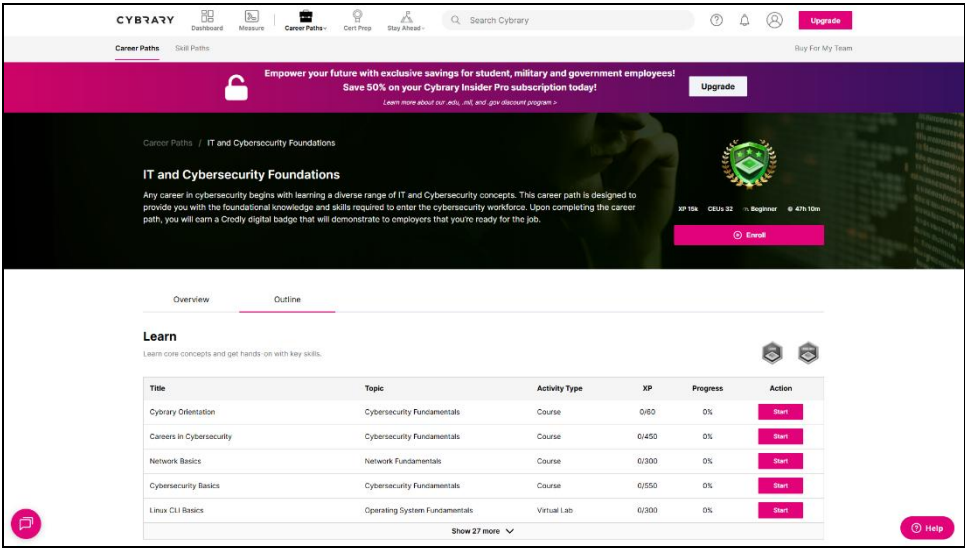


Figure 2.12: Cybrary Course Module Page

Figure 2.12 shows a Course Module page integrating video, transcripts, and checkpoint quizzes. In presenting material in various forms, and providing checks on understanding at intervals, Cybrary takes an academic approach with its structure that is close kin to traditional classroom instruction.

Learn					
Learn core concepts and get hands-on with key skills.					
Title	Topic	Activity Type	XP	Progress	Action
Cybrary Orientation	Cybersecurity Fundamentals	Course	0/60	0%	Start
Careers in Cybersecurity	Cybersecurity Fundamentals	Course	0/450	0%	Start
Network Basics	Network Fundamentals	Course	0/300	0%	Start
Cybersecurity Basics	Cybersecurity Fundamentals	Course	0/550	0%	Start
Linux CLI Basics	Operating System Fundamentals	Virtual Lab	0/300	0%	Start
Show 27 more					

Figure 2.13: Cybrary Learning Progress Dashboard

Figure 2.13 shows the Learner Progress Dashboard, where data like completion percentage, and badges earned is tracked. This tracking mechanism functions to support self-regulated learning by providing feedback on attainment of goals and opportunities for improvement.

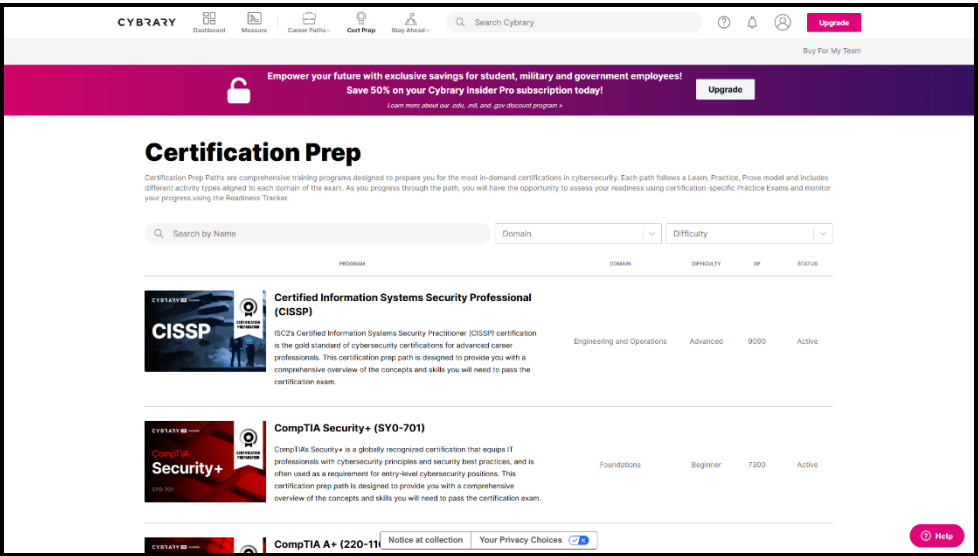


Figure 2.14: Cybrary Certification Preparation Page

Figure 2.14 is the Cybrary certification prep page, where you can find learning paths for various cybersecurity certifications including CompTIA Security+ and CISSP. This design demonstrates how Cybrary incorporates professional certification readiness into its learning path.

Learners enrol on a course or career pathway then progress through a series of modules that integrate theoretical material with assessment. Labs are available for advanced students to test theoretical material. It is assessment driven and tracking of course progress and learner performance through quizzes, dashboards that are fairly easy to for the user to view.

Cybrary does well to itself as its courses are completely organized and detailed, offering cyber professionals to study on a clear path, knowing at all times where they stand and how much they have learnt. The platform’s modular nature, checkpoint quizzes and optional labs make it to ensure that the learners gain both the theoretical knowledge and practical skills, more so for individuals aspiring professional certifications. Though, because Cybrary has a focus on courses and certification-based content, the users are not going to have as interactive simulation like TryHackMe or HackTheBox. This can limit the hands-on involvement and can therefore be less suitable for non-technical or a typical college population who are looking for shorter, engaging awareness training. Therefore, though Cybrary is perfect for those already in the workforce as far of career learners are concerned, in practice its methodology is also not enough for people that learn better with scenario-based learning by doing activities on security awareness.

2.3.3 HackTheBox Academy

HackTheBox Academy brings the HackTheBox ecosystem into structured learning paths focusing on penetration testing labs with a curated list of resources. It is a favourite among high-level learners and cybersecurity experts.

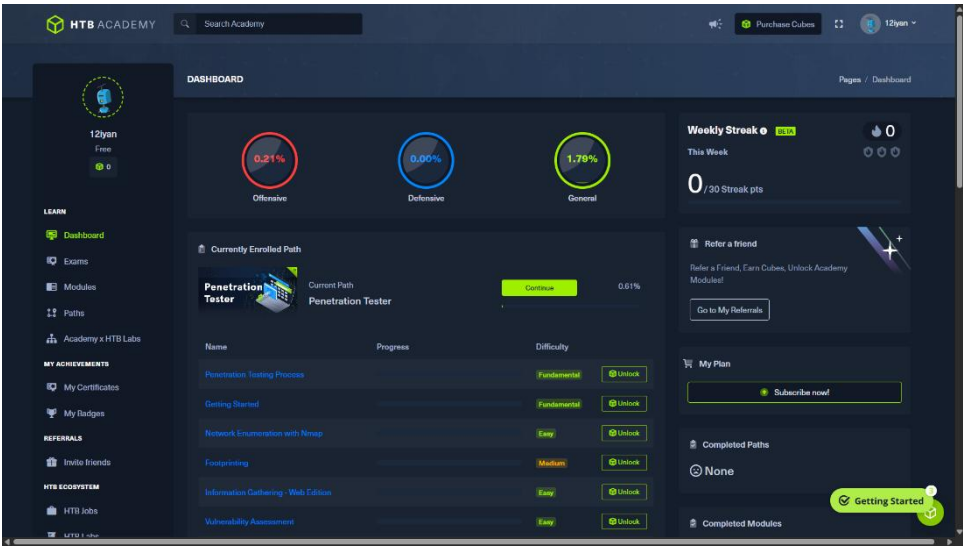


Figure 2.15: HackTheBox Academy Dashboard Page

Figure 2.15 displays the HackTheBox Academy Dashboard, where users can view accumulated points, ranks, and achievements. This gamified interface encourages motivation through competition and visible progress tracking.

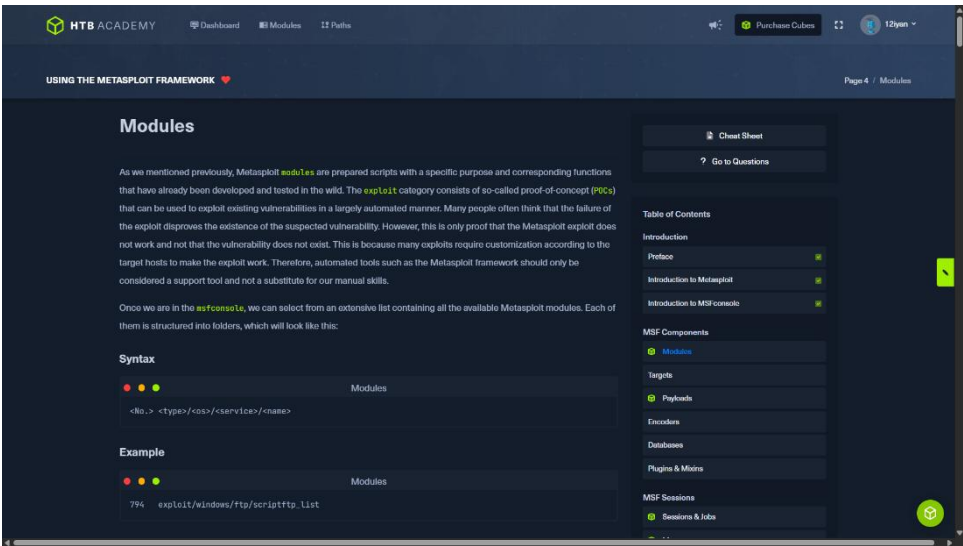


Figure 2.16: HackTheBox Academy Lab Interface Page

Figure 2.16 shows the Lab Interface direction, where learners interact with a set of vulnerable virtual machines or services for exploitation. This design makes the most sense

and is based on real penetration testing environments, which will enable students to be transferred from this space to a real world with ease.

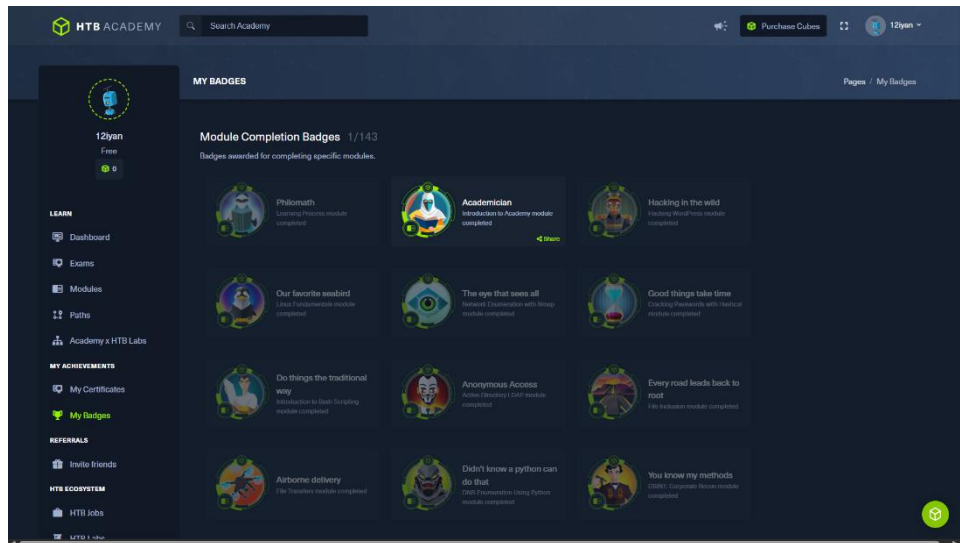


Figure 2.17: HackTheBox Academy Completion Badge Page

Figure 2.17 shows the Learning Track Completion Page which gives learners digital badges when they have completed certain modules or tracks. This badges are used in reward and acknowledge the achievement and skill development.

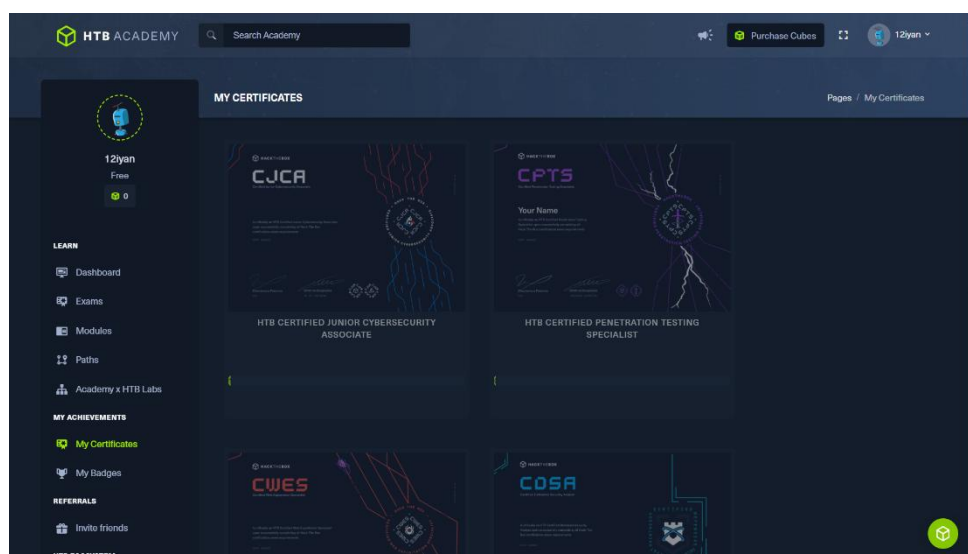


Figure 2.18: HackTheBox Academy Certificate Page

Figure 2.20 shows the Certificate Page, which learners can use to see or save certificates of completion for particular learning paths or modules. This formal recognition provides greater satisfaction and credibility to learners.

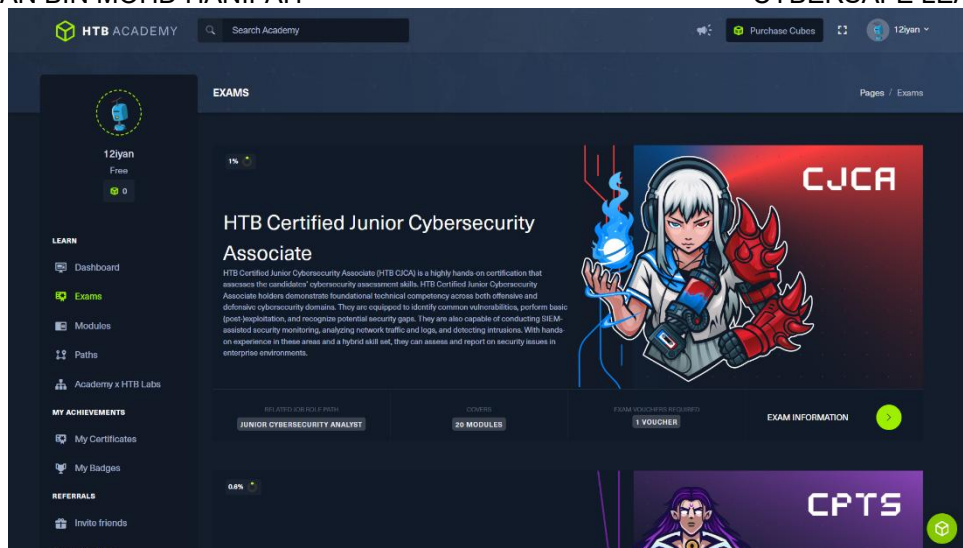


Figure 2.19: HackTheBox Academy Exams Page

Figure 2.21 shows the Exams Page to enable learners take guided assessments that access their understanding and empirical competence. Examination encourages retention of skill and application in real world.

HackTheBox Academy is modeled with a lab-first method. Students are provided with a quick high-level briefing before they attempt to solve a vulnerability challenge in a sandboxed setting. Advancement is based on finding a “flag,” indicating that the task has been executed. Learners progress in rank by solving increasingly challenging labs, and have the option to challenge friends in team competitions.

HackTheBox Academy is truly a one of its kind when it comes to being real life like labs having very close replica of actual vulnerabilities and real-world attack vectors. It's a scenario-based learning approach where participants will encounter a variety of practical security challenges ranging from web vulnerabilities to network attacks, in an environment that closely simulates your computing work stations and your networks. This practice-based approach is an efficient method of building technical skills, problem solving applications and draw insights into adversary techniques. The platform's high technical intensity and reliance on previous knowledge does not seem suitable for mass university or college student awareness training. It offers a depth that's very helpful for advanced students, but may be too high of a ceiling for non-technical students on the labs. However, HackTheBox Academy is a good model for example for scenario-based training that might be modified or even simplified to make the cybersecurity awareness engaging for wider groups of people.

2.4 Comparison

It is also worth comparing online cybersecurity learning platforms in respect of features, target users, usability, emphasis on security and learning outcomes. There are also other training platforms such as TryHackMe, Cybrary and then HackTheBox which all offer their own unique path toward cyber security training from guided labs, cert prep, and full-on advanced hacking simulation. A comparison between these 3 platforms is in the table below with key criteria are taken into consideration.

Table 2.2: Comparison of Existing Project

Criteria / Project	TryHackMe	Cybrary	HackTheBox
Features	Hands-on labs, guided learning paths, gamified challenges, beginner to advanced content.	Video-based courses, structured career paths, certification prep, broader IT training.	Capture-the-flag (CTF) style labs, pro labs, real-world hacking simulations, community-driven challenges.
Users	Students, cybersecurity beginners, and professionals seeking practical labs.	IT and cybersecurity learners, professionals preparing for certifications, corporate teams.	Intermediate to advanced cybersecurity enthusiasts, penetration testers, red teamers.
Navigation	User-friendly dashboard, task-based modules, gamified progress tracking.	Traditional e-learning platform, course catalogs, structured paths.	Technical interface, challenge boards, VPN-based access to labs.
Security Element	Focus on hands-on security skills, attack/defense scenarios, real tools.	Theory + conceptual security knowledge, compliance, certification focus.	Realistic hacking environments, exploit development, offensive security practice.
Output	Practical experience, strong foundation for beginners, progression into advanced labs.	Certification readiness, theoretical understanding, corporate-level upskilling.	Advanced hacking expertise, strong offensive skills, recognition in global CTF community.
Accessibility	Beginner-friendly, low prior knowledge required, web-based interface.	Accessible via standard web browser, moderate tech skills required.	Requires intermediate technical knowledge, VPN setup, and familiarity with Linux/command line.
Gamification	Points, badges, leaderboards, streaks to motivate learning.	Minimal gamification, mostly progress tracking and completion metrics.	Leaderboards, points, ranking in global CTF challenges, competitive environment.
Adaptability	Flexible learning paths, self-paced, suitable for classroom integration.	Fixed courses, career tracks, less flexible for self-directed exploration.	Highly scenario-specific, advanced labs may be adapted for competitions or skill practice but less beginner-friendly.

2.5 Discussion

By comparing TryHackMe, Cybrary and HackTheBox, it is clear that every platform demonstrates specific strengths which cater for different aspects of cybersecurity education.

TryHackMe has structured learning paths which are accessible and guided. This makes it particularly effective for beginners or intermediate learners. Through its interactive labs and game-like design, engagement is maintained as well as foundational skills gradually increase in level. These elements will be essential for classroom use or even formality within universities under the leadership of researchers working on thematic projects. The features that will be implemented from TryHackMe are simple gamified elements such as points, badges, and basic guided learning paths to keep learners motivated and on track.

In contrast, Cybrary is more about professional development and preparing yourself for industry standard certifications. With its wide range of courses covering both the technical and managerial sides to security practices in today's businesses world, it is perfect for corporate training environments as well as certification-seekers themselves seeking industry-recognised creds. The features that will be implemented from Cybrary are progress tracking dashboards and short quizzes to monitor learning outcomes effectively.

HackTheBox Academy however is a completely different experience, focusing on realistic penetration testing and extreme problem-solving. Within this platform, it contains the natural appeal of Capture-the-Flag style activities and a grassroots ecosystem built by the community for learners who have already obtained fundamentals and want to further develop their skills in offensive security. The HackTheBox Academy features that will be added to CyberSafe Learning Hub are some basic, scenario-based exercises and a simple leaderboard to facilitate interaction and have some friendly competition.

In general, choice of a platform is determined by the learner's objectives. TryHackMe shows that it is most useful for intermediate or advanced learning, Cybrary does best in certification or career focused pathing, and HackTheBox Academy is more beneficial to someone looking to do advanced attacks and keep honing the "offensive" skill set. Between them, these three platforms combine to cater to the entire range of cybersecurity learning from basic awareness all the way through professional development and specialized skills.

2.6 Conclusion

This chapter was a survey of prior works for the use of gamification in cybersecurity awareness, and other learning platforms with interactivity, gamified practice or scenario-based learning. Research shows that gamification leads to improved engagement, motivation and retention of learners but there are issues such as pre learning requirements and contextual adaptation which needs to be accounted for. TryHackMe, Cybrary, and HackTheBox Academy are some of the platforms analyzed to identify some divergences. TryHackMe have guided and gamified learning paths for beginners. Cybrary focuses on professional growth and certification. HackTheBox Academy serves excellent realistic challenges for advanced learners.

The features that we will be embracing for the CyberSafe Learning Hub aims primarily in simplicity and low barriers to use, consisting of guided learning paths, points and badges to support gamification, tracking of progress, short quizzes as well as basic scenario-based exercises. It is expected, through this combination, that the project will be able to deliver to university and college level students a user-friendly useful system conveying a range of cyber security issues as well as being practical and easy to use.

3 METHODOLOGY

3.1 Introduction

Methodology is the general strategy that outlines systematical design, development and evaluation of a project. It provides a roadmap that helps the authors organize their work to meet specific goals efficiently. An effective methodology defines how software development stays organized, traceable and adaptive over time (Pressman & Maxim, 2020).

Agile Methodology was used in developing the CyberSafe Learning Hub. Agile has a focus on adaptability, teamwork and incremental development which is more appropriate for web-based systems that are developed with tight user feedback loops. As students and lecturers are both to be involved actively in the project, Agile will provide for quick responsiveness when it comes to their feedback and at the same time a structured as well as purposeful development process.

3.2 Agile Methodology

Agile methodology is a software development practice that promotes continuous incremental progress in an iterative fashion (sprints). There are several stages connected to the sprint, which is planning, design, development, testing, deployment review and launch cycle that iterates throughout the project to provide flexibility and continuous improvement.

According to Popa et al. (2021), the Agile methodology offers flexibility and communication between developers and clients by splitting the project into small portions that can be improved in each iteration. This allows for review of the solution along with feedback, which reinforces continuous work to improve quality and match what users want. Agile tends to be transparent, promotes communication and gives teams the opportunity to produce working editions of the system quickly, mitigating risk with software projects.

This approach is particularly appropriate for this project as there is regular input from both the students (end users) and lecturers (administrators). With short iteration cycles feedback can rapidly be collected and reflected upon which not only keeps the platform engaging, interactive and educational but also effective. Furthermore, Agile allows flexibility in refining gamification features, lesson modules, and progress tracking elements based on real user experiences.

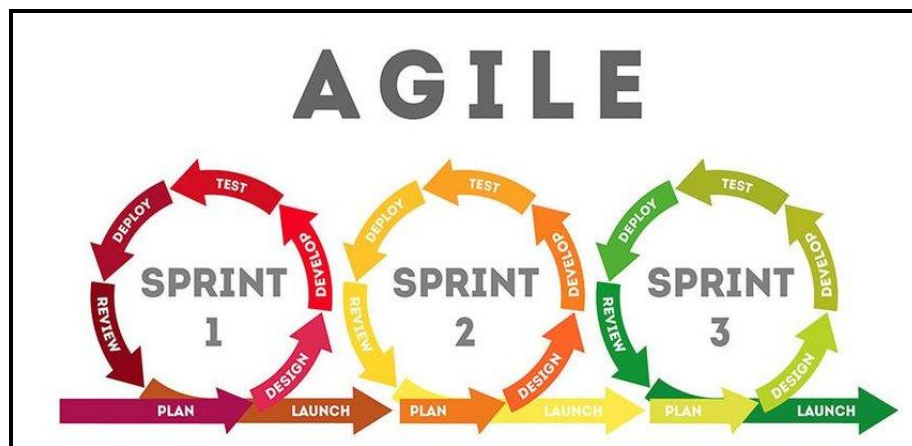


Figure 3.1: Agile Methodology Diagram (Popa et al., 2021)

The process for the Agile methodology can be seen in Figure 3.1, illustrating how development moves through stages of a number of sprints. Every sprint has a generic Plan -> Design -> Develop -> Test -> Deploy -> Review -> Launch that is repeated, leaving plenty of space for iterations and small porting periods. This process provides the space for each phase to reinforce system utility and user satisfaction, which is in line with the project's focus on developing an agile and user-centred cybersecurity learning platform.

3.3 Phases in Agile Methodology

The agile methodology is a process which is represented by discrete and iterative phases that enable to control the software development in an efficient way. The CyberSafe Learning Hub will participate in five essential phases for the project: Planning, Design, Development, Testing and Deployment and Review. There would be deliverables for each stage that would work in unison with the system to make it successful.

3.3.1 Phase 1: Planning

The planning stage is the cornerstone of Agile development, and it concentrates on being inspired by user and client-based needs before any designing or implementing starts. The first stage of this research examined the gap regarding cybersecurity awareness between college students and how they preferred to learn. The primary focus was to ensure that the design of CyberSafe Learning Hub would be driven by user requirements and education objectives.

Interview was conducted with a lecturer of Kolej Teknologi Antarabangsa Cybernetics (KTAC) who also acts as the client and somebody who is familiarize in teaching regarding cyber security to retrieve accurate data which are related to the project. The interview drew attention to the problems in teaching awareness of cybersecurity and what the lecturer expects from interactive learning platform. This conversation led to identifying indispensable system properties like tracking progress, gamified curriculum and role-based access control.

In addition, a survey was distributed to students asking them about their current knowledge of cybersecurity features like online threats and interest in gamified learning. The students' feedback has oriented and shaped what will be incorporated into the system, in terms of its functional requirements and contents or activities included according to their learning styles.

According to the discoveries obtained from these data collection activities, appropriate technology was selected for system development such as Laravel 12 for backend development, MySQL for database management, Bootstrap for front-end design and Google OAuth to ensure secure authentication. The output from this phase is the signed off proposal document, a comprehensive system requirement statement and technology selection report that form the starting point for Agile phases to follow.

3.3.2 Phase 2: Design

In this step architecture and user interface are defined. Flowcharts, use case diagrams and database schema were created to ensure that the development proceeds with systematic approach. Wireframes for students and lecturer dashboards were also created in order to visually explain the concept of lessons, quizzes and gamification. This stage is needed to make sure the back-end and front-end designs fit with user needs and are in line with project objectives.

3.3.3 Phase 3: Development

The development cycle is characterized by continuous coding and integration. The primary features like authentication, role-based dashboards, lessons and challenges CRUD operations, and gamification based on points/badges and progress tracking are implemented in Laravel. Continuous testing happens after each sprint so that all the modules are working fine and bug free. Its outcome is a prototype of the CyberSafe Learning Hub.

3.3.4 Phase 4: Testing

The testing phase is to guarantee the system reliability, security and usability. Several checks are conducted such as unit, integration and system testing. PHPUnit will be used to ensure that the tested module functions as expected with the notifications and data flow. A test with lecturers and students is used to test usability and provide feedback for refinement.

3.3.5 Phase 5: Deployment and Review

After testing, the system is launched in a testing or "staging" environment for trial by real users. Feedback from users and lecturers is gathered with surveys and interviews. Based on this

feedback, the system will be improved for performance and user experience. When approved, the final version will be deployed.

3.4 Requirement

The requirement phase is about collecting both functional and non-functional requirements so that the system satisfies users and client needs. According to Awati (2023), the requirement phase is vital for a project's development as it provides an understanding of requirements for contextual needs, conditions and expectations that must be addressed if the project is to succeed. This procedure aims at determining what the CyberSafe Learning Hub is expected to do and/or how the tooling should behave in order to fulfil these expectations in an efficient manner.

If the requirements are well-captured, then we can develop and test the system in a methodical way with little chance for misunderstanding or technical error. The need for this project was determined through direct feedback, collected via questionnaires and interviews to ensure the final product aligns with user needs and learning goals.

3.4.1 Data Gathering Techniques

Questionnaire and interview have been used to determine the needs of the users and their acceptability. These methods produce quantitative and qualitative results, encompassing an extensive exploration of user requirements and preferences in cybersecurity learning.

3.4.1.1 Questionnaire

Questionnaire is a structured tool developed for collecting opinions, experiences and knowledge from individuals in large numbers (Bhandari, 2021). For the current study, a questionnaire was administered to at least 50 students in Kolej Teknologi Antarabangsa Cybernetics (KTAC) using Google Form.

The questionnaire comprised of questions related to students' current knowledge on cybersecurity typical for a user, their preferred method of studying and learning process and the interest over gamified learning.

3.4.1.2 Interview

An interview is a qualitative research tool that helps to discover a participant's perspective through direct communication and discussion (University of Bath, 2023). An interview was conducted for this project with a lecturer of the KTAC acting as the client's side.

The interview was aimed at an exploration of the lecturers' issues with teaching cybersecurity subjects and some thoughts on how the interactive learning method may make better student participation. The lecturer stressed that classical teaching elements, like already available slides or lectures are not very attractive when it comes to attraction, and offered the recommendation of introducing interactive modules for learning experience such as quizzes and gamification.

3.4.2 Functional Requirement

Functional requirements describe the tasks and or activities CyberSafe Learning Hub should be able to do. These requirements describe what the system must do to achieve the user and client requirements in an efficient manner.

Table 3.1: Functional Requirement Table

Functional Requirement	Description
User Authentication	Allows users to register manually or log in using Google OAuth.
Role-Based Access Control	Provides different access rights for students and lecturers.
Content Management	Allows administrators to create, edit, and delete categories, modules, lessons, quizzes, and quiz questions.
Access to Lessons and Quizzes	Enables students to view and complete cybersecurity awareness modules.
Quiz Scoring and Feedback	Automatically evaluates quiz submissions, enforces an 85% passing threshold, and displays detailed results with correct and incorrect answers.
AI Chatbot Assistance	Provides an AI-powered chatbot during quizzes to help students understand cybersecurity concepts without revealing direct answers.
Progress Tracking	Records and displays each student's learning progress.
Gamification Features	Awards points and badges for completing lessons and quizzes.
Dashboard Monitoring	Enables lecturers to monitor and review student performance.

3.4.3 Non-Functional Requirement

Non-functional requirements specify the quality properties of the system, and include performance, security, usability, reliability and scalability.

Table 3.2: Non-Functional Requirements Table

Category	Requirement
Performance	The system should load each page within 5 seconds under normal conditions.
Usability	The interface must be simple and user-friendly for non-IT students.
Reliability	The system should maintain consistent operation without data loss.
Security	User credentials and progress data must be encrypted and protected.

3.4.4 System Requirement

System requirements delineate what hardware and software are required for the CyberSafe Learning Hub to develop and run. These requirements are there to make sure a system works effectively, meets its functional and non-functional objectives and is easy for users.

Since this project is related to designing a web-based system which could include interactive and gamified characteristics, so it would be mainly recommended to use the reliable hardware and software which should be able to possess capability of using tools for web development, local server operations and maintaining database on proper note.

3.4.4.1 Hardware Requirement

Hardware requirements are the physical components that support system implementation and operation. Good hardware guarantees smooth processes from coding to testing and deploying, without any hiccups or bottlenecks.

In this project, the Lenovo IdeaPad Gaming 3 laptop are used for development, which is powerful enough to perform web programming, executing virtual environments and testing databases.



Figure 3.2: Lenovo IdeaPad Gaming 3

Figure 3.2 shows the Lenovo IdeaPad Gaming 3 which is the laptop that will be used to develop this project.

Table 3.3: Hardware Requirements Table

Specification	Description
Model	Lenovo IdeaPad Gaming 3
Processor	AMD Ryzen 5 5600H (6 Cores, 12 Threads, up to 4.2 GHz)
Graphics	NVIDIA GeForce GTX 1650
RAM	16 GB DDR4
Storage	512 GB SSD
Operating System	Windows 11 (64-bit)

The Lenovo IdeaPad Gaming 3 is a mix of performance and efficiency that developers can work with. The AMD Ryzen 5 5600H CPU provides fantastic multitasking, and fired up with local testing and code compilation is a breeze thanks to 16 GB of DDR4 RAM. The built-in NVIDIA GeForce GTX 1650 GPU can deliver web visuals and modern browsers efficiently. Additionally, having a 512 GB SSD speeds up files access and project loading times, while Windows 11 ensures compatibility with current web development environments such as XAMPP, Visual Studio Code, and Laravel.

3.4.4.2 Software Requirement

The software requirement is the technical tool or framework that needs to be used to construct, test and operate on CyberSafe Learning Hub. Every software component has a role to play in backend development, frontend design, database management and authentication process.

- **Code Editor: Visual Studio Code (VS Code)**

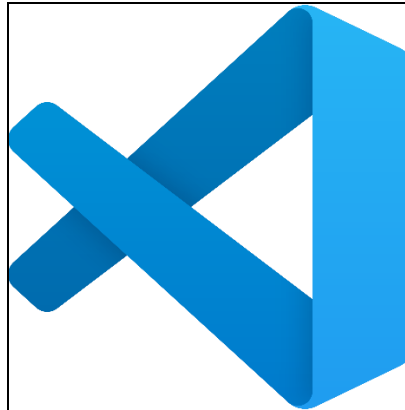


Figure 3.3: Visual Studio Code Logo

The primary source-code editor, was Visual Studio Code. It is compatible with languages like PHP, HTML, CSS and JavaScript and comes with built-in debugging, syntax highlighting, version control etc. These features better streamline workflow and promote enhanced code quality in Laravel development.

- **Backend Framework: Laravel 12**



Figure 3.4: Laravel 12 Logo

The backend framework utilized is Laravel 12 which provides a secure and robust way to authenticate, perform database operations as well as MVC architecture.

Its functionalities, middleware, routing and validation reduce the complexity of creating secure web applications.

- **Database Management System: MySQL 8.0**



Figure 3.5: MySQL Logo

The relational database management system (RDBMS) we use is MySQL 8.0 to save all user data, lesson content, quiz results and gamification records. It supports many features including reliability, scalability, and it's compatible with Laravel's Eloquent ORM.

- **Frontend Framework: Bootstrap 5**



Figure 3.6: Bootstrap Logo

Bootstrap 5 will be used for responsive and user-friendly layout design. This is to ensure that pages are easy to navigate and visually appealing to the users.

- **Authentication API: Google OAuth**



Figure 3.7: Google OAuth Logo

Google OAuth API enables secure authentication by using a third-party identity provider and allowing them to sign in with their Google account. This makes documentation easy to access, and lessens the risk of password-based vulnerabilities.

- **Testing Framework: PHPUnit**



Figure 3.8: PHPUnit Logo

PHPUnit will be used for unit and integration testing to complete the application with efficient outcome. Automations built through testing not only help in ensuring reliability but also in early development cycle's issue.

- **Web Server Environment: XAMPP (Apache)**



Figure 3.9: XAMPP Logo

XAMPP is a relatively easy to use local web server environment containing Apache, MySQL and PHP. It is designed to enable running the Laravel application locally before pushing to the cloud.

3.5 Analysis

The interpretation of the data collected from our requirements gathering can be determined in the analysis phase as it is medically analysed and produced, delivering sound and stunning insight for developing the CyberSafe Learning Hub system design. Based on questionnaires given to students and a interview with a lecturer from Kolej Teknologi Antarabangsa Cybernetics (KTAC), this study attempted to learn about users level of awareness of the cyber security implications around them, their learning preference and what kind of system abilities they required in an online education system. A questionnaire generated quantitative data that showed the students are aware of what cybersecurity information is, yet lacks a lot of practical knowledge and has inconsistent safe habits when online to keep them safe. In the meantime, the interview provided some qualitative points from an educator's perspective, including a desire for structured and interactive content for lessons but also tools to track students' progress through features like quizzes and game elements designed to boost engagement.

3.5.1 Data Gathering Analysis

Data collecting and analysis is the process of scrutinizing hard information gathering method and drawing a conclusion based on meaningful insights which system development will use (Saunders et al 2023). This analysis was based on questionnaires and structured interviews, collected for the CyberSafe Learning Hub project. The primary goal was to learn about the requirements, awareness and expectation of target users which is students and lecturers from Kolej Teknologi Antarabangsa Cybernetics (KTAC).

Using this analysis, the study pinpointed crucial system prospection for critical assets of interest such as cybersecurity awareness material, interactive learning modules and engaging user functionalities. Through a systematic review and synthesis of the collected data, we identified the features, functionalities, and design framework required for creating a user-centric and functional platform. These captured learnings are crucial learning points that will contribute to shaping the CyberSafe Learning Hub, enabling it to meet user needs and add value for students as they navigate cyber security and digital safety.

3.5.1.1 Questionnaire Analysis

A questionnaire was used as a quantitative data collection method through online platform using Google Forms to KTAC students. The survey instrument had 20 close-ended questions on a range of issues organized into four thematic categories that encompassed demographics, awareness about cybersecurity, preferences of learning style and system requirement. The survey was released over the period of 13th—27th October 2025 and resulted in a total of 73 valid responses.

The questionnaire served two goals. First, it sought to confirm that the problem exists through an assessment of students' cybersecurity awareness and behaviours. Findings indicated that students generally had weak cybersecurity awareness and habits, especially concerning password management and phishing prevention activities. This supported our belief in a learning solution such as CyberSafe Learning Hub. Second, this questionnaire aimed to identify system and design requirements such as students' preferred learning styles, motivational factors related to gamification, and essential non-functional aspects such as usability, security, and system performance.

Quantitative results from this pre-development phase more broadly informed specific design requirements for the CyberSafe Learning Hub that were relevant with identified gaps in awareness, and fulfils user's needs.

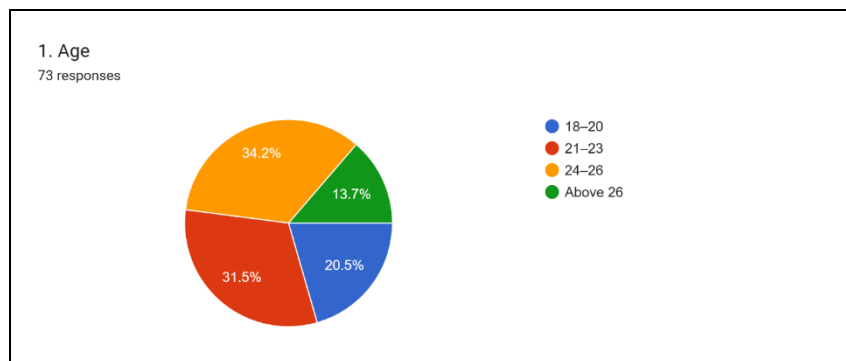


Figure 3.10: Age of Respondents

The age distribution of respondents is displayed in Figure 3.10. Majority are 24–26 years old (34.2%) followed by 21–23 years old (31.5%), 18–20 years old (20.5%) and >26 years of age (13.7%). This suggests that most respondents fall into the average college student age group, which is reasonable to explore the cybersecurity knowledge for college students.

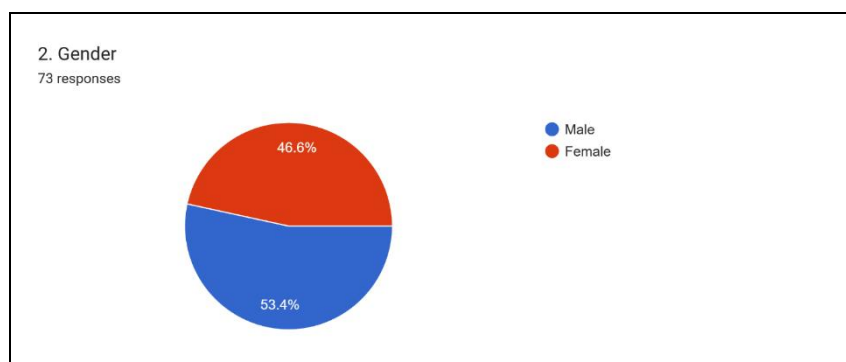


Figure 3.11: Gender of Respondents

Figure 3.11 shows the relative proportion of male and female respondents, with a higher level of males at 53.4% than females at 46.6%. The almost equal gender split ensures that both the male and female reactions are fairly represented, so the results aren't slanted towards one or the other.

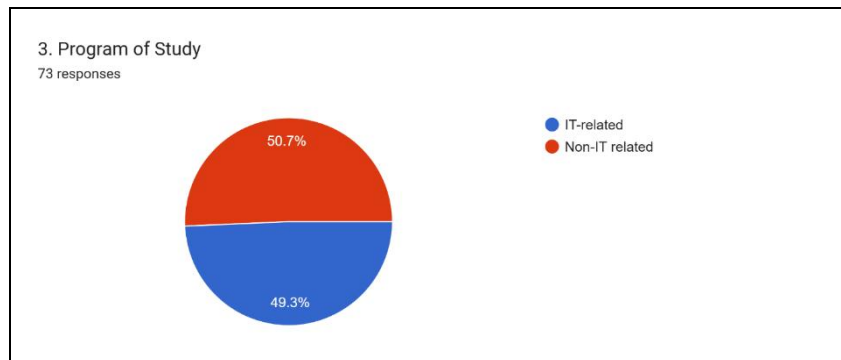


Figure 3.12: Program of Study

The respondents' program of study is illustrated in Figure 3.12 with 49.3% of the participants are studying IT-related, while the remaining 50.7% from another than IT-related field. It is based on a well-balanced proportion that the awareness of cybersecurity is important in all fields, which has inspired the project to engage IT and non-IT students as the target audience for such a platform.

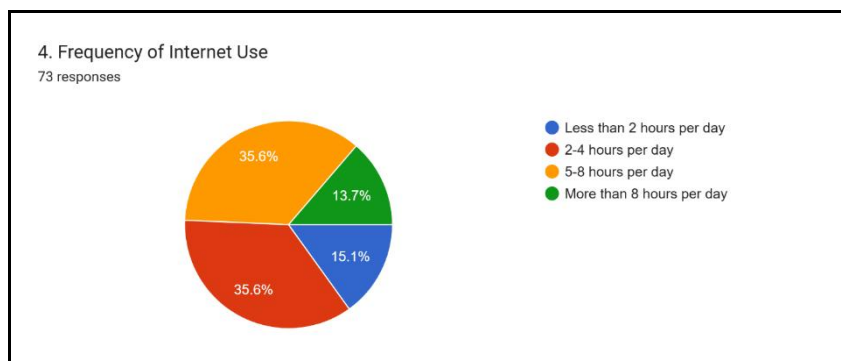


Figure 3.13: Frequency of Internet Use

Figure 3.13 shows the extent to which students used Internet. In terms of daily internet usage, 35.6% reported using the computer for 2-4 hours, another 35.6% used it for 5-8 hours, and 15.1% used it for less than two hours and further use by only 13.7%, who spent over eight hours per day on the computer. The results of these data suggest that internet users who participated in the study are highly at risk to be exposed to cyberthreats and the concept of awareness ceaselessly enforce their importance.

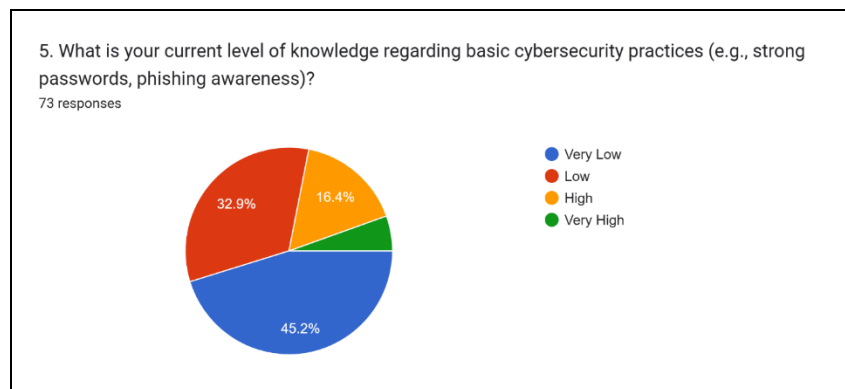


Figure 3.14: Level of Cybersecurity Knowledge

Figure 3.14 illustrates the current level of awareness amongst respondents in basic cybersecurity, like strong passwords and phishing. The findings show that 45.2% rated their knowledge as very low, 32.9% low, 16.4% high, and 5.5% met the 'very high' threshold. It reveals that majority of students are less knowledgeable on cybersecurity and underscores the need for educational interventions in order to make them well informed about online safety.

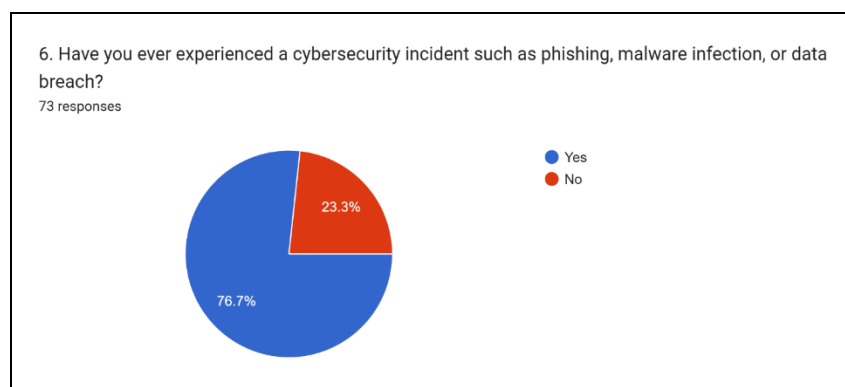


Figure 3.15: Experience of Cybersecurity Incidents

Figure 3.15 shows whether an individual has fallen victim to a cyber-attack such as phishing, malware, or hack. The overall prevalence of such incidents was 76.7% and 23.3% did not experienced them. This suggest that students are consistently under threat of cyber security which highlights the importance of developing awareness and safe online behaviour practices.

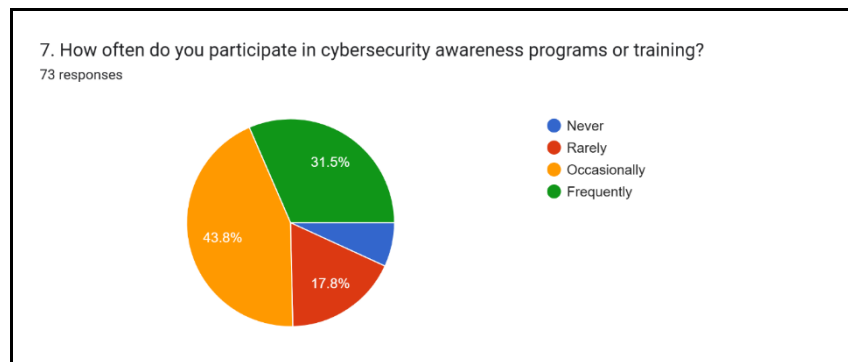


Figure 3.16: Participation in Cybersecurity Awareness Programs

Figure 3.16 displays the frequency of respondents attending cybersecurity awareness programs/training. Results show as 43.8% attend such programs occasionally, 31.5% frequently, 17.8% rarely, and 6.8% never. This implies that some students have been exposed to cyber security learning but the majority of them do not regularly engage in awareness programs.

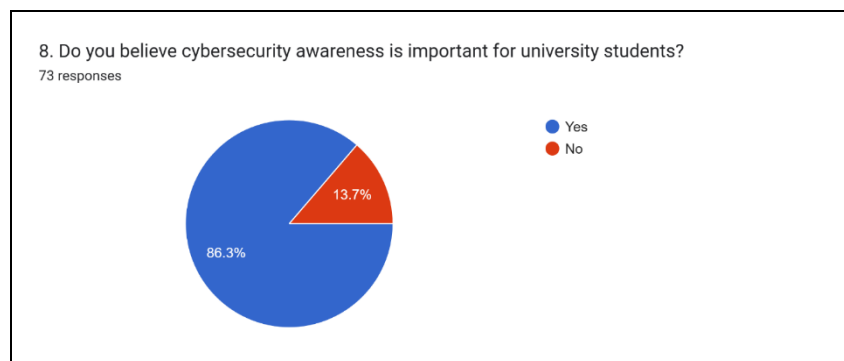


Figure 3.17: Importance of Cybersecurity Awareness

Figure 3.17 displays the answers of the survey as whether cybersecurity awareness is important for university students or not. Most, 86.3%, replied Yes and the rest, 13.7%, said No. This substantial concordance indicates that students understand the importance of cyber-security awareness as an integral part of their digital education.

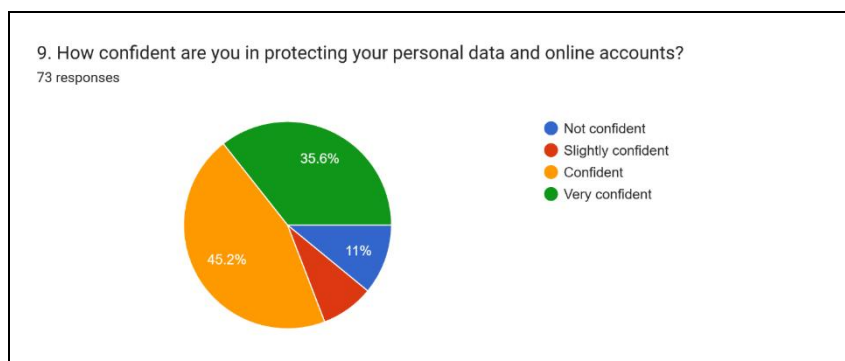


Figure 3.18: Confidence in Protecting Personal Data

Figure 3.18 shows respondents' confidence in the security of their personal data and online accounts. The numbers are 45.2% confident, 35.6% very confident, while 11% of respondents are not confident, and another 8.2% are only slightly confident. These findings suggest that the vast majority of college students exhibit confidence but may have an overestimation of their ability to defend themselves from threats without any formal training in cybersecurity.

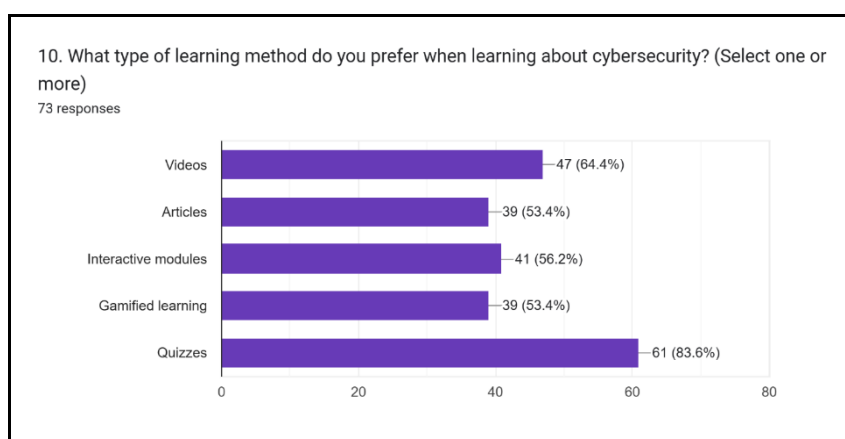


Figure 3.19: Preferred Learning Methods for Cybersecurity

The learning type preferred by the responses of what learning is there for cybersecurity are illustrated in Figure 3.19. Quizzes were the most preferred teaching tool (83.6%), and this was followed by videos (64.4%), interactive modules (56.2%), articles (53.4%) and gamified learning (51%). This indicates that learners prefer interactive and participatory learning, which justifies the integration of gamified and quiz content into the CyberSafe Learning Hub.



Figure 3.20: Frequency of Applying Safe Online Practices

Figure 3.20 shows how often respondents apply safe online practices. The results indicate that 37% stated they always follow safe practices, 35.6% said often, 11% said sometimes, 12.3% said rarely, and 4.1% never apply them. This suggests that while a majority of students consistently maintain online safety, a small group still neglects basic security habits, indicating a need for continuous reinforcement of safe online behaviors.

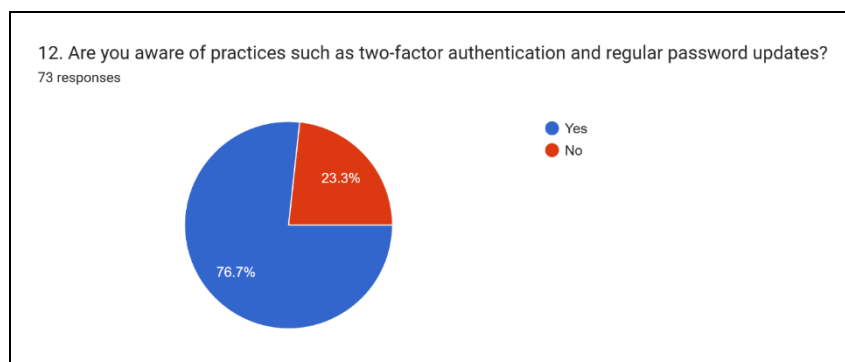


Figure 3.21: Awareness of Security Practices

Figure 3.21 displays respondents' familiarity with cybersecurity activities such as using two-factor authentication or regularly updating their passwords. It was responded Yes by 76.7% and No by 23.3%. Thus, this shows that the majority of students know of these practices but almost one-fourth still do not know about them.

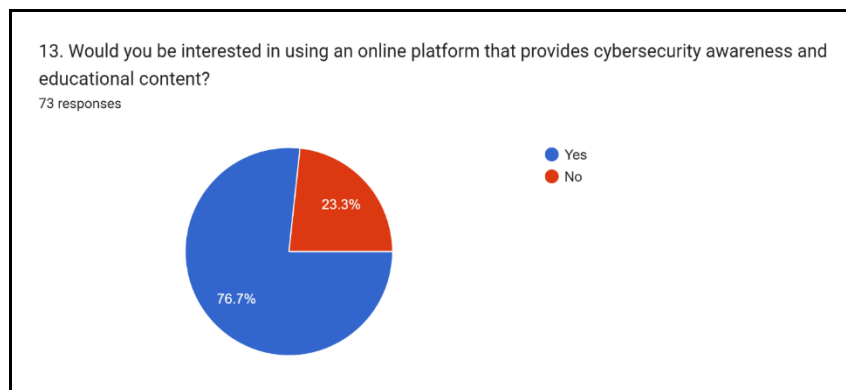


Figure 3.22: Interest in Using Cybersecurity Learning Platforms

Figure 3.22 demonstrates that participants are interested in using an online tool which helps providing them knowledge about cybersecurity related issues as well as education in this regard. There appear to be 76.7% that are interested and 23.3% not interested according to the data. This would indicate a great degree of acceptance and willingness on the part of students to work with a learning platform such as the CyberSafe Learning Hub.

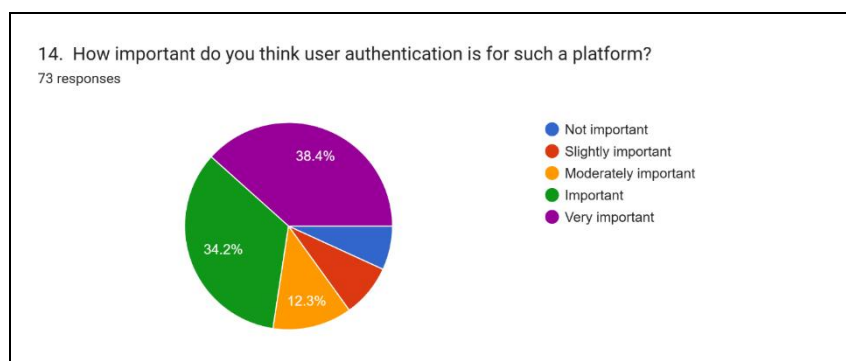


Figure 3.23: Importance of User Authentication

The significance of user authentication on a cybersecurity platform is depicted in Figure 3.23. Results show that 38.4%, rated it very important, while 34.2% important, and other rated as moderately important (12.3%) slightly important (8.2%), not important (6.8%). That would suggest that most are aware of the value of secure access and identity validation.

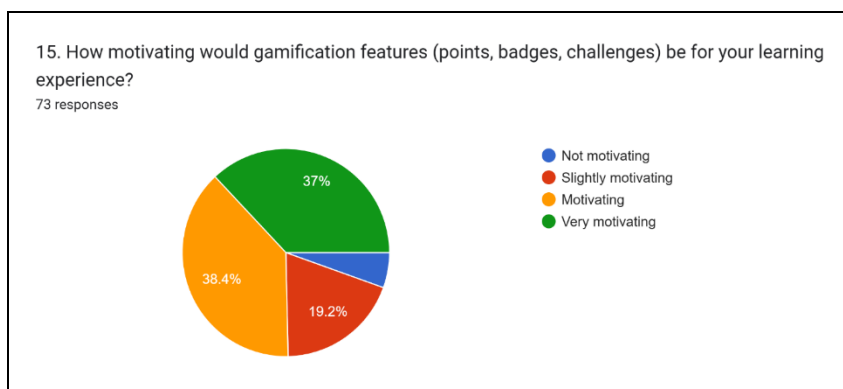


Figure 3.24: Motivation Through Gamification

Figure 3.24 shows how participants perceived gamification elements like points, badges, and challenges as motivating them. The results have shown that 37% find them very motivating, 38.4% motivating, 19.2% slightly motivating and only 5.4% not motivating. These results imply that integrating the game design elements can greatly motivate learner and make them enjoy learning about cybersecurity.

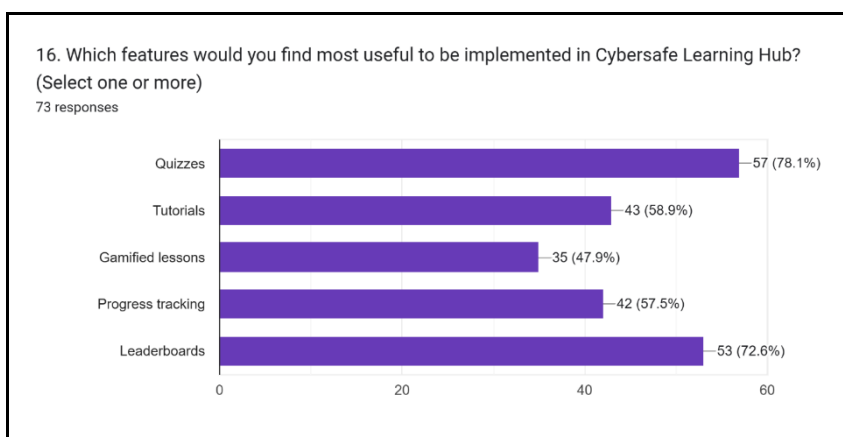


Figure 3.25: Preferred Features in the CyberSafe Learning Hub

Figure 3.25 shows what respondents consider to be the most valuable options from which they can choose for inclusion in a CyberSafe Learner Hub. The findings show that quizzes (78.1%) are the highest-demanded feature, and they are followed by leaderboards (72.6%), tutorials (58.9%), progress tracking tools (57.5%), and gamified lessons (47.9%). It means that students prefer interactive and competitive elements in their learning.

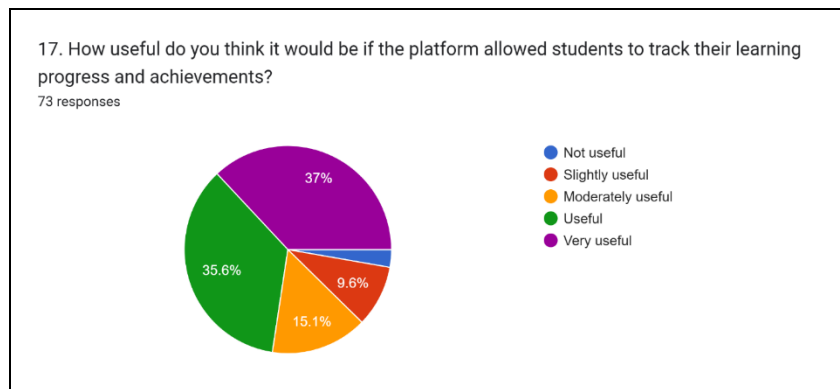


Figure 3.26: Usefulness of Progress Tracking

Figure 3.26 How useful students thought it would be to track learning progress and achievements using the platform. The results indicate that 37% rated it as very useful, 35.6% as useful, 15.1% as somewhat useful, and 9.6%, slightly useful; with only 2.7 % rating it as not useful. This indicates robust support for monitoring progress features in which learners can track improvement.

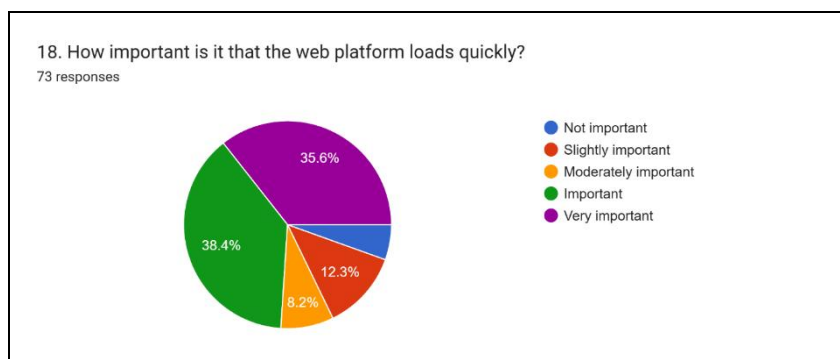


Figure 3.27: Importance of Platform Loading Speed

Figure 3.27 shows the importance of web platform loading speed according to respondents. The figures indicate that 38.4% valued it as important, 35.6% very important, 12.3% moderate importance, 8.2% low importance and 5.5% not important to their studies respectively. This illustrates that the system performance is a basic user expectation.

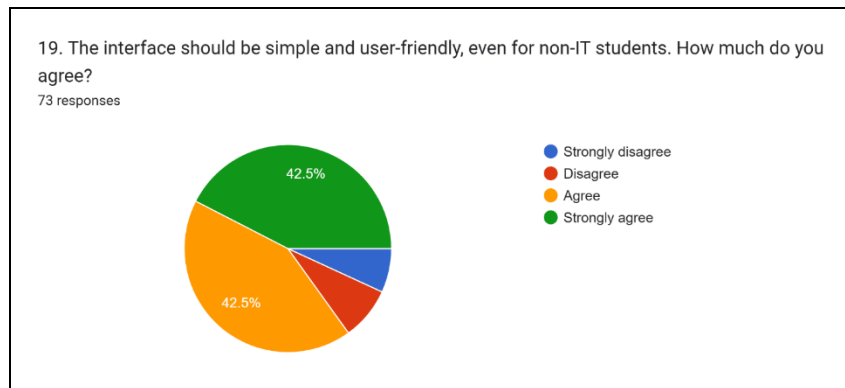


Figure 3.28: System Usability and Interface Design

Figure 3.28 exhibits the agreement among students with respect to an interface that is simple and user-friendly. Strongly agree and agree was 42.5% each, disagree was 8.2%, strongly disagree, 6.8%. This validates the fact that ease of use is important for non-IT students.

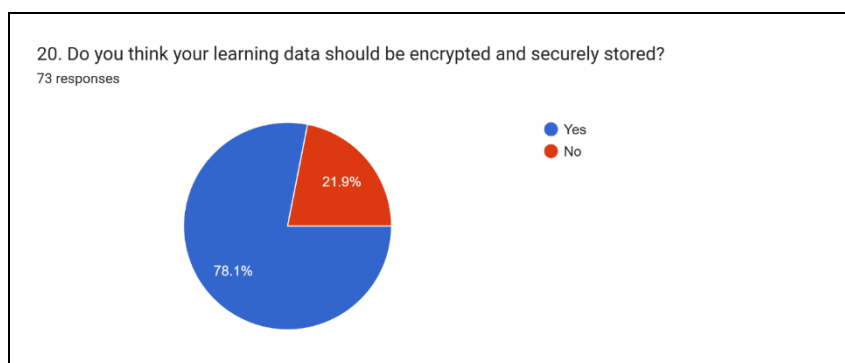


Figure 3.29: Importance of Data Security and Encryption

Figure 3.29 demonstrates the attitudes of students on data security, in example, whether learning data should be encrypted and stored securely. The agreement was 78.1% with disagreement of 21.9%. This also highlighted the need to encrypt and securely manage user data in the CyberSafe Learning Hub.

3.5.1.2 Interview Analysis

Interview with Mr. Syaheedullah Bin Yahya, lecturer of Diploma in Information Technology programme at KTAC on the 9th October 2025. He was chosen for this interview because of his professional knowledge in the information technology field and mentoring students about digital protection. This interview was aimed at collecting expert opinions on the significance of cyber security awareness on college students, and obtaining recommendations on the CyberSafe Learning Hub platform. His insights have been able to give us valuable inputs in terms of current issues we faced, effective learning approach and practical recommendation that could come into places in context of cybersecurity being taught at higher institutions.



Figure 3.30: Interview session with Mr.Syaheedullah

Table 3.4: Analysis of Interview Questions

Question	Answer	Analysis
In your opinion, how important is cybersecurity awareness for college students?	• Very important in today's digital era. • Many students lack awareness of online risks.	Emphasizes the growing need for continuous cybersecurity education among students who are active internet users.
What are the most common cybersecurity challenges or issues you observe among students?	• Weak or reused passwords. • Careless information sharing. • Clicking on suspicious links/emails. • Failure to update devices.	Highlights behavioral issues as the main source of vulnerabilities, stressing the need for habit-based awareness programs.
Have you encountered any cases where students were affected due to a lack of cybersecurity knowledge?	• Yes, cases of phishing and account takeovers. • Students lost access to email or social media.	Demonstrates the real-world consequences of low cybersecurity literacy, supporting the case for more preventive education.
How effective do you think the university's current cybersecurity awareness efforts are?	• Efforts exist but limited. • Campaigns conducted once or twice per semester. • Need for continuous engagement.	Suggests that awareness efforts should shift from periodic campaigns to ongoing engagement for lasting impact.
What learning methods do you find most effective in teaching students about cybersecurity?	• Practical, hands-on activities. • Simulations and real-world exercises. • Less theory, more application.	Endorses experiential learning and simulation-based training as the most effective teaching approach.

Question	Answer	Analysis
Do you think a platform such as the CyberSafe Learning Hub could improve students' understanding of cybersecurity?	• Promising idea if similar to TryHackMe. • Encourages active, self-paced learning. • Needs evaluation after implementation.	Supports gamified, interactive learning for engagement and practical understanding of cybersecurity.
What specific features or functions would you recommend to make the platform more engaging for students?	• Gamification (badges, levels, leaderboards). • Visually appealing interface. • Interactive and varied quizzes.	Recommends motivational elements and user-friendly design to improve engagement and knowledge retention.
From an administrative perspective, how important is Role-Based Access Control (RBAC) in managing lecturer and student permissions within the system?	• Very important for access management. • Ensures proper authorization based on user roles. • Prevents data misuse.	Reinforces the need for structured access control to safeguard data and maintain system integrity.
Should cybersecurity awareness be integrated across all academic disciplines, or only within IT-related courses?	• Should be across all programs. • Every student handle digital data. • Not limited to IT students.	Advocates for inclusive cybersecurity education applicable to all fields, not just technology.
What advice would you give to ensure the CyberSafe Learning Hub supports learning and long-term awareness?	• Update modules regularly. • Use real-world examples. • Involve lecturers and integrate with coursework.	Suggests that platform sustainability depends on consistent updates, curriculum integration, and lecturer participation.

3.5.2 Use Case Model



Figure 3.31: Use Case Diagram for CyberSafe Learning Hub

The Use Case Model in Figure 3.31 illustrates the interactions between the CyberSafe Learning Hub system and its two primary actors: the Student and the Administrator (Lecturer). It outlines the key operations available to each actor, defines the boundaries of the system, and serves as a reference for understanding how each user type engages with the platform to fulfil their respective goals.

The Student is the primary end user of the system. A student may register for a new account using their email and password or sign in through Google OAuth 2.0. Upon logging in for the first time, the student is guided through a brief onboarding process before being directed to the Student Dashboard. From the dashboard, the student can browse available cybersecurity learning modules organised by category, view individual lessons, and mark lessons as complete to track their progress. Upon completing a lesson, the student may attempt the associated quiz.

The quiz system enforces an 85% passing threshold, and students who do not meet this requirement may retake the quiz. During a quiz, the student may interact with the built-in AI Chatbot, which provides concept explanations without revealing direct answers. Upon passing all quizzes within a module, the student is automatically awarded a module badge. When all modules within a category are completed, the system generates and issues a downloadable PDF certificate. The student may also view the Leaderboard, which ranks all students based on their performance scores, encouraging healthy competition and sustained engagement.

The Administrator is responsible for managing all platform content and monitoring student activity. Although the administrator uses the same login entry point as the student, the system detects their role and redirects them to the Admin Dashboard upon authentication. From the admin side, the administrator can create, edit, and delete categories, modules, lessons, and lesson content blocks, as well as manage quizzes and their associated questions and answers. The administrator can also manage registered user accounts, including updating roles and removing users from the system. Through the Analytics module, the administrator can monitor individual student performance, view quiz attempt histories, and track overall platform progress. Additionally, the administrator may send in-platform notifications to individual students or broadcast announcements to all students.

The Use Case Model clearly distinguishes the roles and responsibilities of both actors while highlighting their shared entry point through the authentication process. It provides a structured view of the system's functional scope and confirms that the CyberSafe Learning Hub is designed to support both effective content delivery for students and efficient platform management for administrators.

3.5.3 Flowchart

3.5.3.1 Student Flowchart

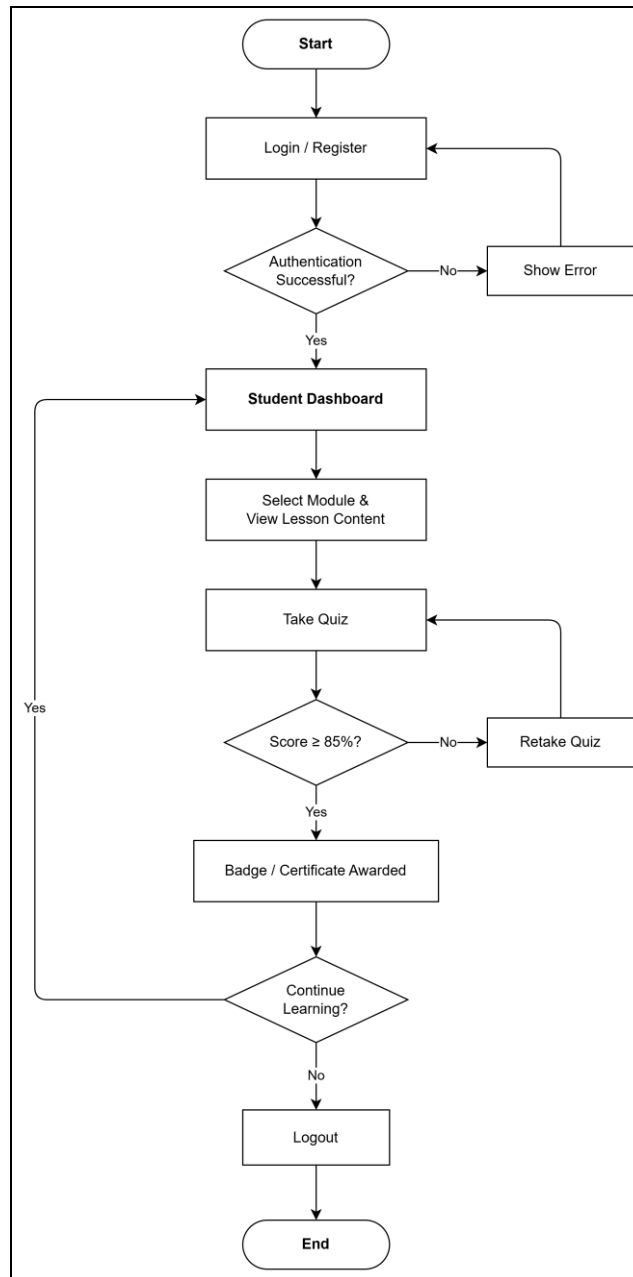


Figure 3.32: User (Student) Flowchart of CyberSafe Learning Hub

Figure 3.32 illustrates the process a student goes through when using the CyberSafe Learning Hub. The flow begins when the student accesses the system and chooses to either register a new account or log in using their email and password or Google OAuth 2.0. If authentication fails, an error message is displayed and the student is prompted to try again. Upon successful authentication, the student is directed to the Student Dashboard, where they can browse and select a cybersecurity learning module. The student proceeds to view the lesson content and, upon completion, attempts the quiz associated with the lesson. The system evaluates the submission and checks whether the student has achieved a score of 85% or above. If the score is below the passing threshold, the

student may retake the quiz. Once the quiz is passed, the system automatically awards a badge or certificate based on the student's progress. The student is then prompted to continue learning or log out. If they choose to continue, they are redirected to the dashboard to select the next module. The flow concludes when the student logs out of the system.

3.5.3.2 Admin Flowchart

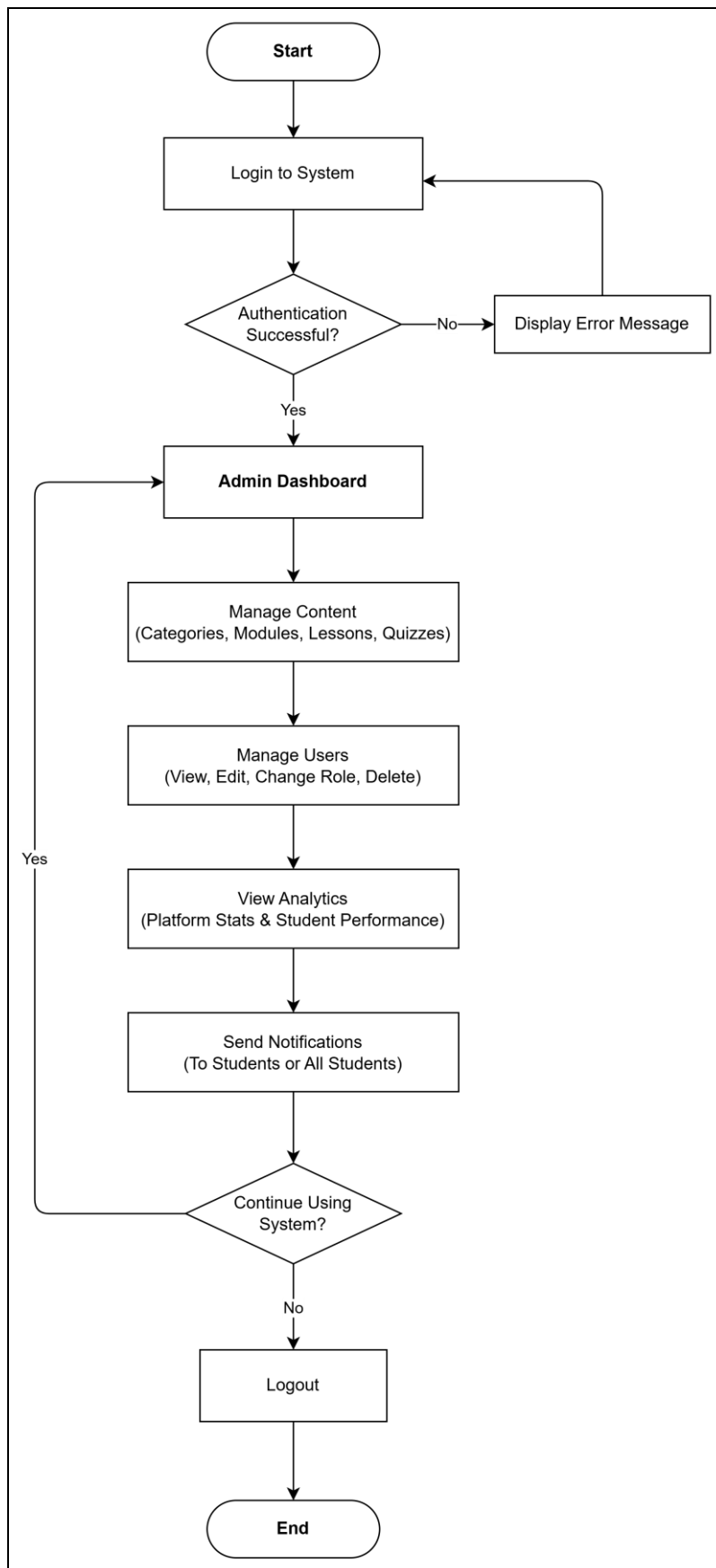


Figure 3.33: User (Administrator/Lecturer) Flowchart of CyberSafe Learning Hub

Figure 3.33 depicts the process an administrator goes through when using the CyberSafe Learning Hub. The flow begins when the administrator navigates to the login page and enters their credentials. If authentication fails, an error message is displayed and the administrator is prompted to try again. Upon successful authentication, the administrator is directed to the Admin Dashboard, which provides an overview of platform statistics and activity. From the dashboard, the administrator can perform a series of management tasks: managing content such as categories, modules, lessons, and quizzes; managing user accounts including editing roles and removing users; viewing analytics to monitor student performance and progress; and sending notifications to individual students or all students on the platform. After completing the required tasks, the administrator is asked whether they wish to continue using the system. If yes, they are returned to the Admin Dashboard. If no, the administrator logs out and the process ends.

3.6 Conclusion

In summary, this chapter explained the process used to create CyberSafe Learning Hub as a learning environment for increasing cybersecurity awareness and literacy in college students. The chapter explained how Agile methodology was utilized to enable iterative development, embed user feedback and continuous improvement within the project. Both quantitative and qualitative methods are applied in order to make the system design consistent with real user needs and learning behaviours.

The information from the questionnaires and interviews helped to inform us about what users knew or did not know regarding cybersecurity, the system for learning that they preferred, system expectation and so forth. According to the questionnaire, although students were aware of the importance of cybersecurity, many did not have a realistic appreciation nor did they adopt safe online behaviour to protect themselves. Interview with the lecturer provided insights from an educator's perspective as well confirming the requirement for more structured, interactive and engaging digital learning materials

The synthesis of this evidence informed the design decisions for the system's functional and non-functional requirements such as gamification, user authentication, progress tracking, usability and performance. These needs provided the basis for the consequent project design and development phases.

In conclusion, this chapter presented the methodological platform upon which rests the whole project. By building the system upon empirical evidence and stakeholder co-creation, the CyberSafe Learning Hub is structured to be both technically secure and robust as well as pedagogically effective and engaging in raising awareness among students about cybersecurity.

4 DESIGN & IMPLEMENTATION

4.1 Introduction

This chapter includes the general layout of the proposed system. The design phase is concerned with converting the system requirements into a detailed and structured blue print that is used to develop the system. It discusses the interface design, database design, system architecture, and security issues so that the system can be functional, reliable and secure. The interaction between the system components and their interaction with each other and the way the system is going to interact with the users is depicted using diagrams and design models. The chapter is a source of implementation phase that is discussed in the next chapter.

4.2 Interface Design

The interface design section shows the wireframes that have been designed in the CyberSafe Learning Hub before the implementation. The wireframes are organised into three parts. The first section deals with the general pages which includes the Landing Page, Login Page, and Register Page that is publicly available to all users irrespective of their roles. The second and third sections discuss the role-specific interfaces of the administrators and students respectively.

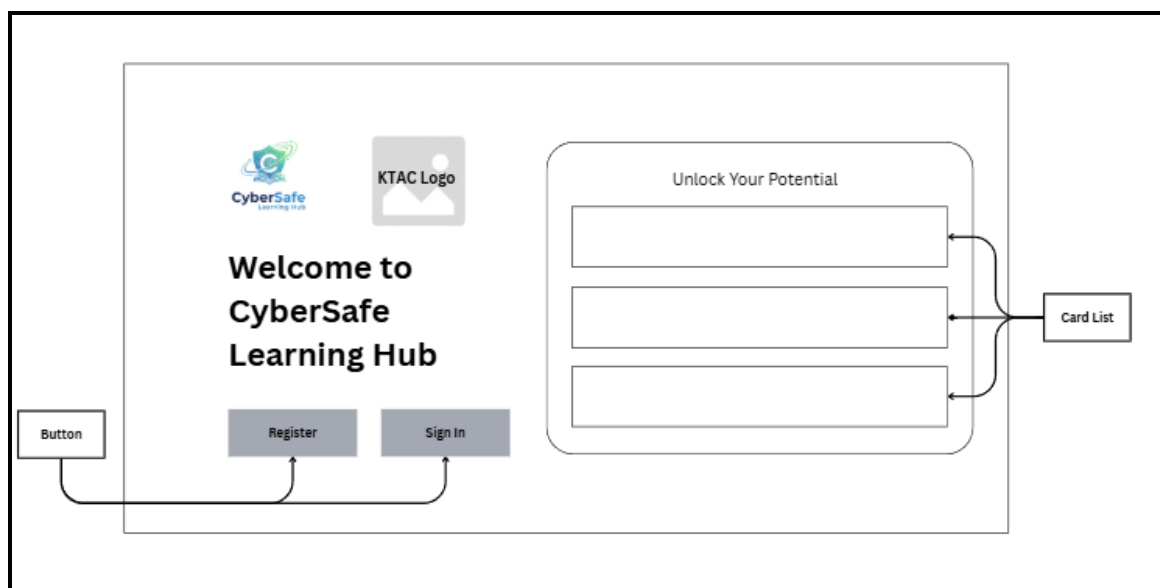


Figure 4.1: Landing Page

Figure 4.1 represents the opening page of the CyberSafe Learning Hub. It is the point of entry into the system and it presents the users with the platform through the CyberSafe logo and a welcome message. The page emphasizes essential elements of the visuals with image cards and offers two major action buttons, Sign In and Register, where users can enter the existing accounts or create a new one.

Figure 4.2: Login Page

The system has a login page as illustrated in figure 4.2. Registered users can use this page to log in by typing in their email address and password. It also offers an alternative of Google sign-in to log in, which makes it convenient and accessible to users.

Figure 4.3: Register Page

Figure 4.3 indicates the registration page whereby new users are able to open an account. The page has textboxes where name, email address, password and password confirmation can be entered. Just like the login page, it has also provided a Google sign-in facility to make the registration process easier.

4.2.1 Admin

The wireframes below represent the administrative side of the CyberSafe Learning Hub. These pages can be accessed by the user only under the administrator role and discuss the fundamental management capabilities of the platform such as dashboards, module and lesson management, quiz management, analytics, and user management.

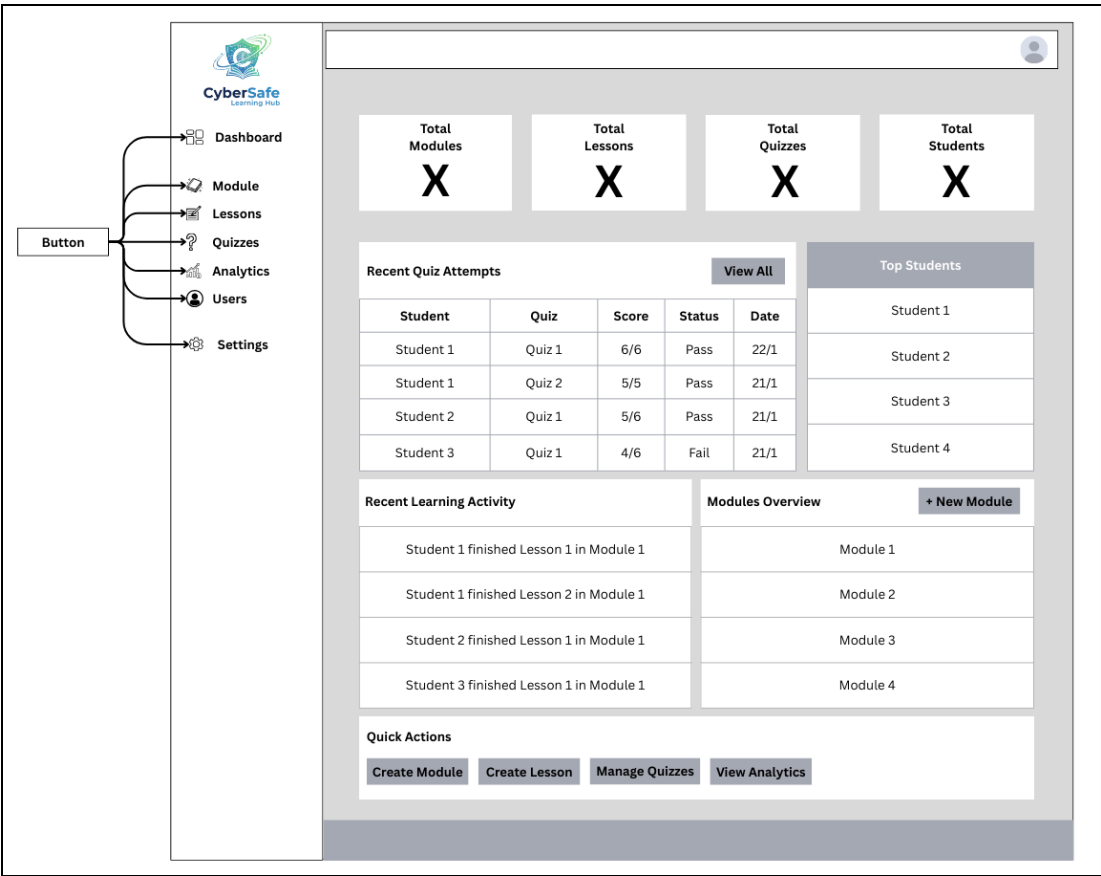


Figure 4.4: Admin Dashboard Page

The page of the admin dashboard as depicted in figure 4.4 gives an overview of the system analytics. It shows major statistics including the total number of students, the total number of quizzes, number of quiz attempts, and average marks. Other features of the dashboard are module completion progress bars, top performers, quick statistics and a recent activity table to assist the administrators in monitoring the general performance of the platform.

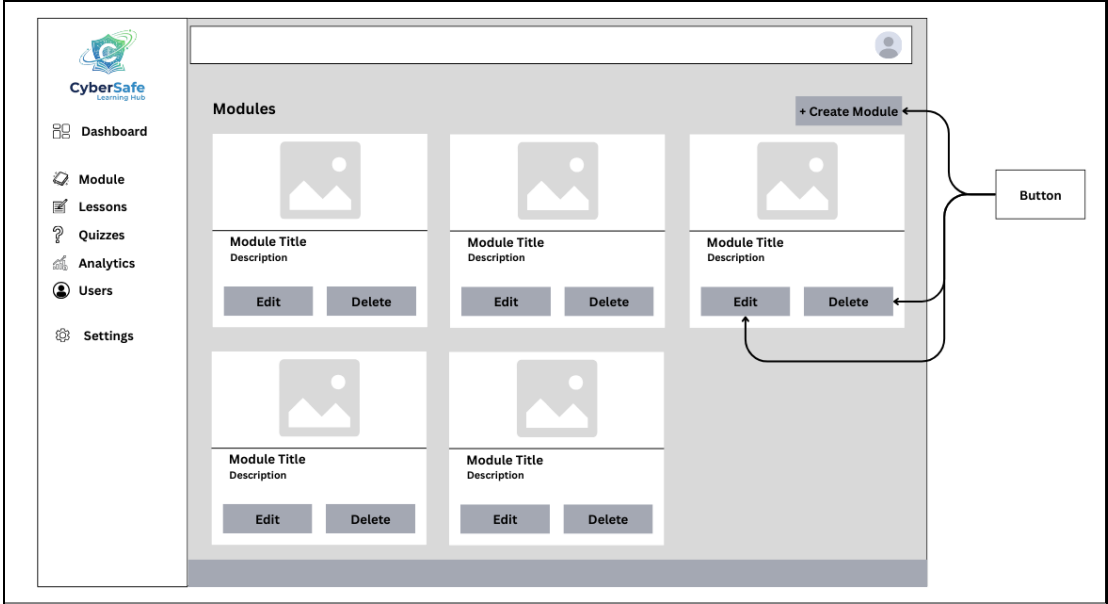


Figure 4.5: Manage Module Page

The figure 4.5 demonstrates the manage module page where administrators can see all the available modules in a card format. All the module cards have a module title, description and image with action buttons to edit or delete the modules. There is also a Create Module button where one can add new modules.

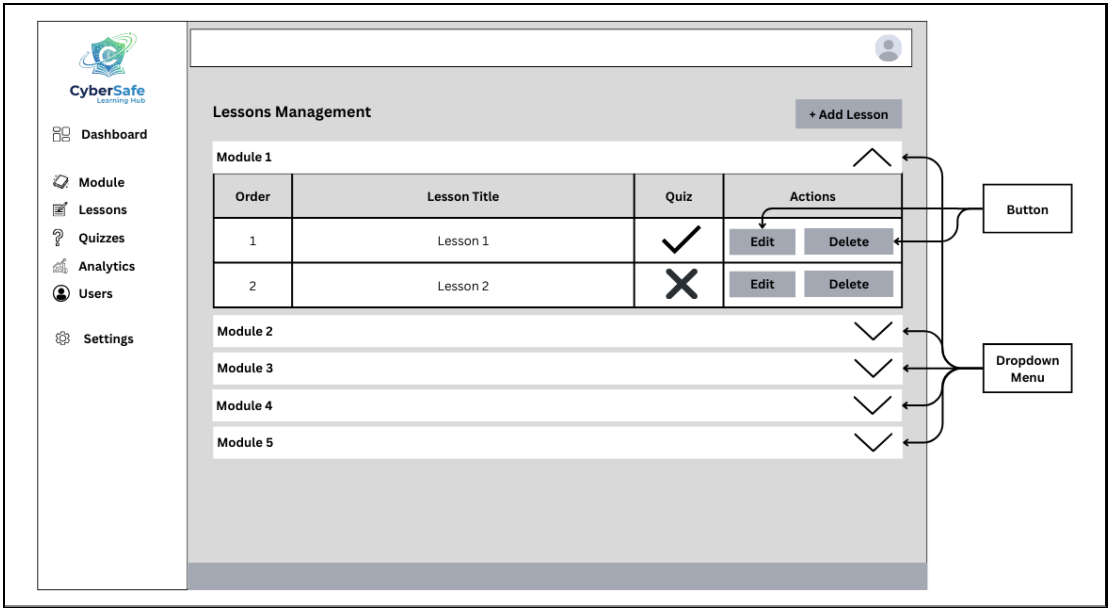


Figure 4.6: Manage Lessons Page

The manage lessons page is depicted in figure 4.6 and it enables the administrators to arrange and manage lessons within every module. The lessons are presented in a tabular format with the lesson order, lesson title, quiz availability, and lesson editing and deletion action buttons. Lesson lists in each module are expanded or collapsed in dropdown menus.

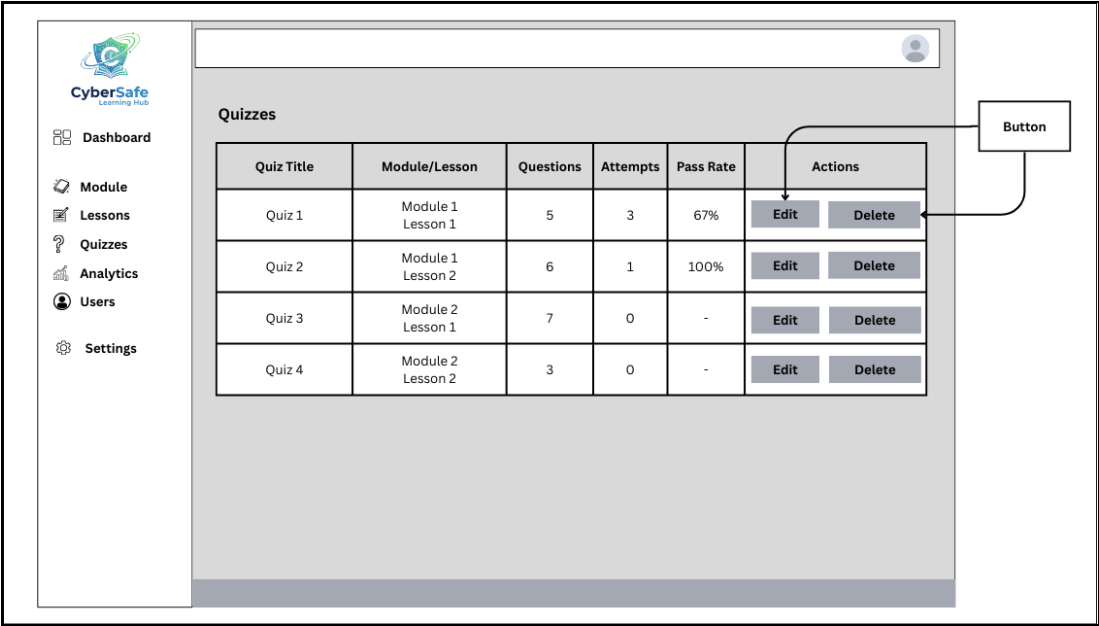


Figure 4.7: Manage Quizzes Page

The manage quizzes page is displayed in figure 4.7. This page shows quizzes in a tabular format with information about quiz title, the module and lesson to which the quiz was associated, the number of questions, attempts, and pass rate. Action buttons allow administrators to edit or delete quizzes easily.

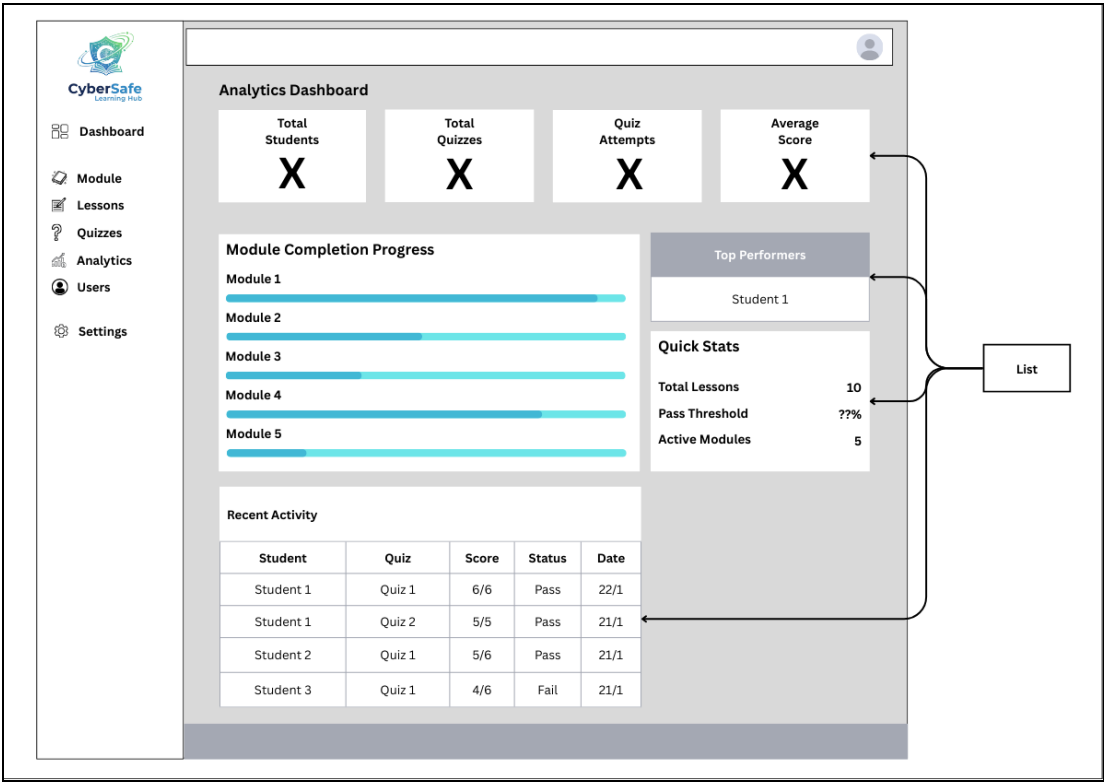


Figure 4.8: Student Analytics Page

The student analytics page is illustrated in figure 4.8 and is dedicated to the analysis of student performance and learning progress. It offers some insights in the form of statistics, performance overviews, and activity tracking, which helps administrators to assess the learning outcomes and determine the areas where improvements can be made.

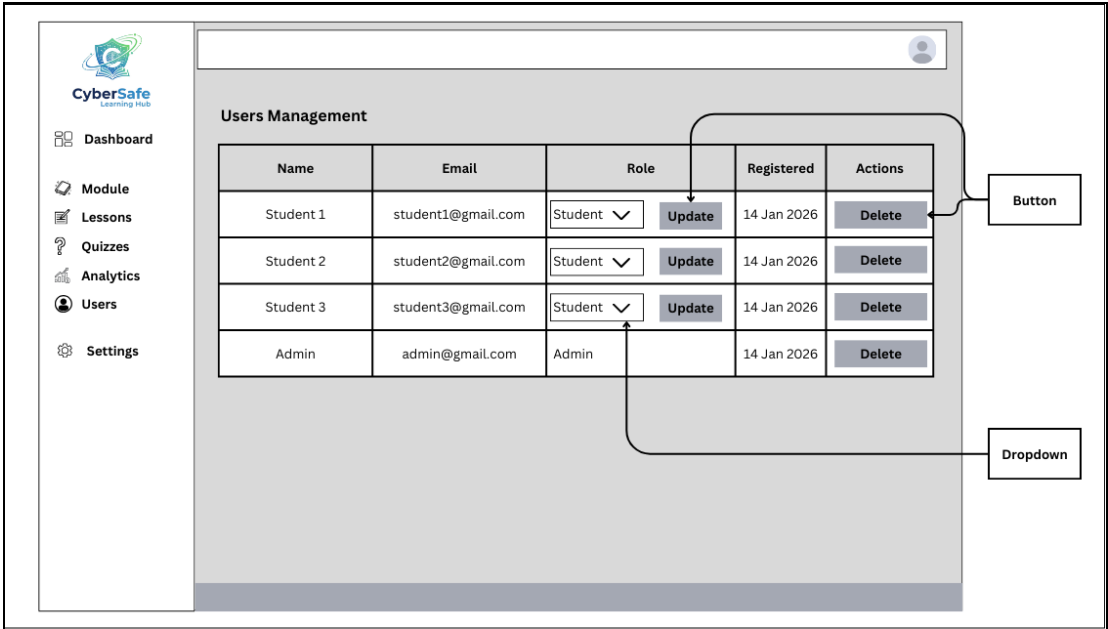


Figure 4.9: Manage Users Page

Figure 4.9 shows the manage users page, where administrators can manage system users. The table has the user names, email addresses, roles, date of registration and actions available. The administrators are able to change the user roles with dropdown menus and delete users with delete buttons which is effective in managing the users and controlling access.

4.2.2 Students

The student-facing pages of the CyberSafe Learning Hub are described by the following wireframes. These pages are available to users who have the student role and discuss the entire learning process, including visiting the dashboard and navigating modules to completing lessons, participating in quizzes, and seeing the results.

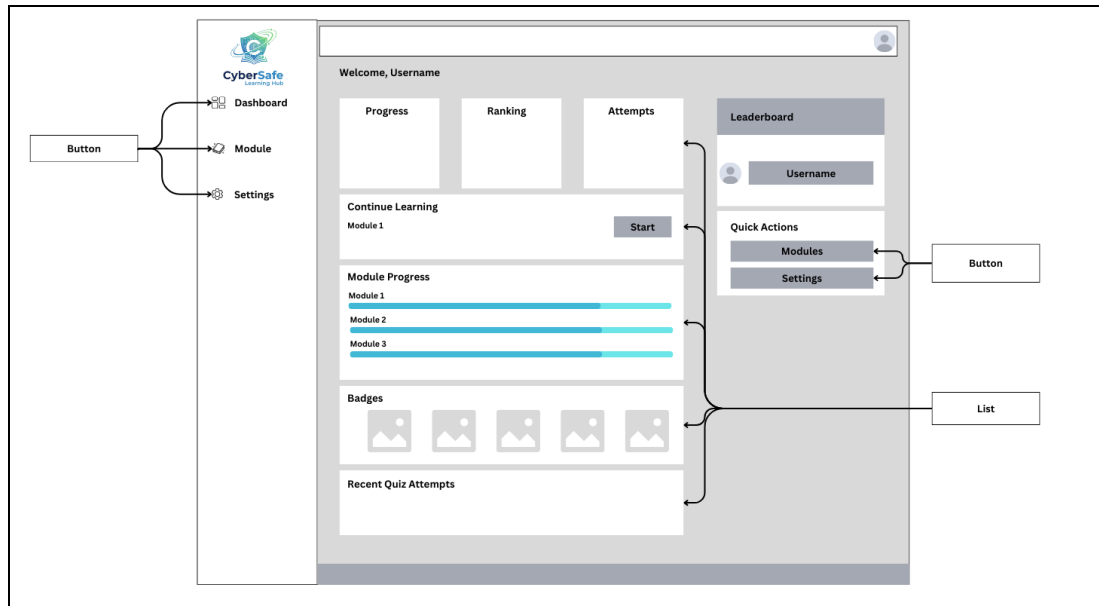


Figure 4.10: Student Dashboard Page

Figure 4.10 shows the student dashboard page of the CyberSafe Learning Hub. This page gives students a review of their progress in learning, such as progress, ranking, and quiz attempts. It also shows progress bars on the modules, badges earned, recent quizzes attempted, and a section of a leaderboard. The quick action buttons enable students to find the modules and settings very easily, which contributes to effective learning management.

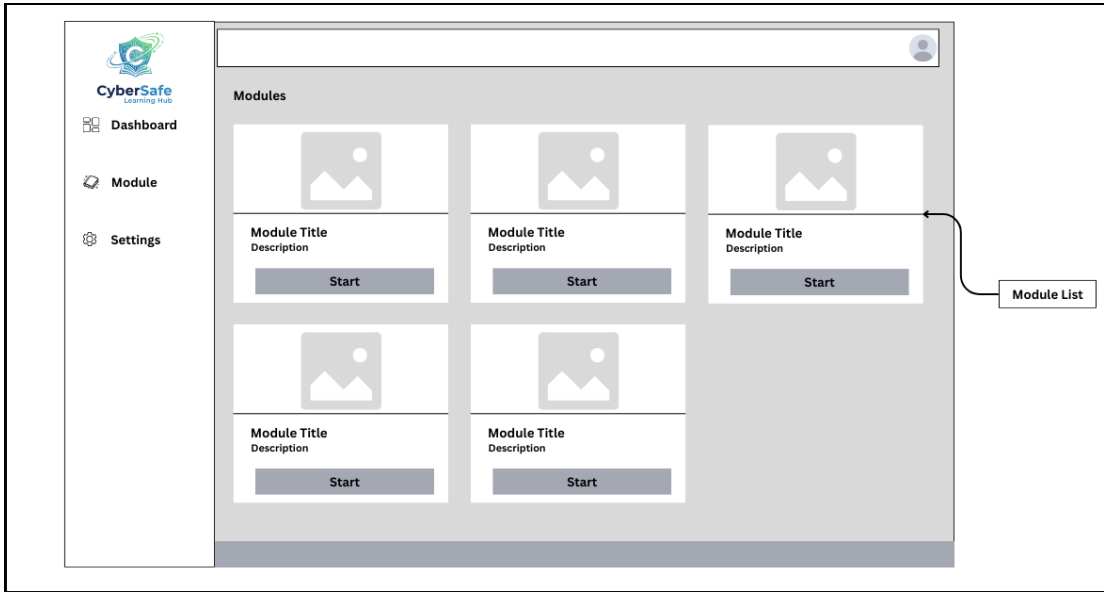


Figure 4.11: View Module Page

Figure 4.11 illustrates the view module page on which students will view all the lessons in a chosen module. The page includes lessons with a start button next to each of them and a module progress indicator, badge earnable section, and a short description of the module to assist students in learning the objectives.

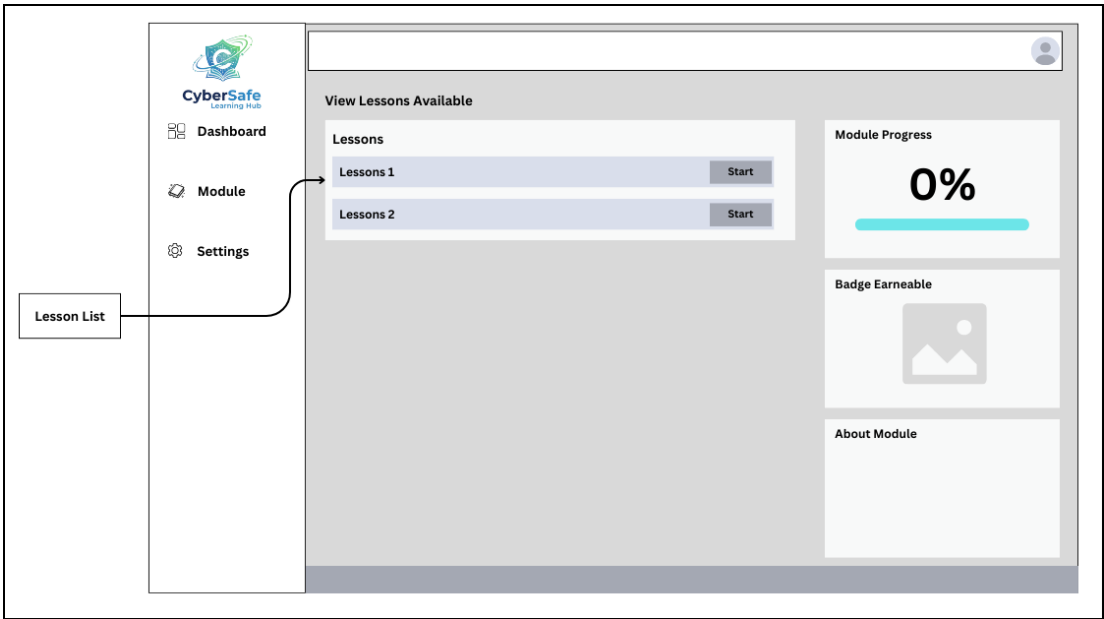


Figure 4.12: View Lesson Page

Figure 4.12 shows the view lesson page, which presents the list of lessons within a module. Students will have the opportunity to choose a lesson to start learning and the page shows the progress of the whole module and the information related to the learning process as well.

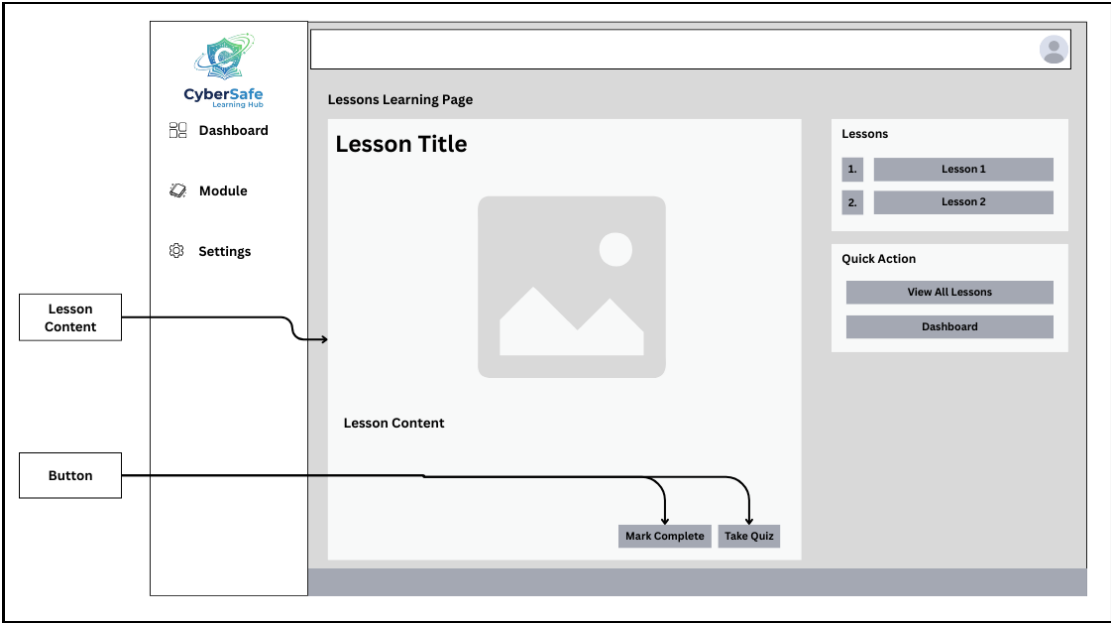


Figure 4.13: Lesson Learning Page

The lesson learning page is demonstrated in Figure 4.13. The lesson title, lesson content, and media related to the lesson are shown on this page to aid in learning. The navigation options enable the student to access other lessons, get back to the dashboard, indicate that the lesson is complete or continue and take a quiz based on the lesson.

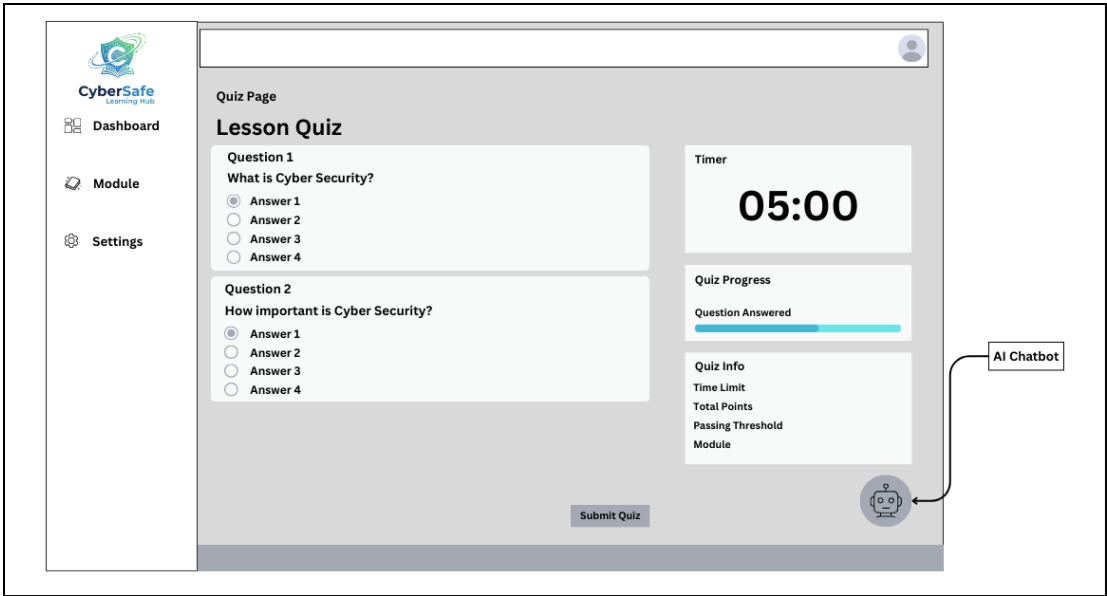


Figure 4.14: Quiz Page

Figure 4.14 represents the quiz page where students are taking quizzes that are associated with lessons. The page has several-choice questions, countdown timer, quiz progress indicator and quiz information like time limit and passing threshold. There is also an AI chatbot that the students can use during the quiz, which improves the learning process.

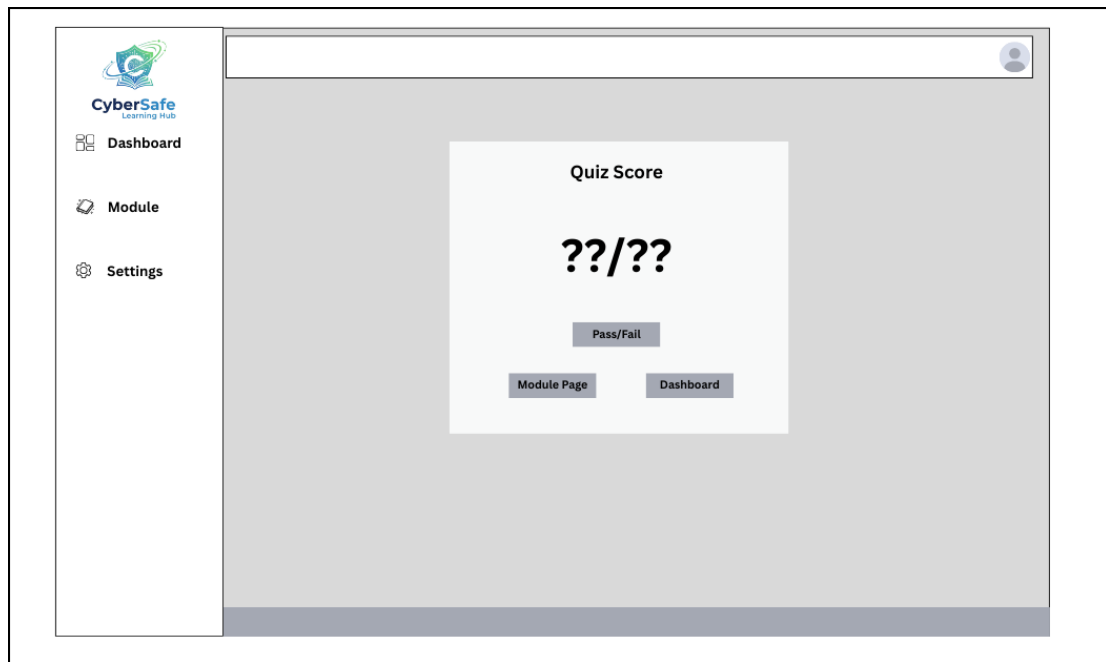


Figure 4.15: Quiz Result Page

The quiz result page can be seen in figure 4.15 and it provides the quiz result and the pass or fail status of the student after submitting the quiz. The page also has navigation buttons that enable the students to go back to the module page or the dashboard so that they can proceed with other learning activities without any problem.

4.2.3 Mobile View (Student)

Since the CyberSafe Learning Hub is to have an interface that is viewable on various devices, the interface that faces the students was also made to suit the mobile screen size. The wireframes below illustrate the change in layout of the main student pages to fit smaller screens so that the smartphones experience can still be consistent and usable.

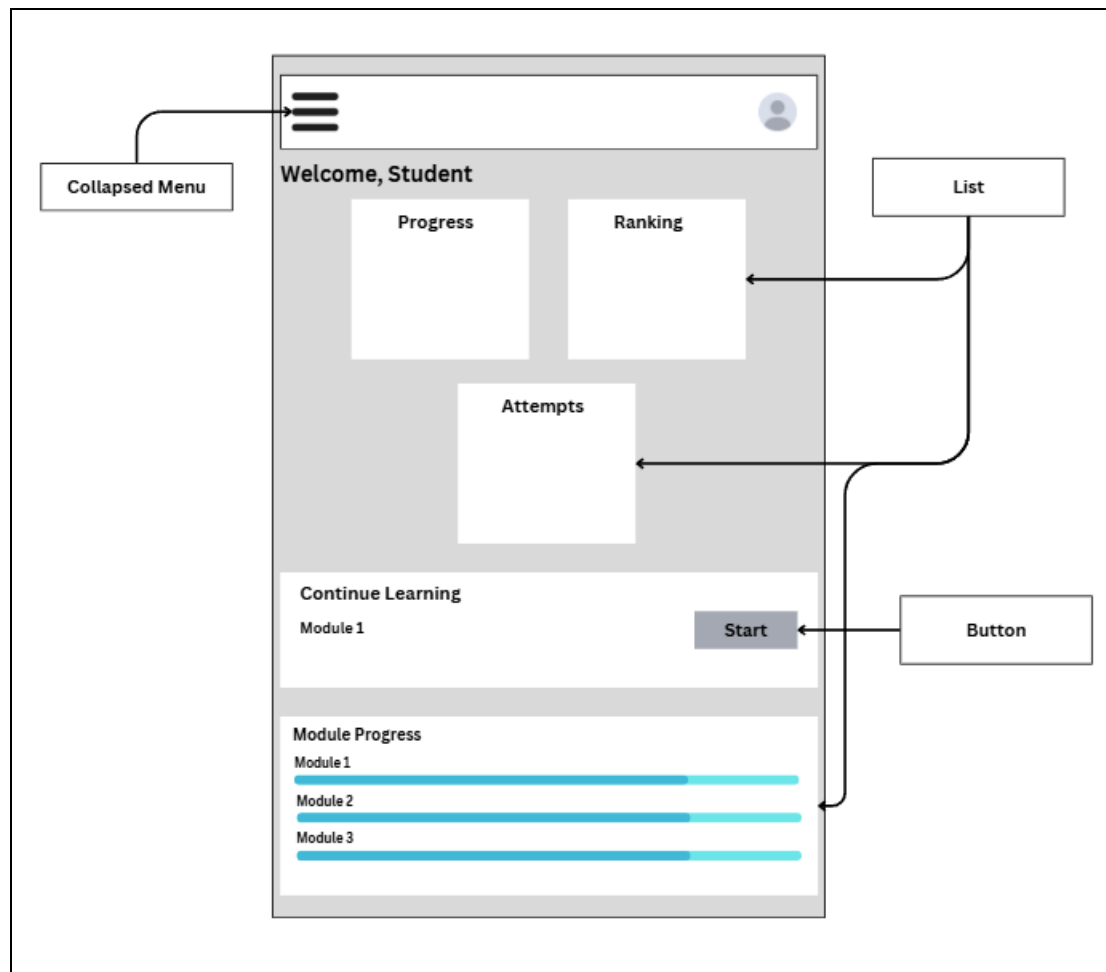


Figure 4.16: Student Dashboard Page (Mobile View)

The mobile view wireframe of the student dashboard page is displayed in Figure 4.16. The design can be customized to use one column format where the progress overviews, the module cards and the quick action buttons are stacked vertically to fit the smaller screen size of the mobile devices.

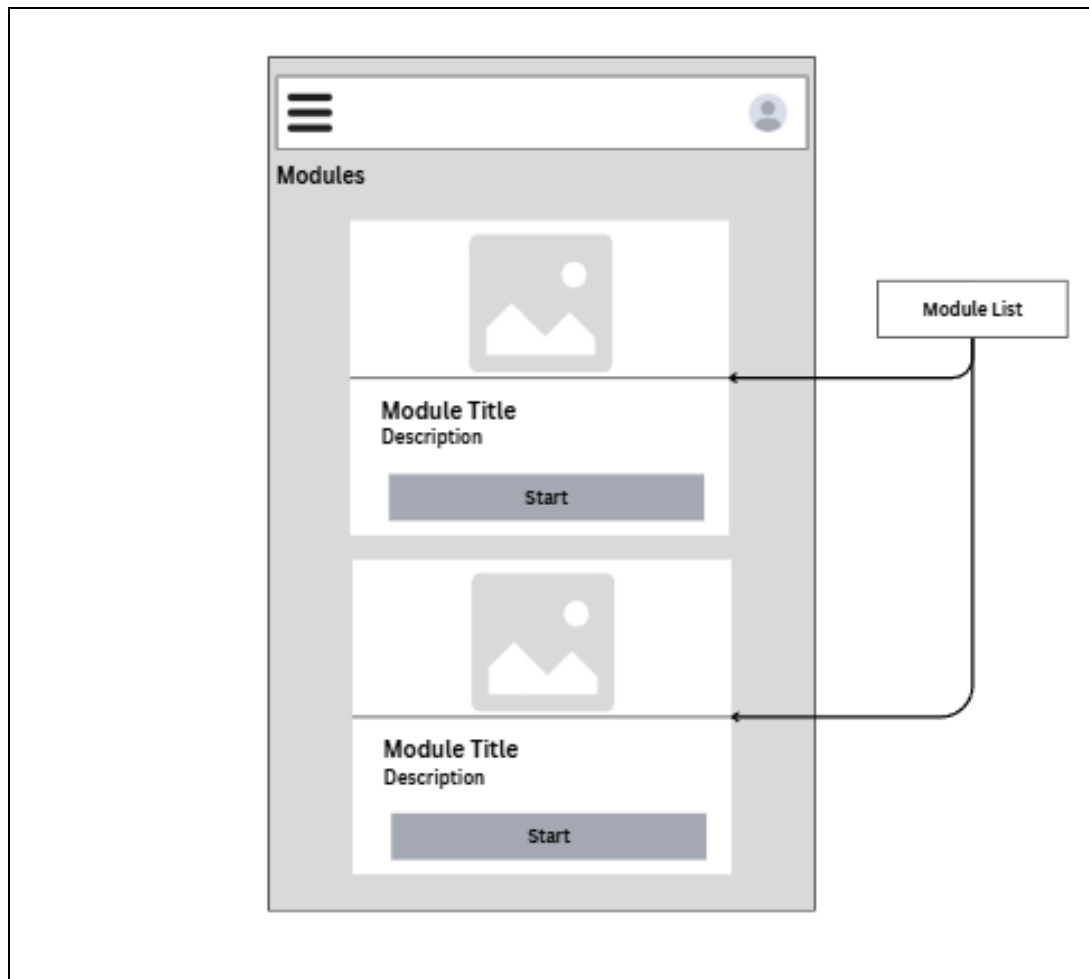


Figure 4.17: View Module Page (Mobile View)

Figure 4.17 shows the mobile view wireframe of the view module page. The module information, lesson list and progress indicator are redesigned into a single column with scrollable list and enable students to navigate content of the module easily in a smaller screen.

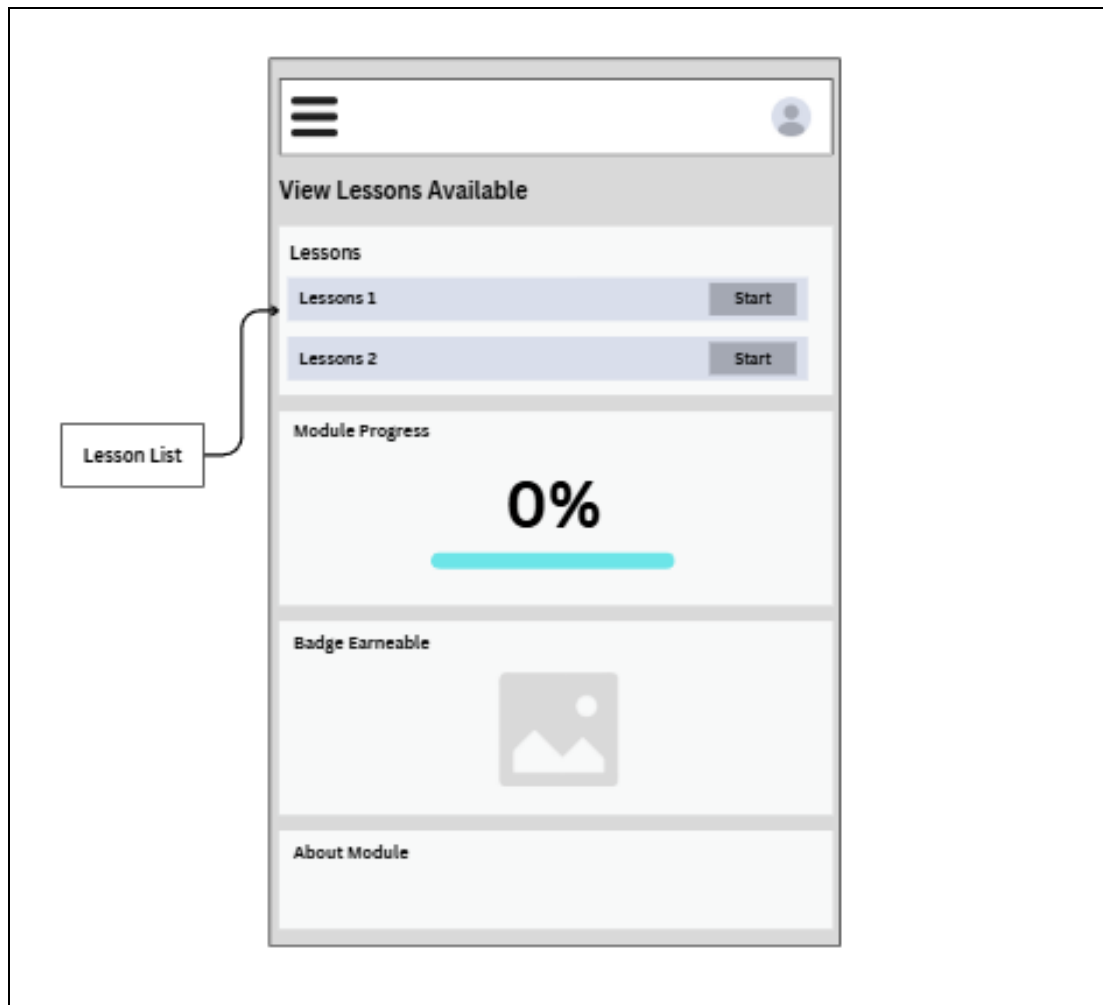


Figure 4.18: View Lesson Page (Mobile View)

The mobile view wireframe of the view lesson page is illustrated in figure 4.18. The list of lessons is presented in the form of a vertically stacked list, and the module progress bar and other information is moved down the list to ensure a clean and readable display on the mobile devices.

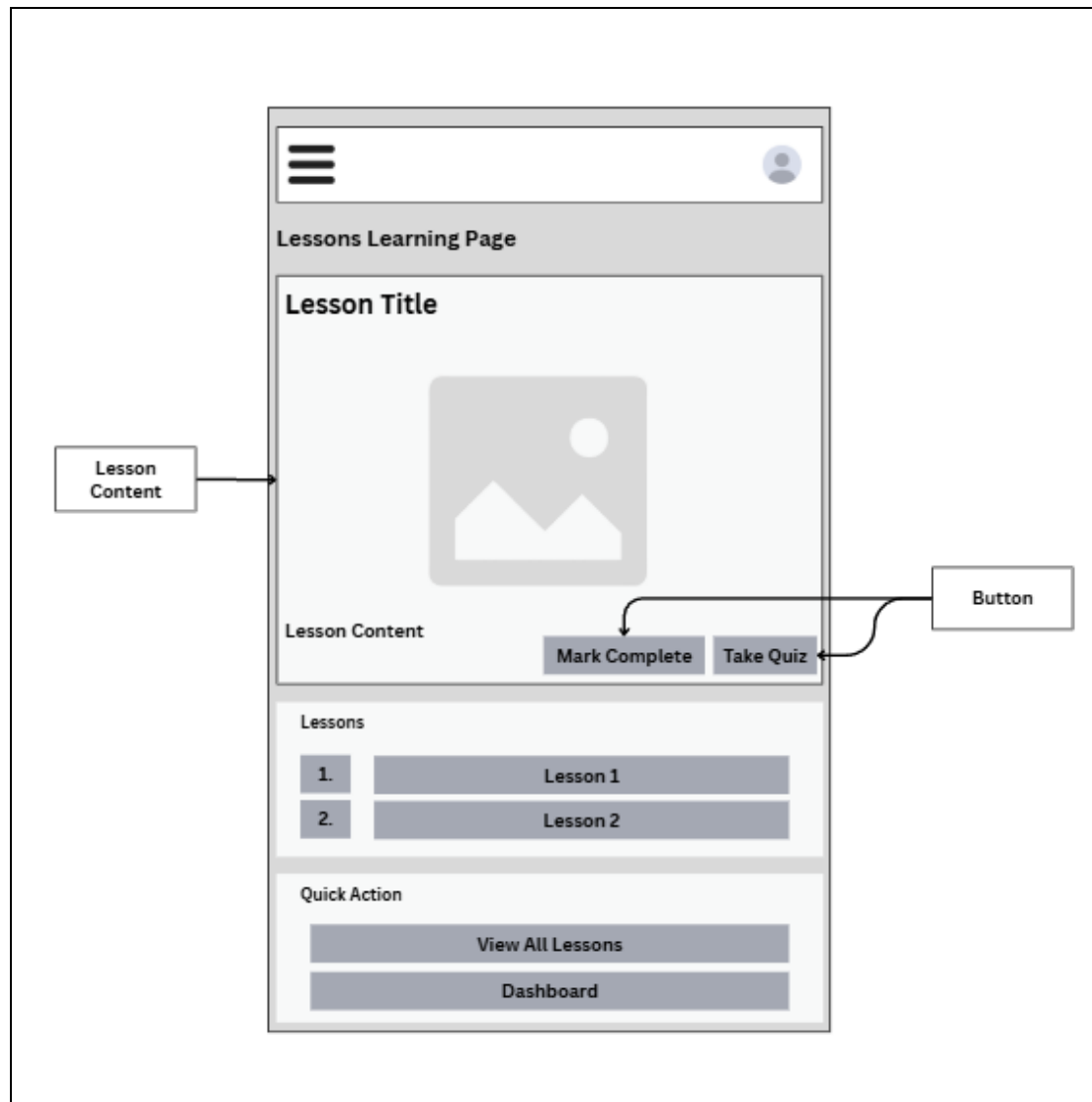


Figure 4.19: Lesson Learning Page (Mobile View)

The mobile view wireframe of the lesson learning page is presented in figure 4.19. The lesson title, content, and navigation buttons are arranged vertically with the Mark as Complete button and quiz navigation being available through a scrollable design to allow all the controls to be accessible on smaller screens.

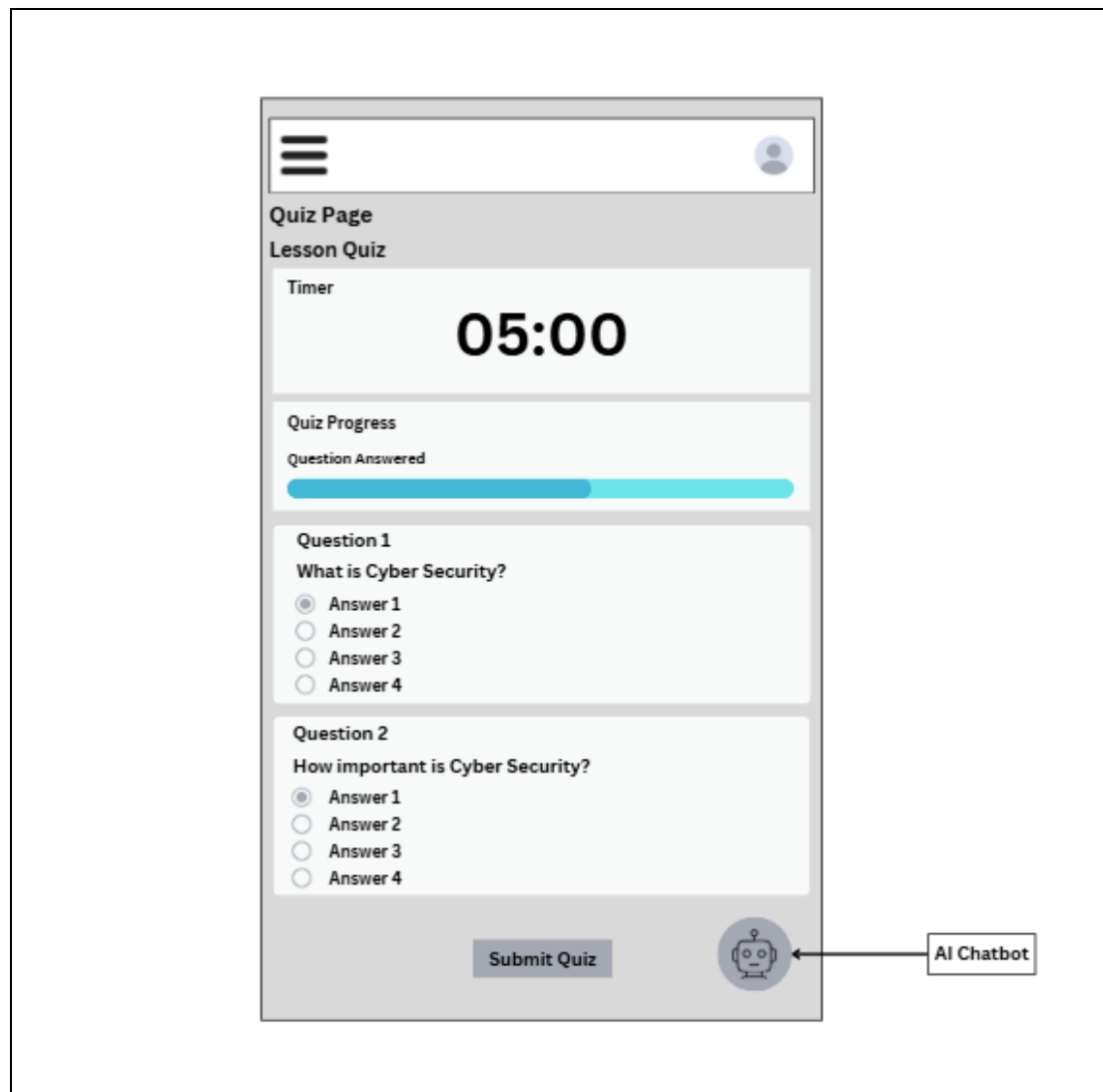


Figure 4.20: Quiz Page (Mobile View)

The quiz page mobile view wireframe is depicted in figure 4.20. The questions in the quiz, the countdown timer, the progress indicator, and the AI chatbot button are all rearranged into a single-column format. The timer and quiz information bar is also reorganized to be displayed above the questions so that one can easily follow the quiz by scrolling through a mobile screen.



Figure 4.21: Quiz Result Page (Mobile View)

The mobile view wireframe of the quiz result page is presented in figure 4.21. Pass or fail status and the score display and navigation buttons are arranged in a centred single column format where the students can easily view their scores and move to the next activity without scrolling horizontally using a mobile phone.

4.3 Database Design

Database design determines how data will be stored, arranged and how information will be managed within the system. A properly designed database guarantees consistency, accuracy and effective data retrieval in the process of system operation. This part outlines the logical database design such as data definitions, entity-entity relationship, and data flow in the system. There are a number of design tools that are used to represent the way data is stored, accessed and processed to support system functionality and these are the data dictionary, data flow diagram and entity relational diagram.

4.3.1 Data Dictionary

Table 4.1: Users Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique user identifier
name	VARCHAR(255)	NOT NULL	User's full name
email	VARCHAR(255)	NOT NULL, UNIQUE	User's email address
email_verified_at	TIMESTAMP	NULLABLE	Email verification timestamp
password	VARCHAR(255)	NOT NULL	Hashed password
google_id	VARCHAR(255)	NULLABLE	Google OAuth ID
avatar	VARCHAR(255)	NULLABLE	Google profile picture URL
remember_token	VARCHAR(100)	NULLABLE	Session remember token
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time
onboarded_at	TIMESTAMP	NULLABLE	When student completed onboarding guide

Table 4.1 illustrates the design of the users table, which is the key node of all user accounts in CyberSafe Learning Hub. Authentication credentials such as email and password are stored in this table to enable traditional login, and the following credentials are stored, google_id and avatar to enable users to authenticate using Google OAuth 2.0. The table is linked to multiple other entities, it connects to roles through the user_roles pivot table to determine user permissions,

to modules through the `created_by` foreign key to track which admin created each module, to `student_progress` to monitor lesson completion, to `quiz_attempts` to record assessment submissions, to `lesson_comments` to enable discussion, and to `achievement_notifications` to deliver system messages. The many-to-many connections with badges and certificates via their corresponding pivot tables enable the system to monitor which of the achievements each student has achieved.

Table 4.2: Roles Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique role identifier
name	VARCHAR(255)	NOT NULL, UNIQUE	Role name (admin, student)
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.2 presents the design of the roles table which determines the permission levels in the system. There are just two records in this table, namely, the type of user, which are 'admin' and student. The users are connected to the table by the `user_roles` pivot table which applies the many to many relationships where the user can have many roles as required. Role assignment is used to define which features and data each user is allowed to access, with admins having complete CRUD access to the content and students having read-only access to published material.

Table 4.3: User Roles (Pivot) Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique record identifier
user_id	BIGINT	FK → users.id	User reference
role_id	BIGINT	FK → roles.id	Role reference

Table 4.3 shows the structure of the `user_roles` pivot table, which implements the many-to-many relationship between users and roles. This junction table contains foreign keys to both the users and roles tables, allowing the system to assign multiple roles to a single user and assign a single role to multiple users. When a user logs in, the system queries this table to determine their permissions and control access to administrative features versus student-facing features.

Table 4.4: Categories Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique category identifier
name	VARCHAR(255)	NOT NULL	Category name
description	TEXT	NULLABLE	Category description
icon	VARCHAR(255)	NULLABLE	Category icon/emoji
order	INT	DEFAULT 0	Display sort order
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.4 shows the structure of the categories table, which provides the top-level organization for learning content. Each category represents a major subject area in cybersecurity education. The table is linked to modules through the category_id foreign key in the modules table, establishing a one-to-many relationship where one category can contain multiple modules. Categories are also linked to certificates, meaning that when a student completes all modules within a category, they become eligible to receive the associated certificate.

Table 4.5: Modules Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique module identifier
category_id	BIGINT	FK → categories.id, NULLABLE	Parent category reference
title	VARCHAR(255)	NOT NULL	Module title
description	TEXT	NOT NULL	Module description
cover_image	VARCHAR(255)	NULLABLE	Module cover image path
created_by	BIGINT	FK → users.id, NULLABLE	Admin who created
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.5 shows the structure of the modules table, which represents individual learning units within categories. Each module is linked to a parent category through the category_id foreign key and to the admin who created it through the created_by foreign key. Modules are connected to lessons in a one-to-many relationship, allowing each module to contain multiple sequential lessons. Additionally, each module has a one-to-one relationship with the badges table, meaning that completing all lessons in a module awards the student the associated badge.

Table 4.6: Lessons Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique lesson identifier
module_id	BIGINT	FK → modules.id, CASCADE	Parent module reference
title	VARCHAR(255)	NOT NULL	Lesson title
content	LONGTEXT	NOT NULL	Rich text lesson content
order	INT	DEFAULT 0	Display order in module
lesson_order	INT	DEFAULT 0	Alternative ordering field
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.6 demonstrates the format of the lessons table that accommodates the real educational content that is provided to learners. The lesson is related to a module through the module_id foreign key. Lessons are connected to lesson_contents in one-to-many association which enable rich multimedia content, containing several text and image blocks. They are also related to lesson_comments, where the students can discuss and ask questions. The relationship between each lesson and quizzes is one to one, so every lesson will have an assessment. The student progress table records the users who have attended which lesson, which forms a many to many relationship between the user and lessons.

Table 4.7: Lesson Contents Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique content block ID
lesson_id	BIGINT	FK → lessons.id, CASCADE	Parent lesson reference
type	ENUM	'text', 'image', 'video'	Content type
width	VARCHAR(10)	DEFAULT '100'	Image display width percentage
alignment	VARCHAR(10)	DEFAULT 'center'	Image alignment (left/center/right)
content	TEXT	NOT NULL	Text content or image path
position	INT	NOT NULL	Display order
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.7 displays the schema of the lesson contents table, through which lesson contents can be assembled in modules. A parent lesson is connected to each content block using a lesson id foreign key. The type field defines the nature of the content as either text or image and the position field defines the order of display. This design enables lessons to include embedded text description and visual illustrations, and they provide interactive multimedia learning experiences.

Table 4.8: Lesson Comments Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique comment identifier
lesson_id	BIGINT	FK → lessons.id, CASCADE	Parent lesson reference
user_id	BIGINT	FK → users.id, CASCADE	Commenting user reference
content	TEXT	NOT NULL	Comment content
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.8 presents the lesson comments table structure that will support student interaction and learning with peers. The comments are connected to a lesson (through lesson_id) and a user (through user_id), and form a many-to-many relationship between the users and the lessons. This enables students to pose questions, provide insights and comment on content with other students and instructors to be able to see how well the content is understood and where the content is generally misunderstood.

Table 4.9: Quizzes Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique quiz identifier
lesson_id	BIGINT	FK → lessons.id, CASCADE	Parent lesson reference
title	VARCHAR(255)	NOT NULL	Quiz title
total_marks	INT	DEFAULT 0	Total possible marks
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.9 presents the format of the quizzes table, which determines tests of knowledge verification. The how many lessons are associated with each quiz is a one-to-many relationship (one lesson is associated with one quiz). Questions are related to quizzes in a many-to-one form whereby each quiz can have several questions.

The quiz attempts table will connect the quizzes to the users and will be used to record the number of times the students have completed each quiz and scored.

Table 4.10: Questions Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique question identifier
quiz_id	BIGINT	FK → quizzes.id, CASCADE	Parent quiz reference
question_text	TEXT	NOT NULL	Question content
marks	INT	DEFAULT 1	Points for correct answer
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

The questions table is structured in Table 4.10 and it represents each assessment item in quizzes. Each question is a part of one quiz through the quiz_id foreign key. Questions and answers are connected in a one-to-many relationship where the question has several possible answers in a multiple-choice format. Mark field defines the number of points the question will be worth, and quizzes can be weighted.

Table 4.: Answers Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique answer identifier
question_id	BIGINT	FK → questions.id, CASCADE	Parent question reference
answer_text	VARCHAR(255)	NOT NULL	Answer option text
is_correct	BOOLEAN	DEFAULT FALSE	Correct answer flag
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

The table 4.11 represents the design of the answers table, which offers the answer options by answering the questions in a quiz. The question_id foreign key is connected to each answer. The is correct field of the type of a boolean field determines the answer that is correct and thus

they can be automatically graded using the is correct field. As the students post quiz attempts, their choice of answers is stored in the quiz answers table, which uses this table to check whether the student made the correct choice.

Table 4.12: Quiz Attempts Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique attempt identifier
user_id	BIGINT	FK → users.id, CASCADE	Student who attempted
quiz_id	BIGINT	FK → quizzes.id, CASCADE	Quiz attempted
score	INT	DEFAULT 0	Points scored
time_taken	INT	NULLABLE	Seconds to complete
completed_at	TIMESTAMP	NULLABLE	Completion timestamp
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.12 shows the structure of the quiz attempts table, which records student quiz submissions. The attempts are associated with a user (through user_id) and a quiz (through quiz_id), which establishes a many-to-many relationship that will enable students to take the quizzes more than once. The points made are stored in the score field, time spent is recorded in time taken and when the student finished is recorded in completed at. The relationship between this table and quiz_answers is one to many where individual question responses are the multiple responses per attempt.

Table 4.13: Quiz Answers Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique record identifier
quiz_attempt_id	BIGINT	FK → quiz_attempts.id, CASCADE	Parent attempt reference
question_id	BIGINT	FK → questions.id, CASCADE	Question answered
answer_id	BIGINT	FK → answers.id, SET NULL, NULLABLE	Selected answer
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.13 displays the design of the quiz answers table, which stores responses of individual questions in quiz attempts. Records are associated with a quiz attempt (through quiz attempt id), question (through question id), and answer chosen (through answer id). The is correct field is filled by matching the answer chosen with the correct answer in answers table. This granular tracking can allow the system to create specific analytics that will provide information about which questions students find the most difficult.

Table 4.14: Student Progress Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique progress identifier
user_id	BIGINT	FK → users.id, CASCADE	Student reference
lesson_id	BIGINT	FK → lessons.id, CASCADE	Lesson reference
status	ENUM	'not_started', 'in_progress', 'completed'	Progress status
completed_at	TIMESTAMP	NULLABLE	Completion timestamp
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.14 presents the design of the student progress table, which records the completion of lessons per student. This table establishes a many-to-many connection between users and lessons as user id and lesson id uses a foreign key. Status field is an enumeration with three states: not started, in progress and completed. Once a student finishes a lesson, this table is updated and the system will ensure that no lesson in a module has been left behind. In that case it invokes badge award logic to make a record in the user badges table.

Table 4.15: Badges Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique badge identifier
module_id	BIGINT	FK → modules.id, CASCADE, UNIQUE	One badge per module
name	VARCHAR(255)	NOT NULL	Badge name
description	TEXT	NULLABLE	Badge description
icon	VARCHAR(255)	DEFAULT '🏆'	Badge emoji/icon
image	VARCHAR(255)	NULLABLE	Badge image path
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.15 indicates the design of badges table that sets out achievement awards on completion of modules. The relationship is one to one with each badge having only one module in the module module foreign key that has a unique constraint. When the system finds out that a student has done all the lessons in a module by requesting the student progress table, a record is created in the user badges pivot table and achievement notification is created in the achievement notification table.

Table 4.16: User Badges Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique record identifier
user_id	BIGINT	FK → users.id, CASCADE	Student who earned
badge_id	BIGINT	FK → badges.id, CASCADE	Badge earned
earned_at	TIMESTAMP	NULLABLE	When badge was earned
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.16 presents the schema of the user badges pivot table, which logs badge awards to students. This table has a many-to-many setup between badges and users by using user-id and badge-id foreign keys. Upon the awarding of a badge, the system inserts a record at this point with the earned at timestamp and also inserts an achievement notification as an informative to the student. The distinctive uniqueness of (user_id, badge_id) ensures that awards are not duplicated.

Table 4.17: Certificates Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique certificate identifier
category_id	BIGINT	FK → categories.id, CASCADE	Category for completion
name	VARCHAR(255)	NOT NULL	Certificate name
description	TEXT	NULLABLE	Certificate description
template	VARCHAR(255)	NULLABLE	Template file path
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.17 shows the structure of the certificates table, which defines completion certificates for categories. The category id foreign key is used to associate each certificate with one category. Upon passing the student through all the modules in a category (defined by checking student

progress and comparing against all the lessons in all modules in that category), the system inserts a record into the user certificates table and a PDF is generated using the template stored within this table.

Table 4.18: User Certificates Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique record identifier
user_id	BIGINT	FK → users.id, CASCADE	Student who earned
certificate_id	BIGINT	FK → certificates.id, CASCADE	Certificate earned
issued_at	TIMESTAMP	NULLABLE	When certificate was issued
certificate_number	VARCHAR(255)	UNIQUE	Unique certificate number
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.18 provides the layout of the user certificates pivot table that will store the issuance of certificates to students. This table enforces a many to many relationship between users and certificates using user id and certificate id as foreign keys. A certificate is issued once the system assigns a certificate number (used to verify), the issued at timestamp is recorded and an achievement notification is created. The distinct constraint with (user_id, certificate_id) is so that a student is provided with one certificate at a given time.

Table 4.19: Achievement Notifications Table

Column	Data Type	Constraints	Description
id	BIGINT	PK, AUTO_INCREMENT	Unique notification identifier
user_id	BIGINT	FK → users.id, CASCADE	Recipient user
type	ENUM	'badge', 'certificate', 'admin_message'	Notification type
title	VARCHAR(255)	NOT NULL	Notification title
description	VARCHAR(255)	NULLABLE	Notification message
icon	VARCHAR(255)	NULLABLE	Display icon/emoji
image	VARCHAR(255)	NULLABLE	Display image path
is_seen	BOOLEAN	DEFAULT FALSE	Read status flag
created_at	TIMESTAMP	NULLABLE	Record creation time
updated_at	TIMESTAMP	NULLABLE	Last update time

Table 4.19 shows the structure of the achievement notifications table, which manages the notification system for student achievements and administrative messages. The user is associated with each notification by the user id foreign key. Type field differentiates badge awards, issuing certificates, and messages to the administrator. Where badges or certificates are provided by the user via the user badges or user certificates tables, the system will automatically generate the relevant notification records here. The `is_seen` flag is a Boolean to indicate whether the student has read the notification, and the `(userid, is seen)` index is optimized to answer queries on the number of unread notifications in the user interface.

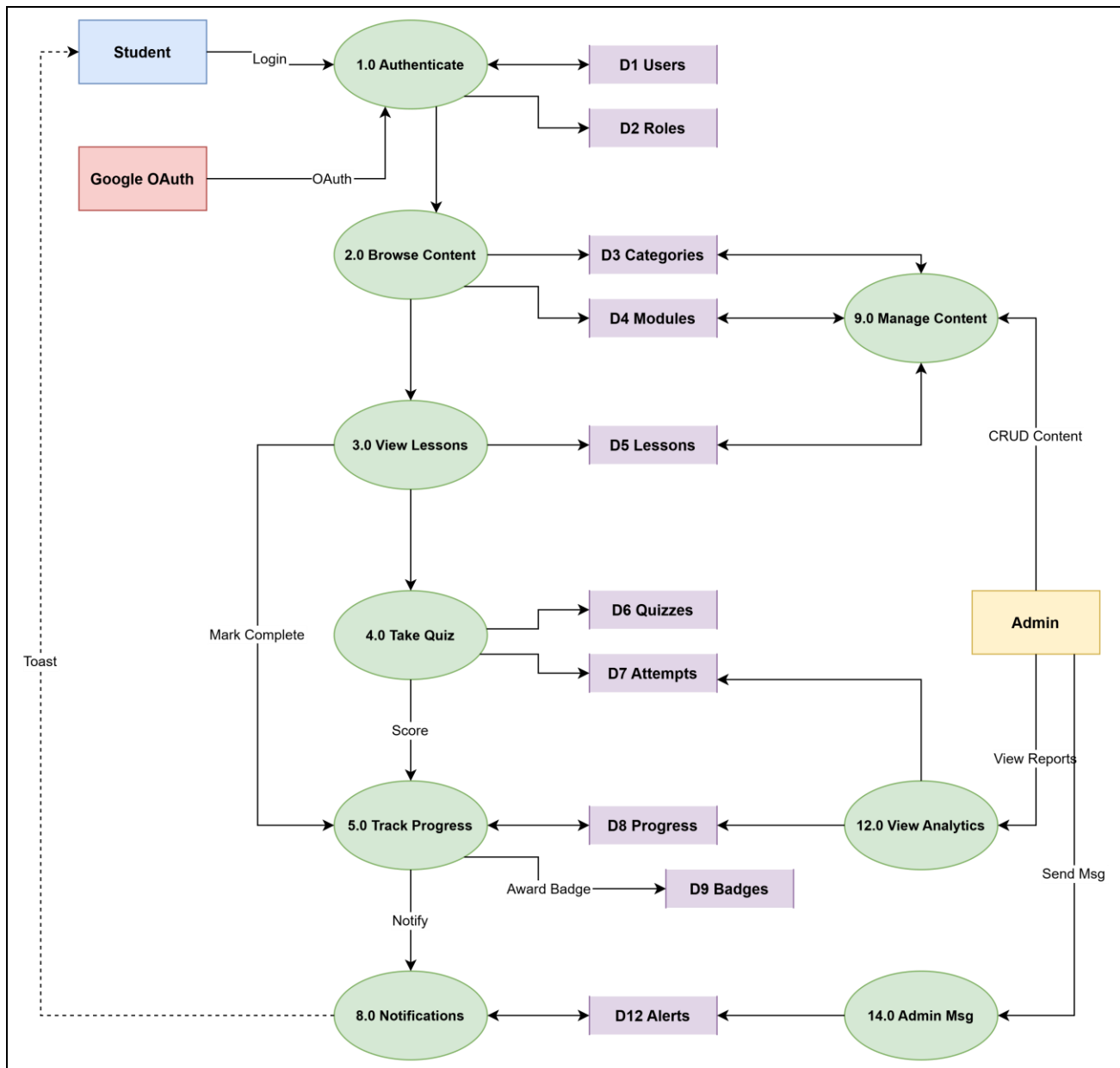


Figure 4.22: Data Flow Diagram

Figure 4.22 represents Level 1 Data Flow Diagram (DFD) of the CyberSafe Learning Hub. The DFD shows the flow of data between users, processes and data stores in the system. The diagram has been split into two major flows; the student flow and the admin flow. The student experience starts with authentication (Process 1.0). On the initial log in with email and password or with Google OAuth 2.0, the system will authenticate the user credentials with the Users data store (D1) and authenticate the user role with the Roles data store (D2). After authentication, the student will have access to the available modules and categories (Process 2.0), the data being retrieved in the Categories (D3) and Modules (D4) data stores. The system reads lesson contents in Lessons data store (D5) and presents them to the student when the student opens a lesson (Process 3.0).

The student is able to take a quiz after completing a lesson (Process 4.0). The system will retrieve the quiz questions in the Quizzes data store (D6) and store the answers and the score of the student in the Quiz Attempts data store (D7). The student is constantly updated with their completion status in the Progress data store (D8) by the progress tracking process (Process 5.0). A system automatically issues a badge and records to the Badges data store when a student has completed all the lessons in a module (D9). A certificate is awarded once all modules in a particular category are successfully done. These two events cause achievement notifications (Process 8.0) to be stored in the data store Alerts (D12) and presented to the student in real time.

On the administrative side, administrators handle all learning content in the content management process (Process 9.0). They are able to create, modify, and delete categories, modules, and lessons with the modifications being written directly to the Categories (D3), Modules (D4), and Lessons (D5) data stores. The analytics process (Process 12.0) also allows administrators to see platform-wide performance by reading the data in the Progress (D8) and Quiz Attempts (D7) data stores to create student engagement, quiz score, and completion rate reports. Also, administrators are able to send announcements to students via the messaging process (Process 14.0) that writes the notification to the Alerts data store (D12) to be sent to the concerned students.

4.3.3 Entity Relational Diagram (ERD)

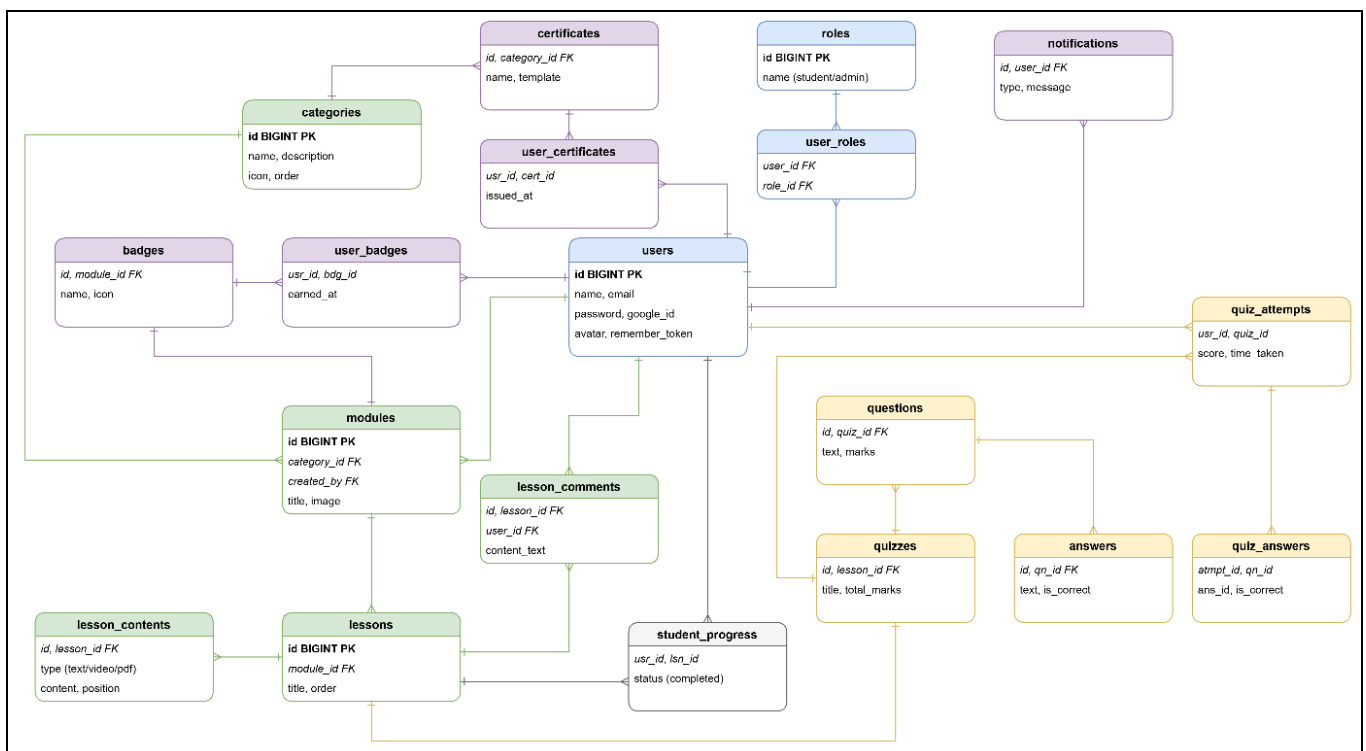


Figure 4.23: Entity Relational Diagram (ERD)

Figure 4.23 shows the Entity-Relationship Diagram (ERD) of CyberSafe Learning Hub's database structure. The ERD identifies the data structure and correlation of the various entities within the learning management system. It has significant objects such as users, roles, categories, modules, lessons, quizzes, questions, answers, badges, certificates, and achievement notifications. Primary and foreign keys are used to link each entity to demonstrate the flow of data among them. As an example, categories and users are associated with modules, i.e. each module is a part of a category and it is created by a particular user, an admin. Moreover, lessons are linked to modules through the `module_id` foreign key, which implies that each lesson is part of one module, and a module may have several lessons. In the same manner, the quizzes are associated with lessons in one-to-one relationship, with each lesson corresponding to one quiz. The student progress tracking is achieved by the use of the `student_progress` table which is used to connect the users to lessons, so the system can know which lessons the individual student has done. Badges are linked to modules and hence one module is linked to one badge which students can obtain when they complete the module. Certificates are associated with categories meaning that when students have successfully done all modules in a category, they get a certificate. The `user_badges` and `user_certificates` pivot tables adopt the many-to-many relationship whereby the same badge or certificate can be earned by more than one student. The ERD used in this system illustrates the interaction between separate elements of the cybersecurity learning platform that are necessary to guarantee successful delivery of content, track progress, and award achievement.

4.4 Security System Framework

Security System Framework shows how the security mechanisms are applied in the system to secure data, system resources, and user access. This framework defines the security components used at various stages of the system such as user authentication, authorization, data protection, and system control. The diagram gives a good picture of the interaction between security components to ensure that unauthorized access is prevented and data confidentiality, integrity, and availability are maintained.

4.4.1 Security Framework Diagram

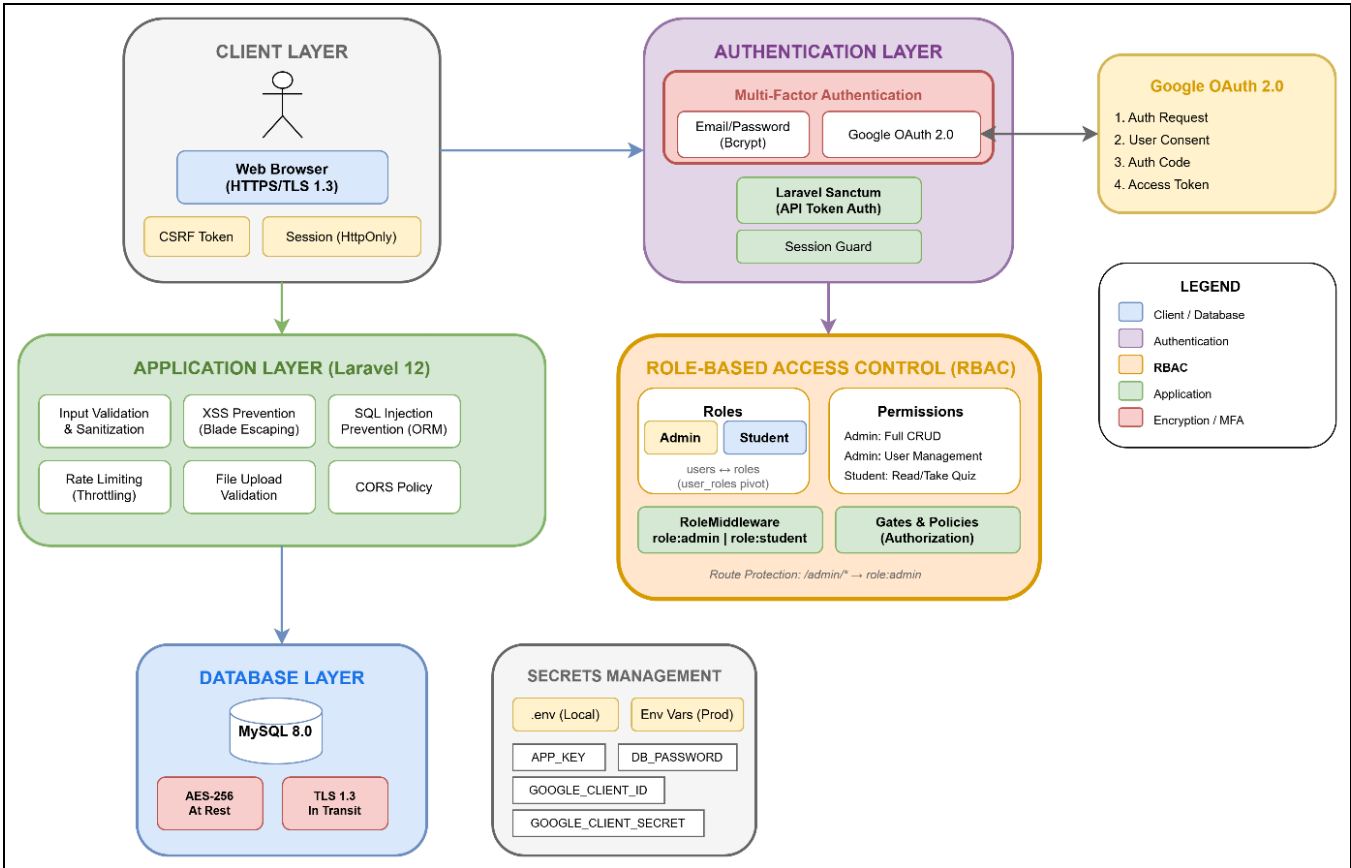


Figure 4.24: Security System Framework Diagram

Figure 4.24 presents the Security Framework Diagram (SFD) of the multi-layered security architecture of CyberSafe Learning Hub. The SFD shows the defense-in-depth strategy that is deployed to secure user data and system integrity in five different layers. On the Client Layer, all the communications are encrypted with HTTPS and TLS 1.3, and the data confidentiality is guaranteed in the process of transmitting the data between the users and the server. The Application Layer is used to deploy authentication schemes such as Multi-Factor Authentication (MFA) and integration of Google OAuth 2.0, which enables users to gain access to the system through either their conventional credentials or via their Google accounts. Laravel Sanctum takes care of API tokens of authenticated sessions. Role-Based Access Control (RBAC) is used to authorize users based on their roles (admin or student) which define their access privileges.

The system is based on Gates and Policies provided by Laravel to perform fine-grained authorization checks on access to specific resources. At this layer, input validation is done to ensure that malicious data is not entered. The Business logic layer is secure because it has the built-in security features of Laravel that prevent common web vulnerabilities such as Cross-site Scripting (XSS), Cross-site Request Forgery (CSRF), and SQL Injection attacks. Rate limiting helps to eliminate brute force attacks and API abuse. Sensitive information at the Data Layer is encrypted at rest with AES-256 encryption which means that data is secured even when the database is breached. The Infrastructure Layer handles secrets and credentials by using environment variables in .env files, so that no sensitive configuration information is ever hard-coded in the application. The SFD illustrates the interplay of several security controls in order to form a holistic security posture that safeguards the learning platform against a wide range of threat vectors.

4.5 Implementation Introduction

This section explains how the proposed system will be implemented according to the designs, which have been discussed earlier in this chapter. It describes the platform, tools, and technologies to develop the system and the way they support the system requirements. This part gives a description of the execution platform, implementation tools, and system interfaces applied to make the system work as desired.

4.6 Execution Platform

The implementation platform is the environment of operating systems, server environment, and cloud infrastructure on which the CyberSafe Learning Hub was developed, tested, and eventually released towards end users. It was important to choose the appropriate platforms that would be compatible with all development tools and would provide good performance during production.

4.6.1 Development Platform

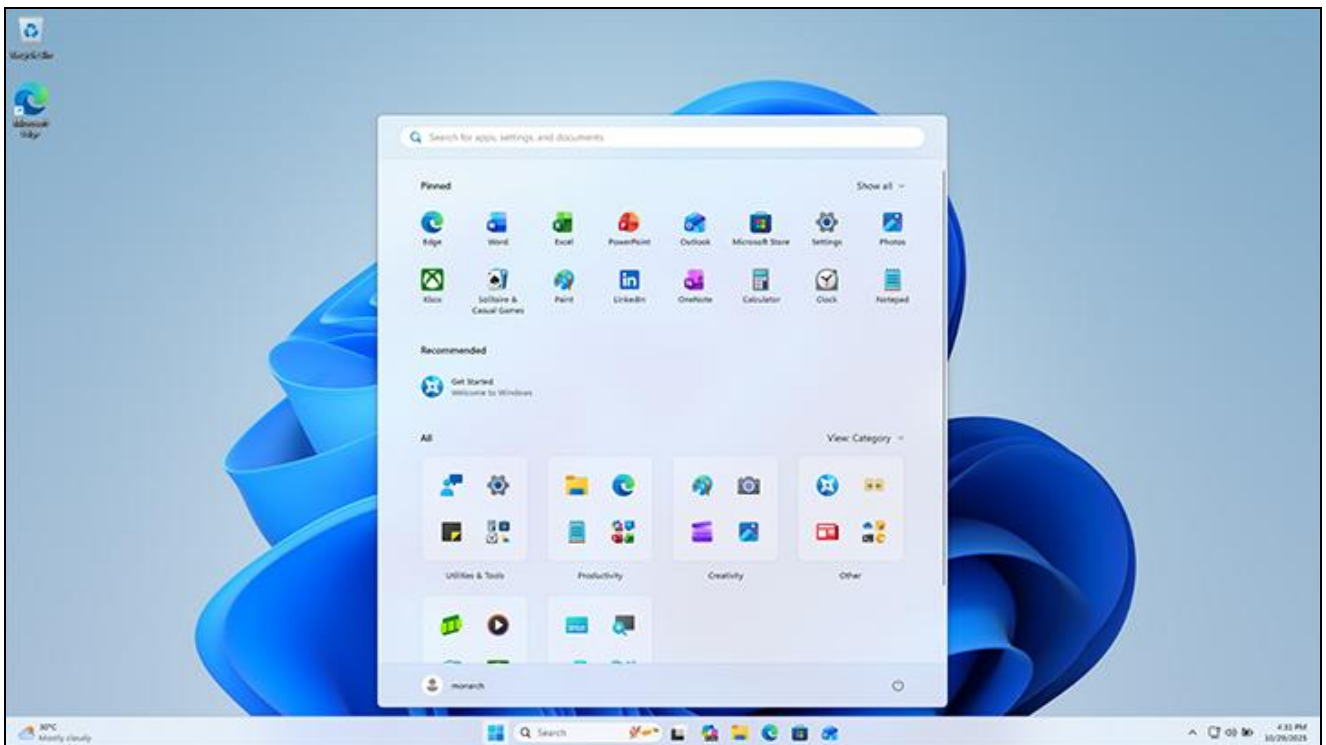


Figure 4.25: Windows 11 Pro

The image of Windows 11 Pro package is depicted in figure 4.25. The whole CyberSafe Learning Hub has been created on a machine with Windows 11 Pro as the main operating system. Windows 11 Pro was selected because it can be used with most of the tools needed in this project such as PHP 8.2 and Composer, Node.js 20 and npm, MySQL, Git, and Visual Studio Code. The enhanced multitasking of the operating system enabled the developer to execute several running processes at any given time during the development process, including the Laravel Artisan server (php artisan serve), the Vite frontend compiler (npm run dev), a queue listener to background jobs, and browser testing at the same time without affecting the performance. Windows 11 Pro also allowed native terminal access via PowerShell, which made it easy to run Laravel CLI commands, database migrations, and deployment scripts in the development environment.

4.6.2 Hosting Platform

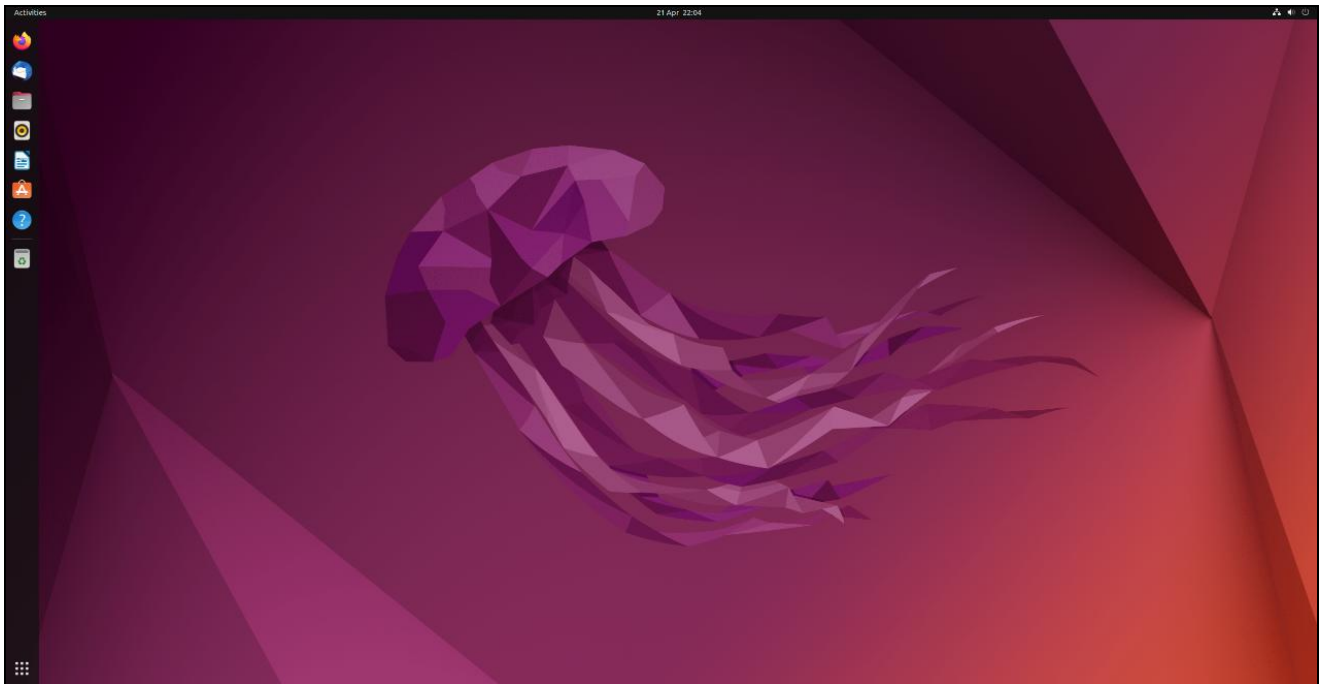


Figure 4.26: Ubuntu 24.04 LTS

Figure 4.26 depicts the picture of Ubuntu 24.04 LTS package. In order to roll out the production, the CyberSafe Learning Hub is launched on a DigitalOcean cloud Droplet running Ubuntu 24.04 LTS. The reason why Ubuntu has been selected as the server operating system is due to its long support period, good community support and its popularity with web hosting systems. It is the most suitable to execute containerised applications on cloud virtual machines due to its light presence and resource management. Deployment is handled using the Coolify self-hosting platform which automates the build/deployment pipeline every time a new code is pushed to GitHub. The app is deployed on the server as four Docker containers working together: a PHP-FPM container that can run the Laravel application code, an Nginx container that serves as the web server and reverse proxy, a MySQL 8.0 container that manages all the persistent data, and a phpMyAdmin container that can be used to access database administration through the web. This ubuntu containerised architecture ensures that the behaviour is the same in all environments, the scaling is easy, and the maintenance of the production system is also simplified.

4.7 Implementation Tools

Implementation tools are the software tools that are used to construct, execute, and test the CyberSafe Learning Hub. These tools are imperative in a successful development process as well as the system functioning as desired. Different stages of the project, such as coding, user interface design, testing, and deployment, are supported by the selected tools.

4.7.1 Software

The section discusses software tools and structures that were employed during the development, deployment, and management of the CyberSafe Learning Hub. The following tools address the whole development lifecycle, such as code writing and maintenance, database maintenance, deploying the application to a live server, and integrating third-party services. The choice of each tool was guided by its appropriateness to a complete stack Laravel web application, its dependability, community support, and the compatibility with the other components of the technology stack. All the tools provided a cohesive development environment that helped in the delivery of the system in a smooth and systematic manner.

4.7.1.1 Visual Studio Code

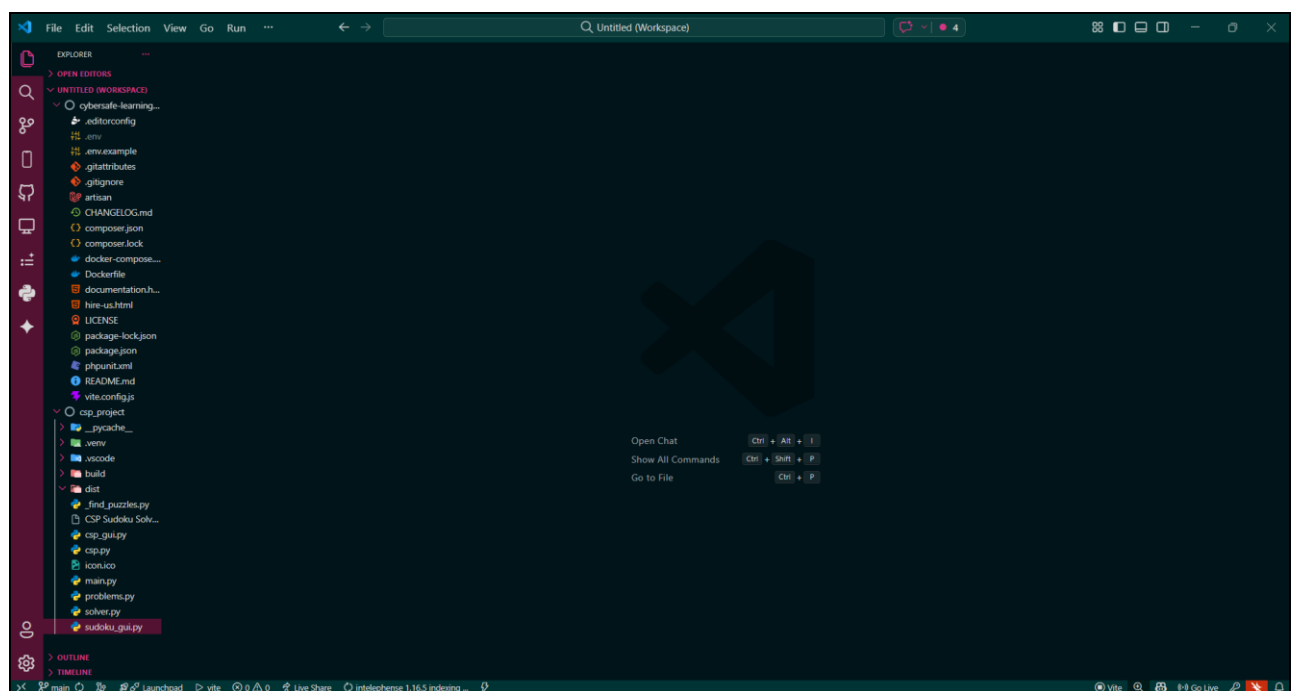


Figure 4.27: Visual Studio Code Interface

Figure 4.27 represents the interface of Visual Studio code that was used to make the CyberSafe Learning Hub. Visual Studio Code or VS Code was the primary code editor on which the CyberSafe Learning Hub was developed. This software gave it a lean and loose platform to code and support code of all system components (admin panel, student interface, quiz system, and AI chatbot).

It also supports various programming languages such as PHP, JavaScript, HTML, and CSS that made it appropriate in a full stack Laravel project that encompasses various technologies. The productivity was enhanced with speed and reduced errors due to built in features such as syntax highlighting, IntelliSense (automatic code completion) and debugging tools. The extension marketplace of VS Code also enabled the installation of handy tools such as Laravel Blade Snippets, PHP Intelephense, Livewire snippets and Git integration, which made the development process much easier.

4.7.1.2 Laravel 12 Framework

The CyberSafe Learning Hub was developed based on Laravel 12 as the main backend framework. Laravel is a framework based on PHP web application that adheres to the Model-View-Controller (MVC) architectural pattern. It was chosen due to the elegant syntax, in-built authentication, strong Eloquent ORM to perform database operation, and strong middleware system to protect routes. The Blade templating engine was used to build dynamic, reusable HTML templates, and the migration system allowed management of the schema of the database version. The framework also offered inbuilt security measures which included CSRF protection, SQL injection protection by use of parameterised queries and password hashing by use of bcrypt. Also, the routing system and middleware of Laravel enabled the easy adoption of role-based access control, which separated the functionality of an administrator and a student.

4.7.1.3 Livewire

Livewire and its companion Volt were employed to generate reactive and dynamic frontend components of the Laravel application. Livewire is a Laravel full-stack framework that simplifies the creation of dynamic interfaces, without the need to leave the comfort of PHP. Livewire enabled interactive functionality such as real-time form validation, dynamic settings pages and live profile updates to be implemented in all PHP instead of writing complex JavaScript. The user settings pages (profile and password management) were created using Volt, a single-file component approach to Livewire. This technology option saved the development time greatly because it did not require a separate frontend JavaScript framework but offered a smooth and modern user experience.

4.7.1.4 Bootstrap 5

The CSS framework applied in the design of the user interface of the CyberSafe Learning Hub was bootstrap 5.3. Bootstrap was a full suite of ready-to-use responsive UI elements, including navigation bars, cards, buttons, modals, forms, and grid layouts. It allowed the development of a mobile-first, responsive design that easily adjusts to various screen sizes - desktop monitors, tablets, and smartphones. The utility classes and component system in the framework enabled quick prototyping of the UI and made all pages to be styled in a similar way. The SCSS source files of Bootstrap were compiled using Vite and the theme colours and component styles were customised to fit the cybersecurity-themed branding of the site.

4.7.1.5 MySQL 8.0

The relational database management system (RDBMS) that will be used in the CyberSafe Learning Hub is MySQL 8.0. All persistent application data such as user accounts, roles, learning modules, lessons, lesson content blocks, quiz questions, answers, quiz attempts, student progress record, badges, certificates, achievement notifications and lesson comments were stored in MySQL. MySQL can be deployed in production in a Docker container and the data stored using Docker volumes to make it durable. Laravel migration system which offered version controlled reversible database changes was used to manage the database schema. Eloquent ORM of Laravel was employed to communicate with MySQL, which offered an expressive and safe method of querying and manipulating data without typing raw SQL, thus avoiding SQL injection issues.

4.7.1.6 Nginx

Nginx was used as the high-performance web server for the production deployment of the CyberSafe Learning Hub. Nginx serves as a reverse proxy, which receives all the incoming requests via the browser of the users in the form of HTTPS and directs PHP requests to the PHP-FPM application container to be processed. Nginx serves the compiled CSS, JavaScript bundles, images, and uploaded content directly to provide the best performance and less load on the server. The Nginx settings were modified to accommodate the URL routing of the Larval application, file upload limits and correct delivery of files which are linked to the storage. The event-oriented nature of Nginx renders it very effective in managing simultaneous connections to make the platform remain responsive to the load.

4.7.1.7 Docker

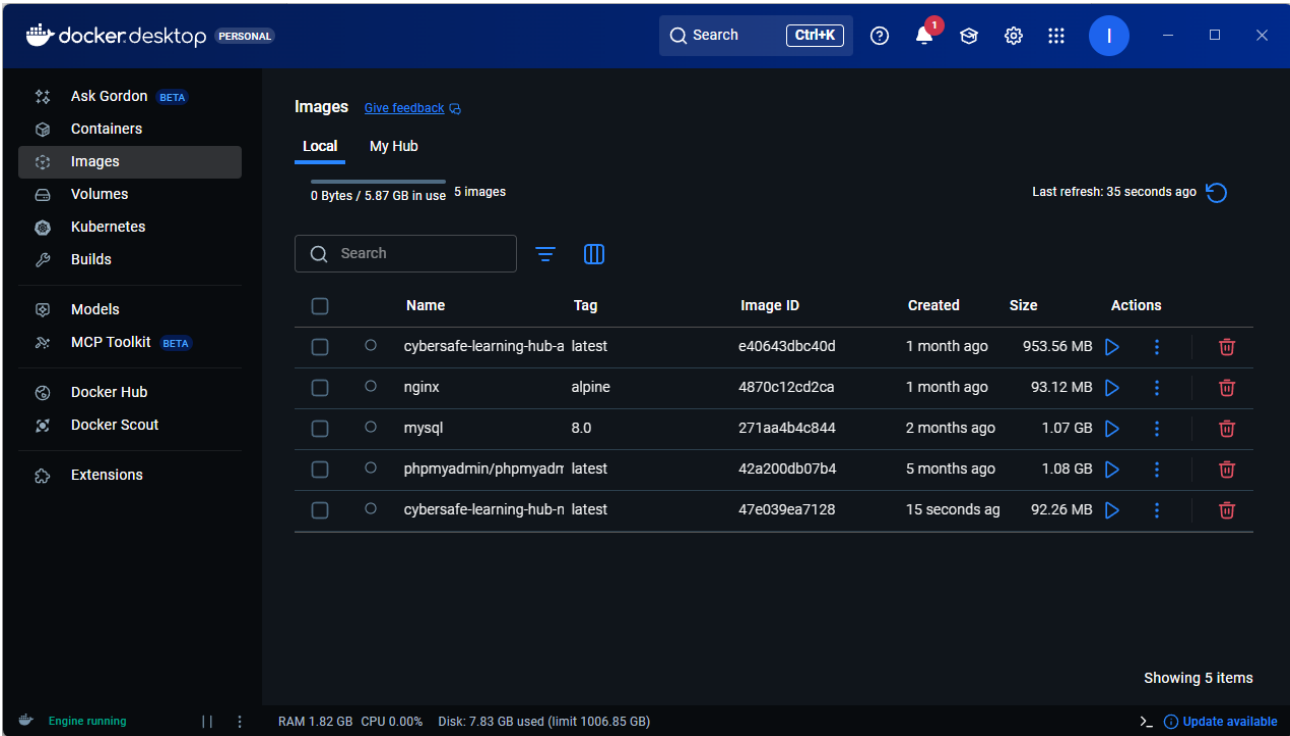


Figure 4.28: Docker Interface

Figure 4.28 shows the interface of Docker. The CyberSafe Learning Hub was packaged and deployed on Docker as the containerisation platform in a consistent and reproducible way. A custom Dockerfile was developed which installs PHP 8.2 and extensions (PDO, MySQL, GD, BCMath, Zip, Mbstring), Composer to manage PHP dependencies and Node.js 20 to compile frontend assets. The docker-compose.yml file is a coordination of four containers that collaborate with each other: the Larval application (PHP-FPM), Nginx web server, MySQL database and phpMyAdmin. Docker makes the application to run the same in development, testing, and production environments, and it does not matter whether it works on my machine. This containerised method also facilitates deployment using the Coolify platform that automatically builds and pushes the Docker containers on the DigitalOcean server.

4.7.1.8 DigitalOcean

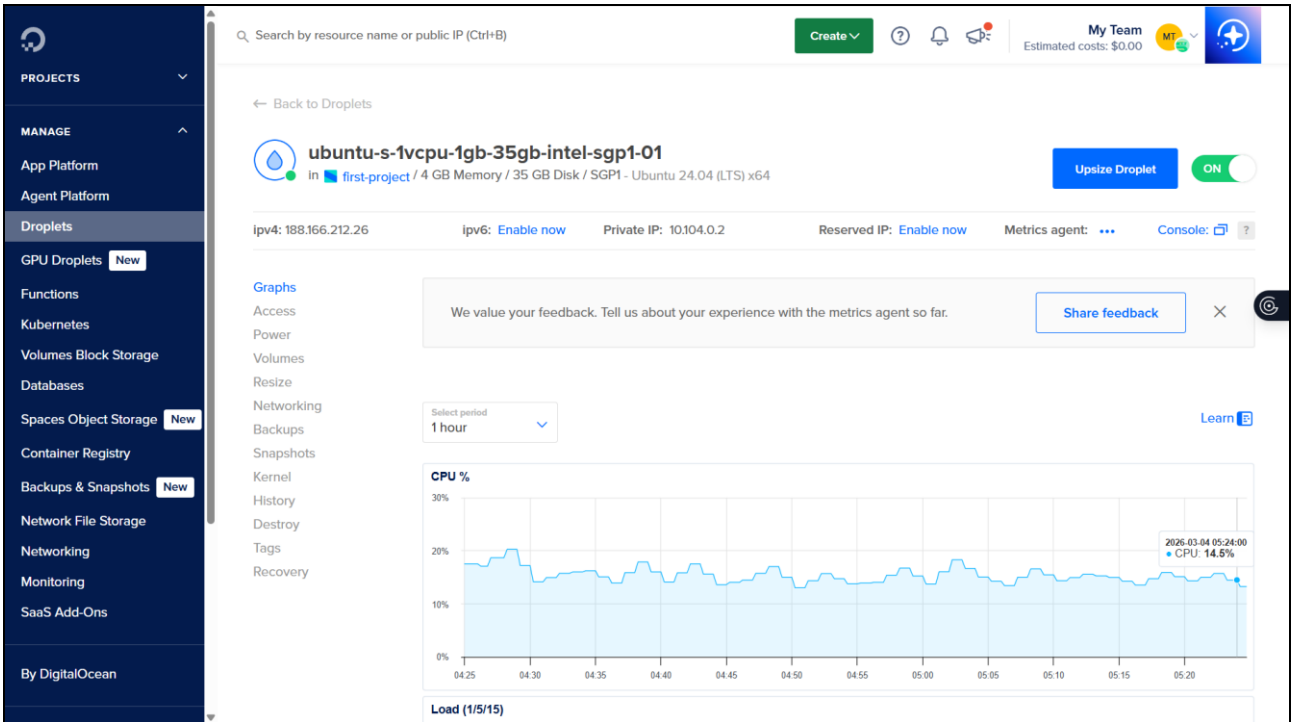


Figure 4.29: DigitalOcean Interface

Figure 4.29 shows the interface of DigitalOcean. DigitalOcean was the cloud computing provider that hosted the CyberSafe Learning Hub in a production environment, which is accessible through the internet. The app was installed on a DigitalOcean Droplet (Virtual Private Server) with Ubuntu 22.04 LTS with the Coolify self-hosting platform. DigitalOcean was an affordable and dependable cloud platform that also offered such features as dedicated IP addresses, SSD-based storage, and scaled resources. The process of deployment was automated; it is when code is pushed to GitHub, Coolify identifies the changes and automatically rebuilds and redeploys the Docker containers to ensure continuous delivery. The network infrastructure of DigitalOcean also provides HTTPS through the use of the SSL certificates, which guarantees the encryption of the communication between the user and the platform.

4.7.1.9 Coolify

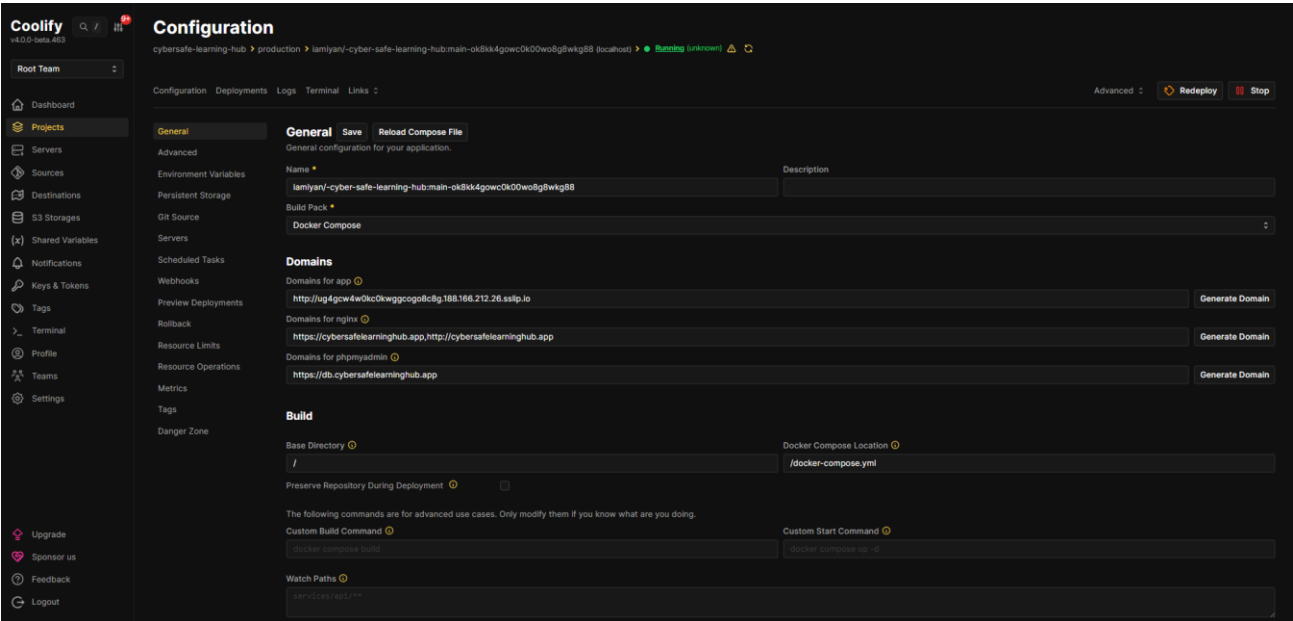


Figure 4.30: Coolify Interface

Figure 4.30 reveals the interface of the Coolify self-hosting platform that is used to administrate the deployment of the CyberSafe Learning Hub. Coolify is an open-source, self-hosted platform-as-a-service (PaaS) an easy-to-use, web-based dashboard to manage application deployments on cloud servers. Coolify is deployed in this project in the DigitalOcean Droplet with Ubuntu 22.04 LTS as the orchestration layer between GitHub and the Docker containers. When new code is committed to the main branch on GitHub, Coolify automatically identifies the changes, builds a new Docker image based on the project docker-compose.yml and Dockerfile, and redeploys all containers automatically. It also has support to configure environment variables, and provisioning of SSL certificate through Let's Encrypt, and real time deployment logs to monitor build progress and troubleshooting. With Coolify, deployment pipeline becomes fully automated, dependable and reproducible, eliminating the necessity to maintain the server manually and deploy with scripted commands.

4.7.1.10 Vite

Vite 6.2 was used as the modern frontend build tool for the CyberSafe Learning Hub. Vite was used to assemble and package all frontend resources such as CSS, SCSS stylesheets, JavaScript files and vendor libraries. Vite offered an incredibly quick Hot Module Replacement (HMR) server during development, which immediately updated the browser with any code changes without loading a full page, which greatly accelerated the development process. To make production, Vite bundled and optimised all assets into minified bundles to reduce page load times. Vite was also integrated with the Blade templates in laravel using the larval-vite-plugin that automatically creates the appropriate asset URLs in both development and production modes.

4.7.1.11 Laravel Socialite

Laravel Socialite was used to implement Google OAuth 2.0 authentication in the CyberSafe Learning Hub. Socialite offers a rich and fluent interface to authenticate users using third-party OAuth providers, like Google, Facebook and GitHub. In this project, Google was set as the main OAuth provider, and students and administrators could log in safely using their existing Google accounts. This has removed the necessity of users to create and store individual passwords, enhancing security and user experience. Socialite supports the complete OAuth process such as redirecting users to Google authentication page, accepting the callback with user details and creating or associating the user accounts in database.

4.7.1.12 Groq AI

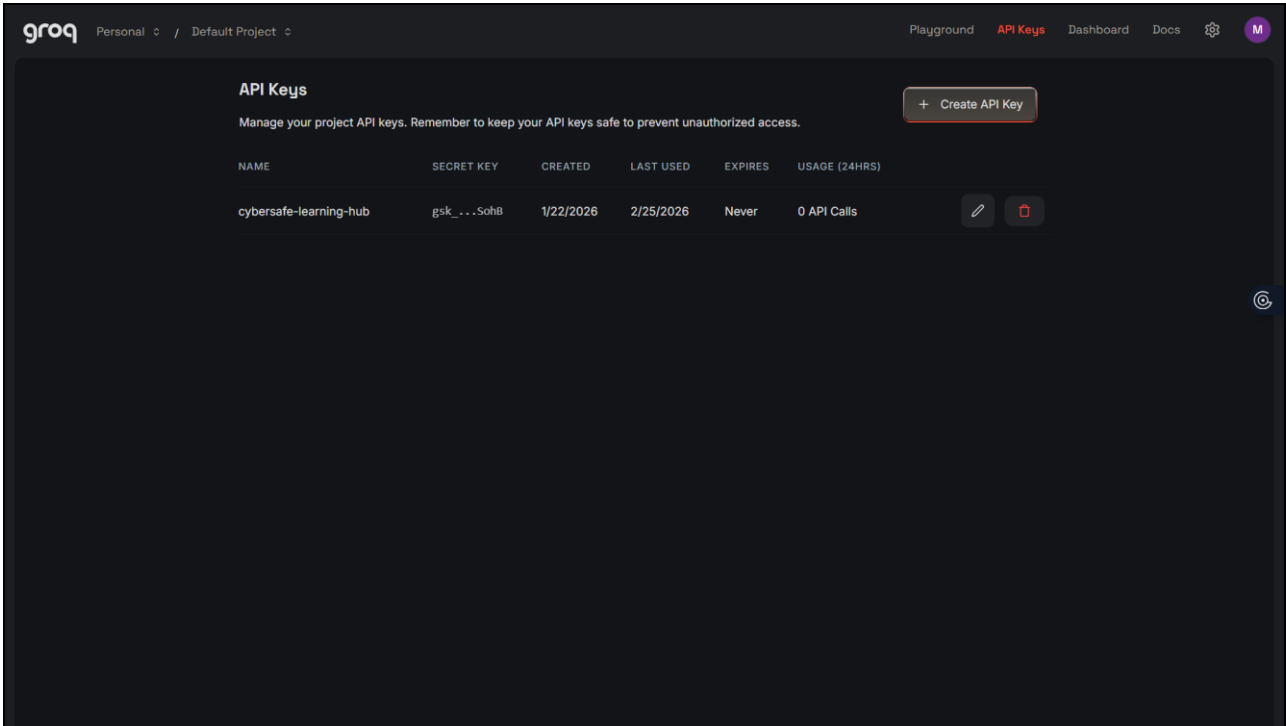


Figure 4.31: Groq AI - Llama 3.3 Interface

Figure 4.31 depicts the Groq AI API keys page on which the AI chatbot was to be integrated into the CyberSafe Learning Hub. The CyberSafe Learning Hub is a chatbot based on the Groq API that uses the Llama 3.3-70B Versatile model with an AI-powered chatbot. This chatbot is an assistant cybersecurity tutor that can be used by students during quizzes. Groq API was selected due to its high inference speed and high free tier, which is appropriate to use in an educational project. The chatbot is coded to include stringent system prompts to serve as a learning tool. It is a description of the concepts of cybersecurity, hints, and problem-solving without providing direct answers to the quiz. Such integration will provide the platform with an intelligent, interactive learning element that will improve the learning process and allow the students to gain more insight into the aspects of cybersecurity.

4.7.1.13 phpMyAdmin

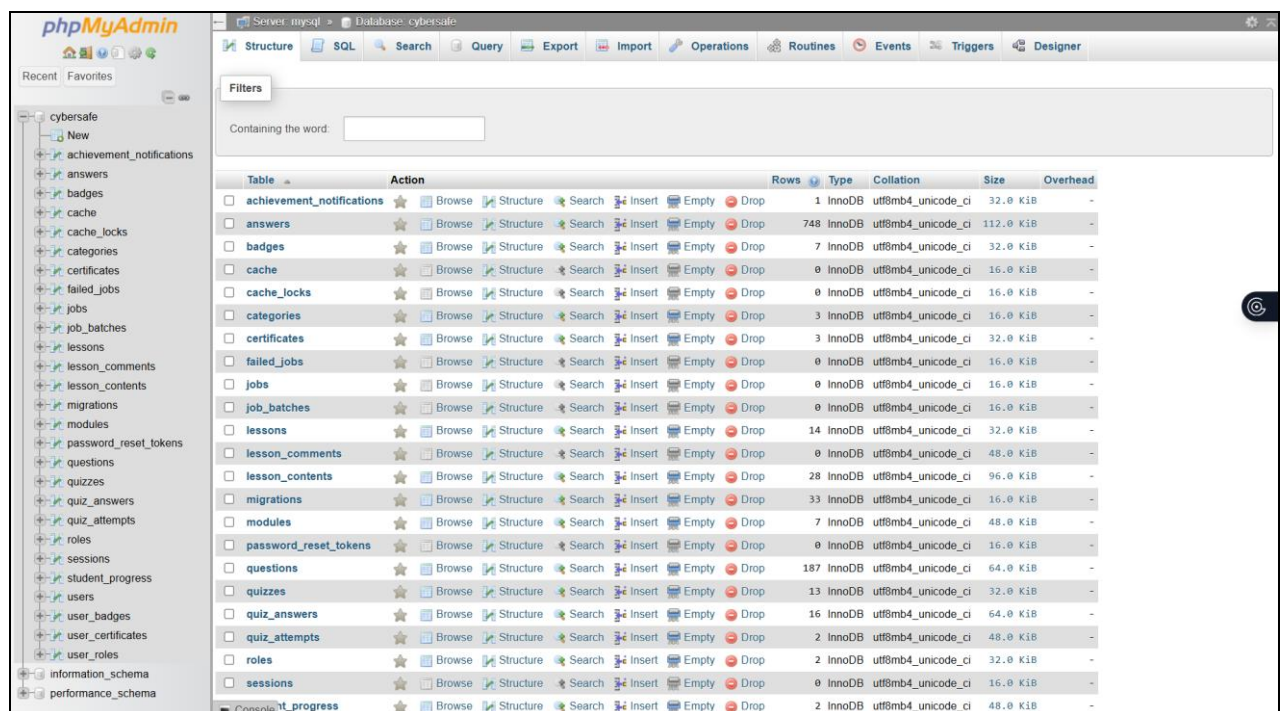


Figure 4.32: phpMyAdmin Interface

Figure 4.32 depicts the phpMyAdmin interface that was used to manage the CyberSafe Learning Hub database. The web-based database administration tool was phpMyAdmin that was employed in the management of the MySQL database of the CyberSafe Learning Hub. It operates as an independent Docker container in the production setup, and is a graphical interface to view, modify, and manage database tables, records and relationships. The phpMyAdmin was very handy in the development and maintenance process to check the student progress data, quiz attempt records, user accounts, and debug data-related problems. It was easier to comprehend intricate database relations without entering manual SQL queries due to its visual interface.

4.7.1.14 Composer

The PHP dependency manager of the CyberSafe Learning Hub was composer. It managed and installed all the PHP packages it needed the Laravel application, such as the Laravel framework, Socialite to authenticate users via OAuth, Livewire to create reactive components and several development tools, including Pest (testing framework), Pint (code formatting) and Faker (test data generation). Composer makes dependencies compatible with each other and automatically resolves version conflicts. All the needed packages with their version constraints are defined in composer.json, and reproducible installations in both development and production environments are guaranteed by composer.lock.

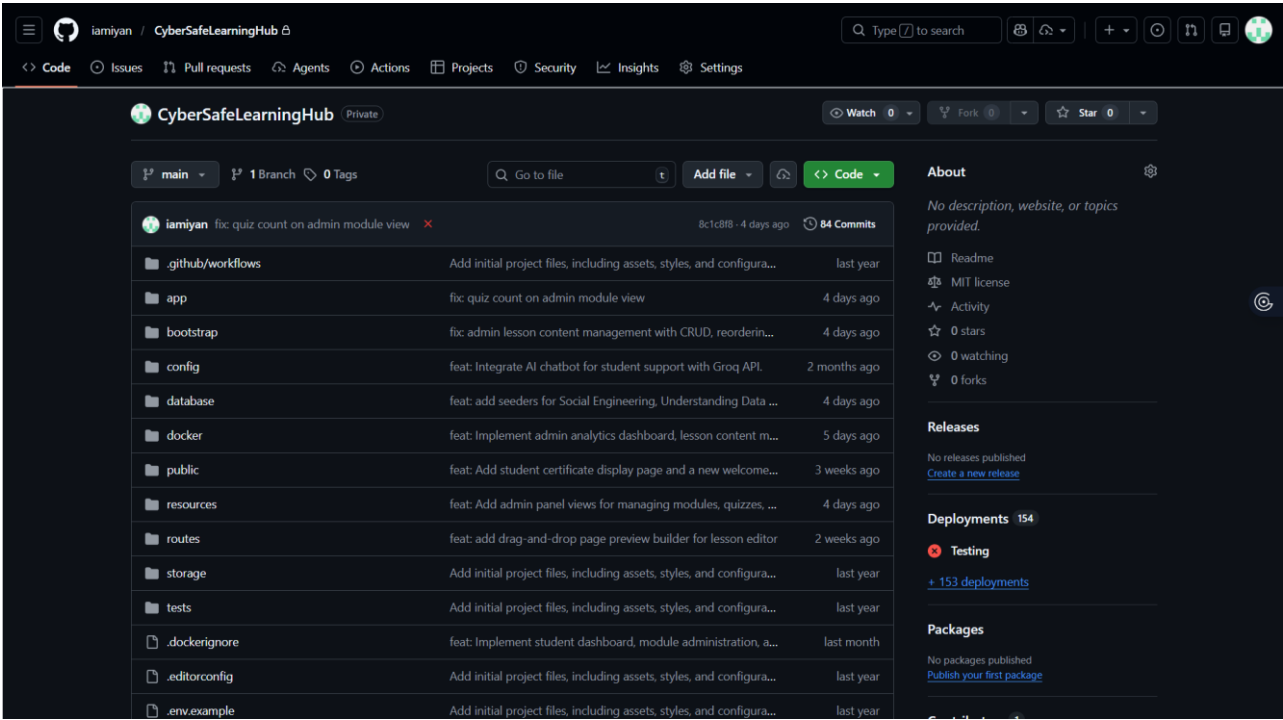


Figure 4.33: GitHub Interface

The interface of the GitHub repository of the CyberSafe Learning Hub project is presented in Figure 4.33. The version control and source code management were managed using Git and GitHub during the development of the CyberSafe Learning Hub. Git was used to trace all the changes done to the code so that the developer could have a full record of the changes made and could revert to the earlier changes in case there was need to do so and could also branch code in order to develop a feature. GitHub was the host platform that was used as a remote repository which served as a centralized place to keep the source code of the project. Also, GitHub was connected to the DigitalOcean deployment platform to allow automatic deployment, with each push to the main branch, an automated build and deployment process would run to keep the production server constantly up-to-date with the latest stable code.

4.7.2 Programming Language

The following section explains the programming languages applied to develop the CyberSafe Learning Hub. As the system is a full-stack web application, various languages were needed to support various parts of the platform - not only server-side business logic and database communication, but also organizing web content and visual styles. The languages were selected due to their compatibility with the Laravel framework and their popularity in the contemporary web development. The complementary roles were to be played in the provision of a functional, secure and responsive educational platform by different languages.

4.7.2.1 PHP

The main server-side programming language that was employed to create the CyberSafe Learning Hub in the Laravel framework is PHP 8.2. All the business logic like user authentication, role based access control, scoring quiz with 85 percent pass rate, issuance of badges on module completion, issuance of certificates on category and all database operations using Eloquent ORM were done in Laravel using PHP. Object oriented nature of PHP was exploited to produce maintainable code in structure, through Controllers, Models, Services and Middleware classes. The new features of PHP 8.2 including typed properties, enums, and better performance helped to write cleaner and more efficient code.

```

1 reference | 0 overrides
187 public function result(QuizAttempt $attempt)
188 {
189     // Security: only owner can view
190     if ($attempt->user_id !== auth()->id()) {
191         abort(403);
192     }
193
194     $attempt->load('quiz.questions.answers');
195
196     // Calculate percentage and pass/fail using question count
197     $totalQuestions = $attempt->quiz->questions->count();
198     $percentage = $totalQuestions > 0
199         ? ($attempt->score / $totalQuestions) * 100
200         : 0;
201
202     $passed = $percentage >= (self::PASS_THRESHOLD * 100);
203     $canRetake = !$passed;
204
205     return view('student.quizzes.result', compact('attempt', 'percentage', 'passed', 'canRetake'));

```

Figure 4.34: PHP Code Snippet – Quiz Result Controller

A snippet of PHP code in Figure 4.34 demonstrates how PHP was utilized in the CyberSafe Learning Hub to process the backend logic of access control, score calculations, and database interaction using the Eloquent ORM of Laravel.

4.7.2.2 JavaScript

JavaScript (ES6+) was used for client-side interactivity throughout the CyberSafe Learning Hub. JavaScript was used in the quiz module to support AJAX form submission so that the quiz could be taken without reloading the page, a countdown timer could be used, and the results could be shown with the help of popup modals. In the case of the AI chatbot, the real-time communication was handled with the API endpoint at Groq using JavaScript, and chat messages were rendered dynamically. Interactive lesson content viewing with progressive loading, content reordering in the administration panel by drag-and-drop, and other micro-animations and hover effects were also written in JavaScript and added to the user experience.

```

677 <script>
678 const totalQuestions = {{ $quiz->questions->count() }};
679 const QUIZ_TIME_SECONDS = totalQuestions * 2 * 60; // 2 minutes per question
680 let timeRemaining = QUIZ_TIME_SECONDS;
681 let timerInterval;
682
683 // Start the timer
684 function startTimer() {
685     timerInterval = setInterval(() => {
686         timeRemaining--;
687         updateTimerDisplay();
688
689         if (timeRemaining <= 0) {
690             clearInterval(timerInterval);
691             alert('Time is up! Your quiz will be submitted automatically.');
```

692 // Auto-submit using the AJAX function

693 confirmSubmit();

694 return;

695 }

696

697 // Warning at 1 minute

698 if (timeRemaining === 60) {

699 document.getElementById('timerCard').classList.add('warning');

700 document.getElementById('timerCard').classList.remove('critical');

701 }

702

703 // Critical at 30 seconds

704 if (timeRemaining === 30) {

705 document.getElementById('timerCard').classList.remove('warning');

706 document.getElementById('timerCard').classList.add('critical');

707 }

708 }, 1000);

709 }

710

711 function updateTimerDisplay() {

712 const minutes = Math.floor(timeRemaining / 60);

713 const seconds = timeRemaining % 60;

714 document.getElementById('timerDisplay').textContent =

715 `\${minutes.toString().padStart(2, '0')}:\${seconds.toString().padStart(2, '0')}`;

716 }

Figure 4.35: JavaScript Code Snippet – Quiz Timer

Figure 4.35 presents a JavaScript code snippet of the CyberSafe Learning Hub, demonstrating the use of JavaScript to add interactivity onto the client-side, including the quiz countdown timer and automatic submission of the form to the quiz interface.

4.7.2.3 HTML5

All web pages in the CyberSafe Learning Hub were structured with HTML5 using the Blade templating engine (.blade.php files) of Laravel. Semantic HTML5 tags including <header>, <nav>, <main>, <section>, <article>, and <footer> were used throughout the application to make its pages well structured, accessible, and search engine friendly. All user interactions were done through HTML forms such as login, quiz submissions, commenting on lessons, content creation, and module management. The Blade templating engine built upon the functionality of HTML by adding template inheritance, conditional rendering, loops and component-based architecture.

```

39      {{-- Questions --}}
40      @foreach($quiz->questions as $index => $question)
41          <div class="card mb-3 question-card" data-question="{{ $index + 1 }}">
42              <div class="card-header d-flex justify-content-between align-items-center">
43                  <span class="badge bg-primary me-2">Question {{ $index + 1 }}</span>
44                  <small class="text-muted">{{ $question->marks ?? 1 }} point(s)</small>
45              </div>
46              <div class="card-body">
47                  <p class="fw-bold mb-3">{{ $question->question_text }}</p>
48
49                  <div class="d-flex flex-column gap-2">
50                      @foreach($question->answers as $answer)
51                          <label class="answer-option p-3 rounded border d-flex align-items-center gap-3"
52                              style="cursor: pointer; transition: all 0.2s ease;">
53                              <input type="radio"
54                                  name="answers[{{ $question->id }}]"
55                                  value="{{ $answer->id }}"
56                                  class="form-check-input m-0"
57                                  required>
58                              <span>{{ $answer->answer_text }}</span>
59                          </label>
60                      @endforeach
61                  </div>
62              </div>
63          </div>
64      @endforeach

```

Figure 4.36: HTML5 Code Snippet – Quiz Question Template

Figure 4.36 presents a snippet of an HTML5 Blade template of the CyberSafe Learning Hub demonstrating the way HTML5 semantic elements and Laravel Blade instructions were employed to organize the quiz question interface and dynamically render it.

4.7.2.4 CSS

All the visual styling of the CyberSafe Learning Hub was done in CSS3 and SCSS (Sass). CSS3 has such tools as Flexbox, CSS Grid, transitions, animations, custom properties (variables), and media queries to design a modern and responsive layout that can be adjusted to the various sizes of the screens. SCSS, which was created using Vite offered features such as nesting, mix ins, variables and partials, which allowed creating maintainable and modular stylesheets. The styling featured bespoke colour themes of the cybersecurity brand identity, hover effects, gradient backgrounds, card-based designs, and responsive navigation.

```

261 .chat-fab {
262     width: 60px;
263     height: 60px;
264     border-radius: 50%;
265     background: linear-gradient(135deg, #10b981, #059669);
266     border: none;
267     color: white;
268     font-size: 28px;
269     cursor: pointer;
270     box-shadow: 0 4px 15px rgba(16, 185, 129, 0.4);
271     transition: all 0.3s ease;
272     display: flex;
273     align-items: center;
274     justify-content: center;
275 }
276
277 .chat-fab:hover {
278     transform: scale(1.1);
279     box-shadow: 0 6px 20px rgba(16, 185, 129, 0.5);
280 }

```

Figure 4.37: CSS Code Snippet – Chat Widget Styling

Figure 4.37 presents a CSS code snippet of the CyberSafe Learning Hub, which demonstrates how CSS3 properties (transitions, gradients, box shadows, hover effects, etc.) were utilized to design a modern and responsive visual design of the platform.

4.8 System Interface

The CyberSafe Learning Hub comprises several modules of interfaces; each module is user and purpose specific. The actual interfaces of the system by module are listed below.

4.8.1 Landing Page (Public)

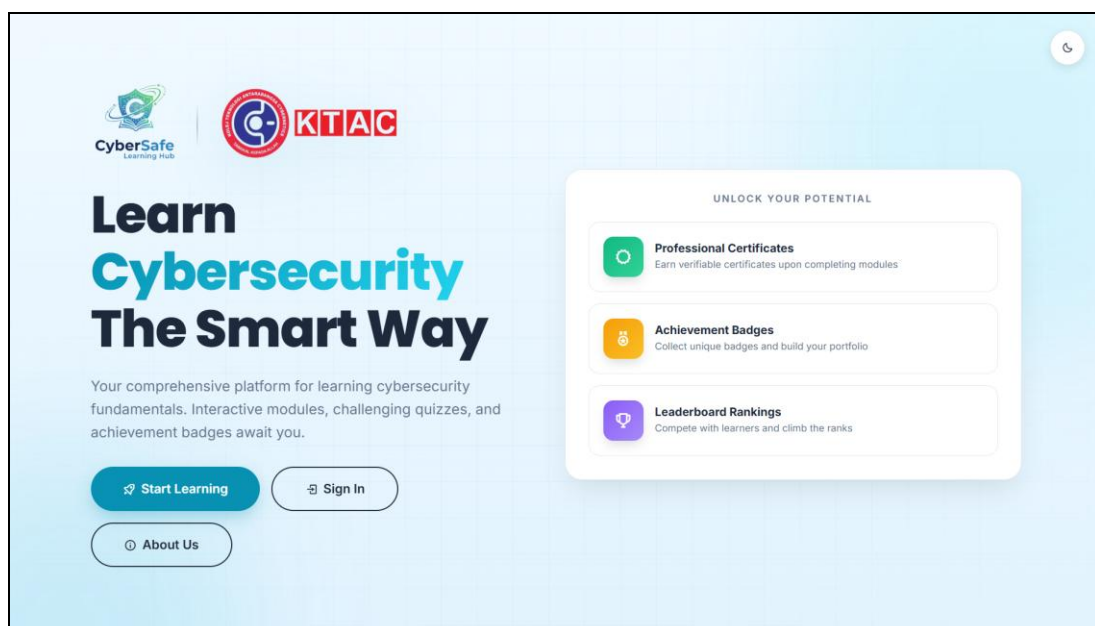


Figure 4.38: CyberSafe Learning Hub Landing Page (Desktop View)

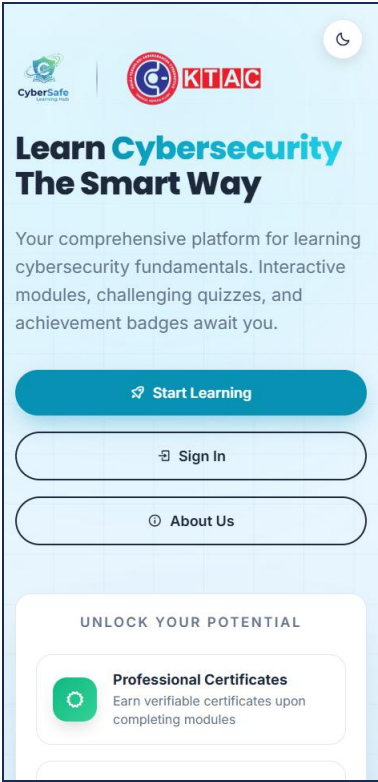


Figure 4.39: CyberSafe Learning Hub Landing Page (Mobile View)

Figure 4.38 and Figure 4.39 are the desktop and mobile view of the Landing Page of the CyberSafe Learning Hub respectively. The opening page is the key point of entry by all users. It has a hero section where the platform is presented, a section with available categories of cybersecurity and learning modules, and a call-to-action where users can sign in using Google OAuth or create an email account. The responsive design will provide the first impression as professional regardless of the size of the device.

4.8.2 Login Page

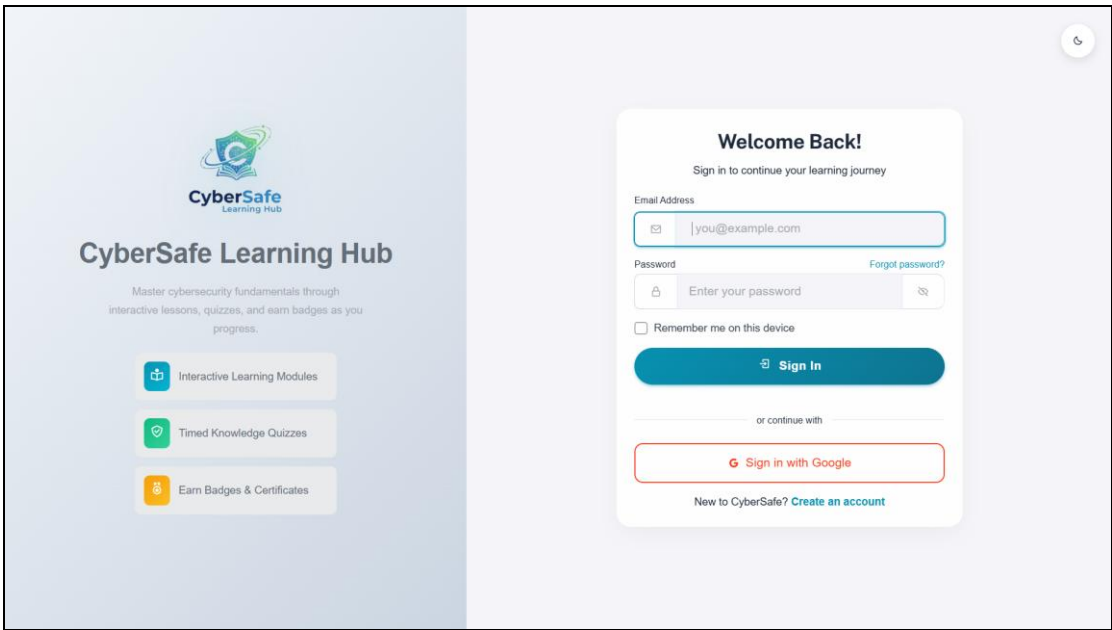


Figure 4.40: Login Page (Desktop View)

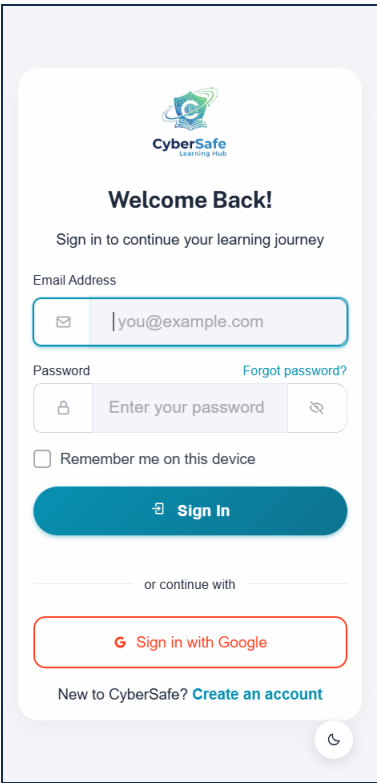


Figure 4.41: Login Page (Mobile View)

Figure 4.40 and Figure 4.41 depict the desktop and mobile view of the Login Page of the CyberSafe Learning Hub respectively. The registered users are authenticated by the use of email address and password in the login page. It also has a different sign-in method using Google OAuth 2.0 that enables users to use their current Google accounts to create a quick sign-in. New users who have not created an account can also have a connection to the registration page.

4.8.3 Register Page

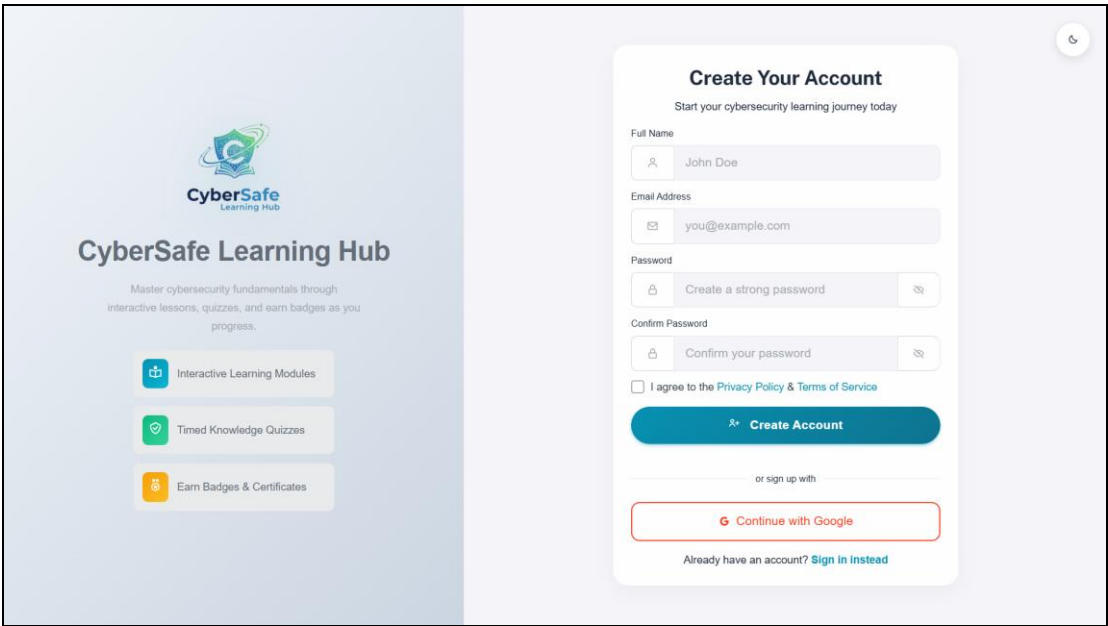


Figure 4.42: Register Page (Desktop View)

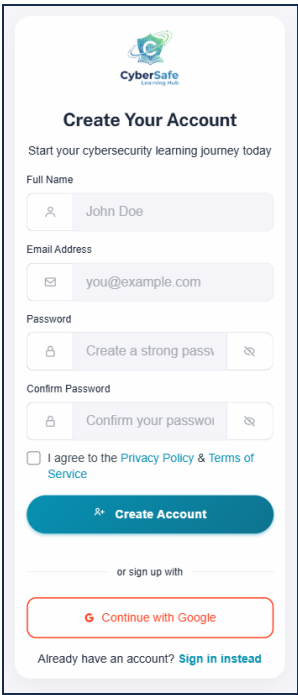
The image shows a mobile view of the 'Create Your Account' page. At the top is the CyberSafe Learning Hub logo. Below it, the title 'Create Your Account' is followed by the subtitle 'Start your cybersecurity learning journey today'. The form includes fields for 'Full Name' (with a person icon and the text 'John Doe'), 'Email Address' (with an envelope icon and the text 'you@example.com'), 'Password' (with a lock icon and the text 'Create a strong passv'), and 'Confirm Password' (with a lock icon and the text 'Confirm your passwoi'). There is a checkbox for 'I agree to the Privacy Policy & Terms of Service'. A large blue button labeled 'Create Account' is below the form. Below the button, it says 'or sign up with' followed by a red button labeled 'Continue with Google'. At the bottom, it says 'Already have an account? Sign in instead'.

Figure 4.43: Register Page (Mobile View)

The Register Page of the CyberSafe Learning Hub can be viewed in a desktop and mobile environment as shown in Figure 4.42 and Figure 4.43 respectively. New users are able to create an account on the registration page, where they fill their name, email address, and password. There is also a Google sign-up option to create an account faster. After successful registration, the user is automatically given the student role and redirected to the onboarding flow.

4.8.4 Google OAuth Login

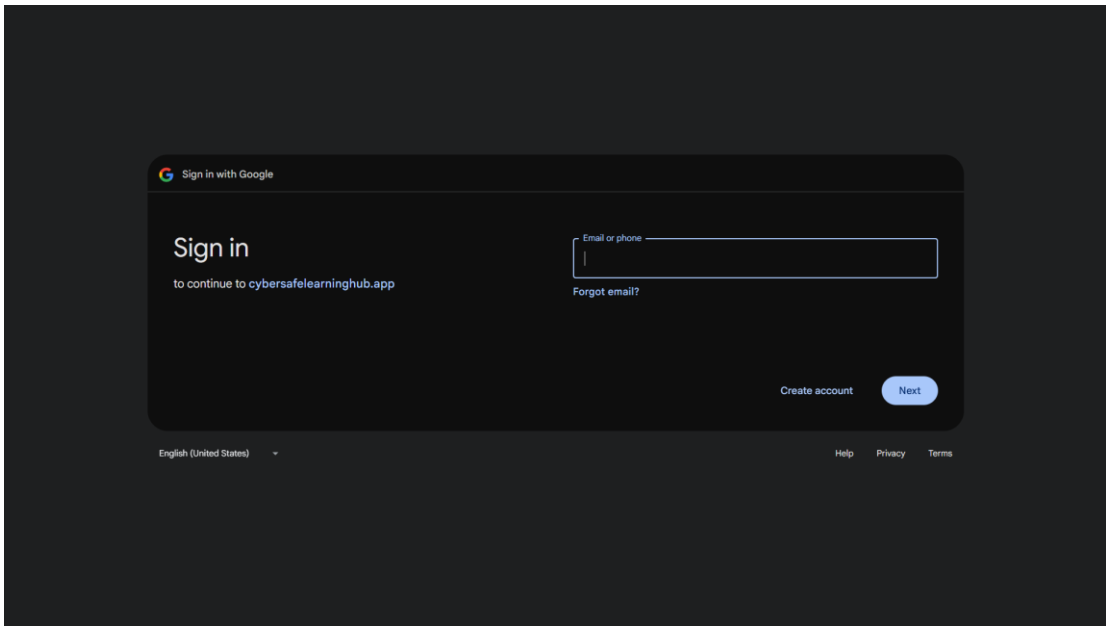
The image shows a desktop view of the Google OAuth 2.0 Authentication screen. It has a dark background. At the top, it says 'Sign in with Google'. Below that, the text 'Sign in' is followed by 'to continue to cybersafelearninghub.app'. There is a text input field for 'Email or phone' with a placeholder 'I'. Below the input field is a link 'Forgot email?'. At the bottom right, there are two buttons: 'Create account' and 'Next'. At the bottom left, it says 'English (United States)' with a dropdown arrow. At the bottom right, there are links for 'Help', 'Privacy', and 'Terms'.

Figure 4.44: Google OAuth 2.0 Authentication Screen (Desktop View)

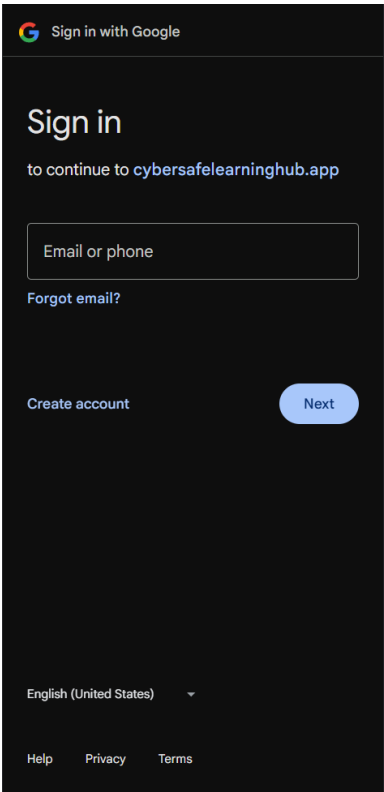


Figure 4.45: Google OAuth 2.0 Authentication Screen (Mobile View)

Figure 4.44 and Figure 4.45 depict the Google OAuth 2.0 authentication interface in desktop and mobile view respectively. This screen is shown when the users choose to sign in with Google, which allows them to have a safe, smooth sign-in experience as Google authentication infrastructure is used through Laravel Socialite.

4.8.5 Student Dashboard

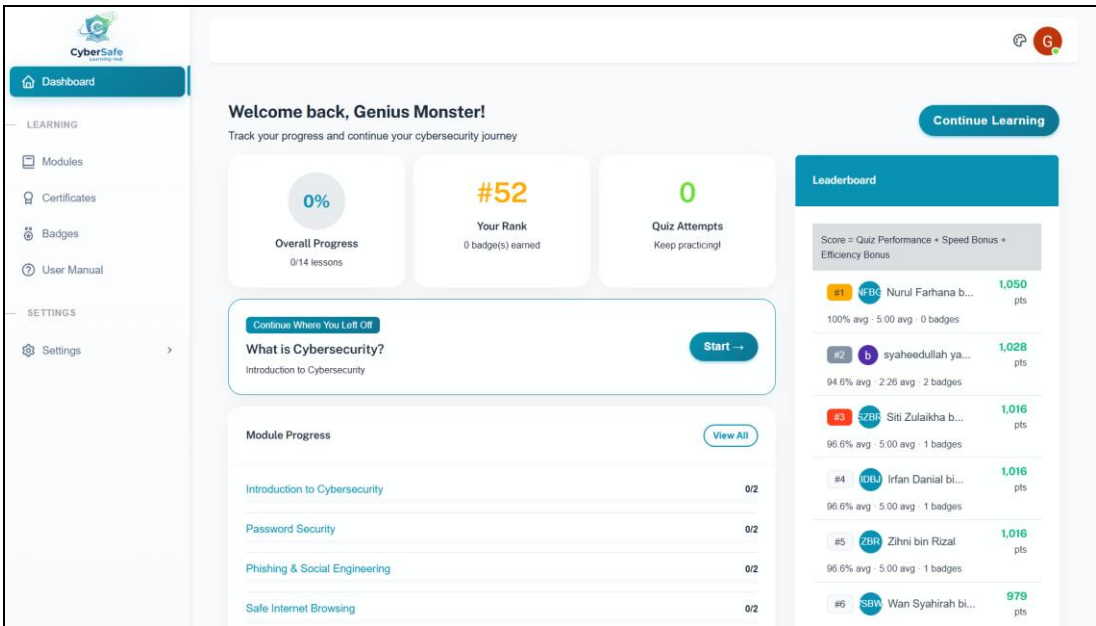


Figure 4.46: Student Dashboard (Desktop View)

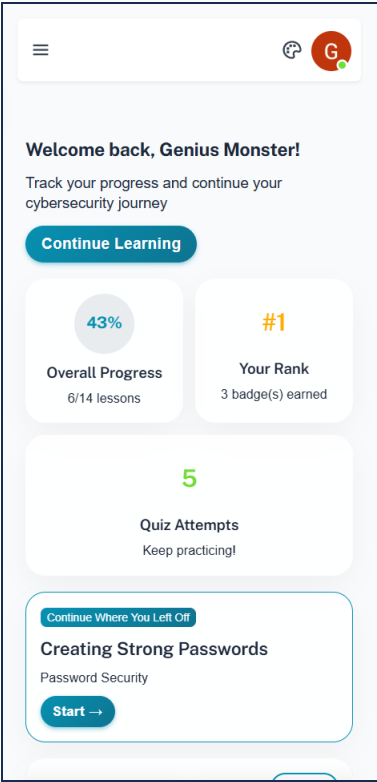


Figure 4.47: Student Dashboard (Mobile View)

Figure 4.46 and Figure 4.47 are the views of the Student Dashboard on desktop and mobile respectively. The dashboard shows the personalised learning summary of the student such as the modules enrolled and progress statistics, recently awarded badges and certificates, achievement notifications, and the overall performance.

4.8.6 Module Listing (Student View)

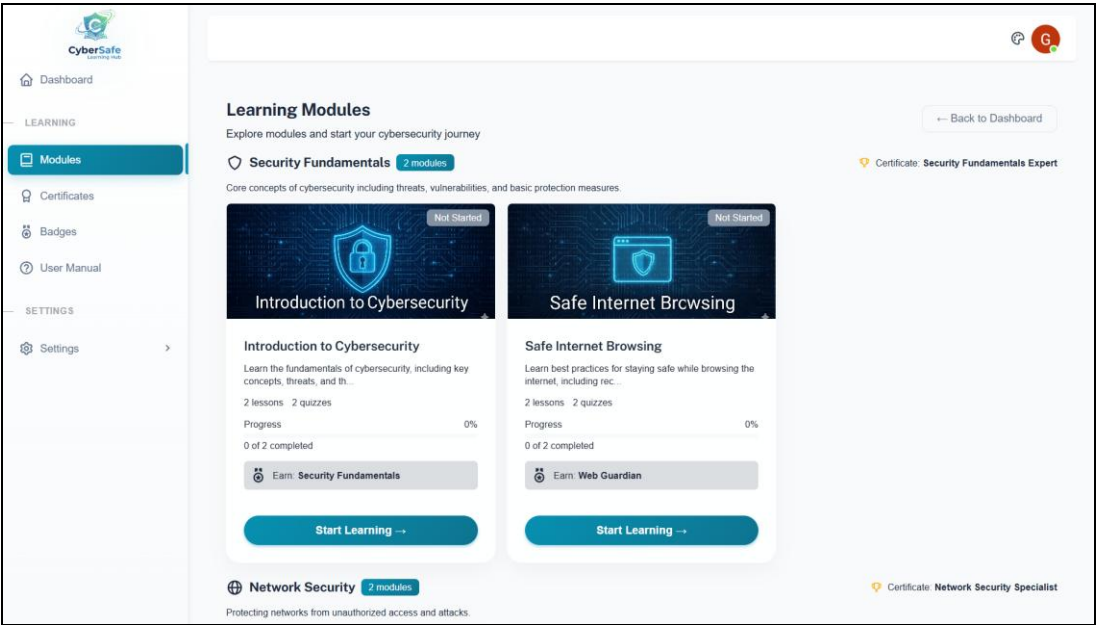


Figure 4.48: Student Module Listing Page (Desktop View)

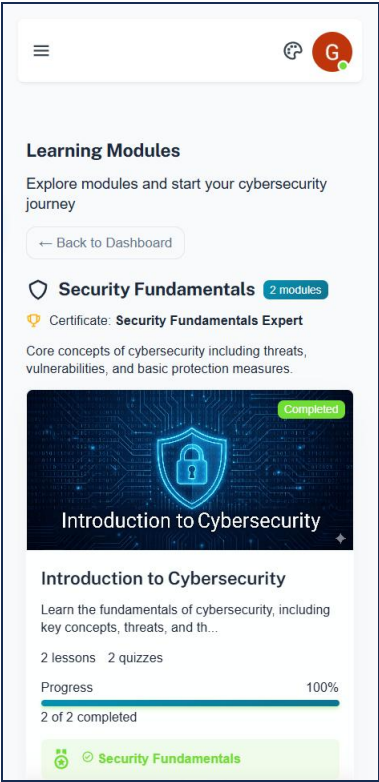


Figure 4.49: Student Module Listing Page (Mobile View)

Figure 4.48 and Figure 4.49 display the Module Listing page in desktop and mobile respectively. All the existing cybersecurity learning modules can be found on the page and classified according to category. The module cards display the title, description, lessons taken and the progress made by the student.

4.8.7 Module Detail with Lesson List (Student View)

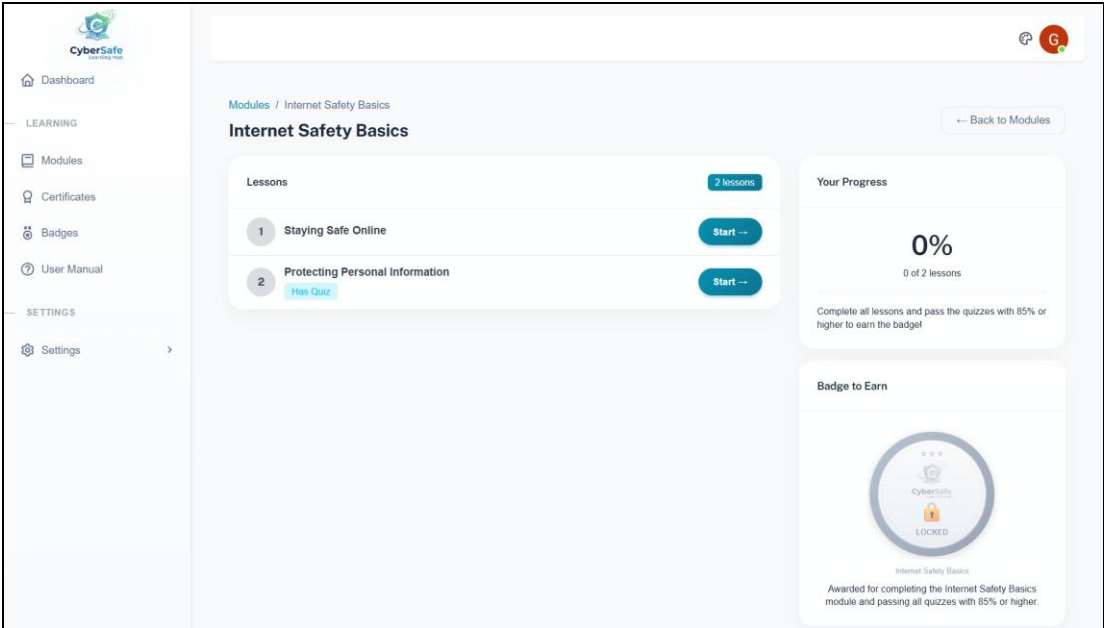


Figure 4.50: Module Detail Page with Lesson List (Desktop View)

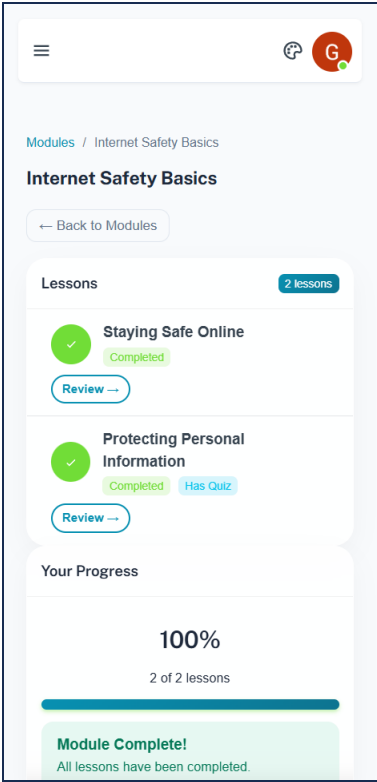


Figure 4.51: Module Detail Page with Lesson List (Mobile View)

Figure 4.50 and Figure 4.51 depict the Module Detail page in desktop and mobile format respectively. Learners are able to view the lesson titles, lesson completion, and access individual lessons. There is also a module completion percentage displayed on the page.

4.8.8 Lesson Content View (Student View)

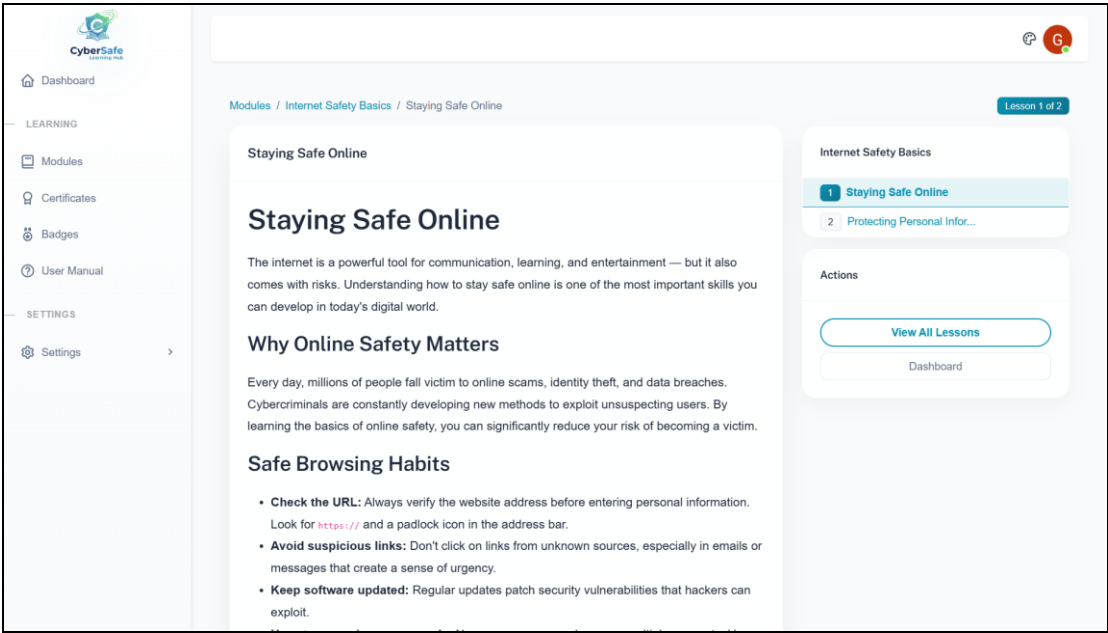


Figure 4.52: Lesson Content View (Desktop View)

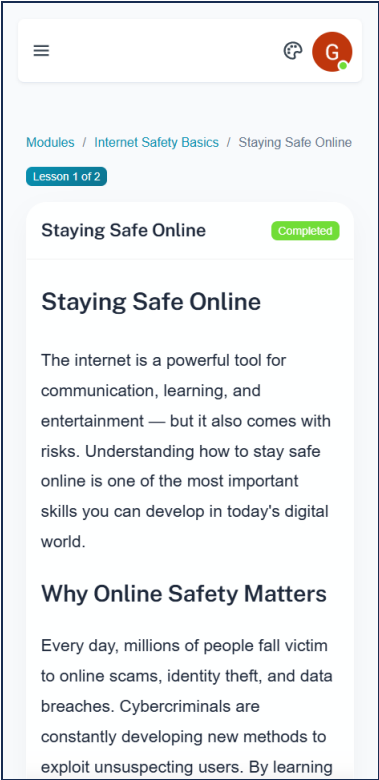


Figure 4.53: Lesson Content View (Mobile View)

Figures 4.52 and Figure 4.53 represent the Lesson Content View in desktop and mobile respectively. The lesson contents blocks (text and images) are arranged in sequence on the page and a discussion and comments section is provided beneath. Students have a Mark as Complete button that helps them keep track of their progress.

4.8.9 Quiz Interface (Student View)

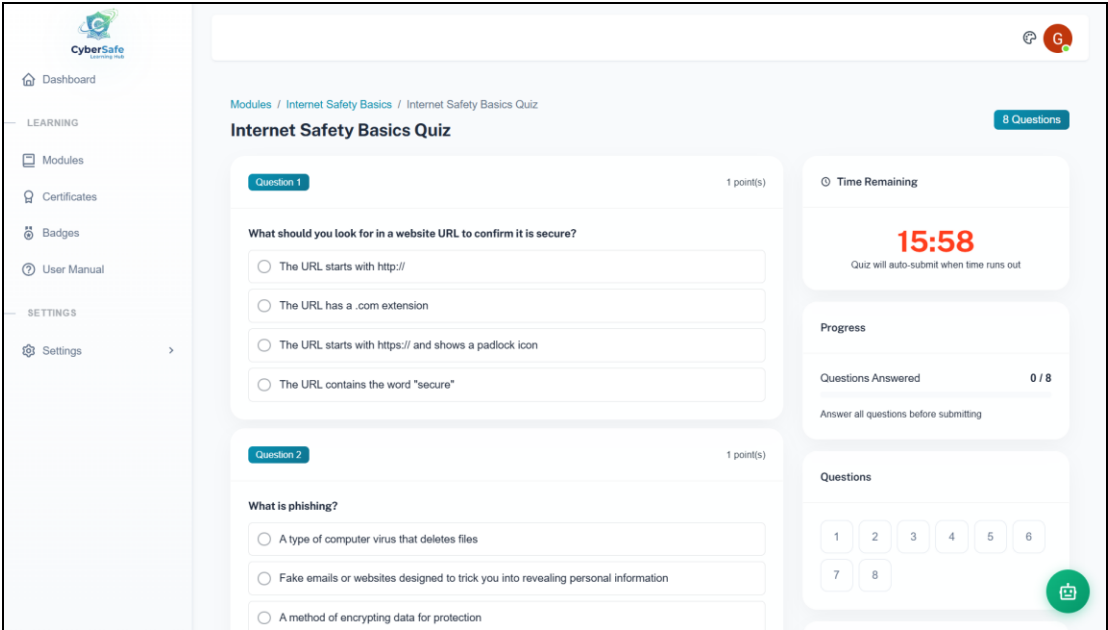


Figure 4.54: Quiz Interface (Desktop View)

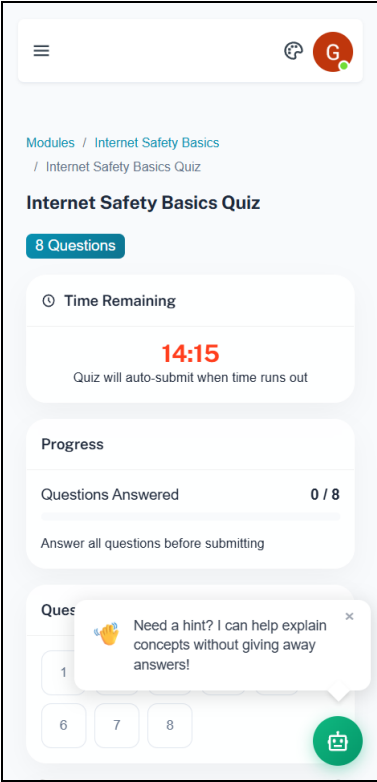


Figure 4.55: Quiz Interface (Mobile View)

Figure 4.54 and Figure 4.55 are the desktop and the mobile Quiz Interface, respectively. It has a countdown timer, navigation of the questions, a button of an AI Chatbot assistant to clarify the concept and submit button. A pass of 85% and above is required to pass the quiz.

4.8.10 Quiz Result

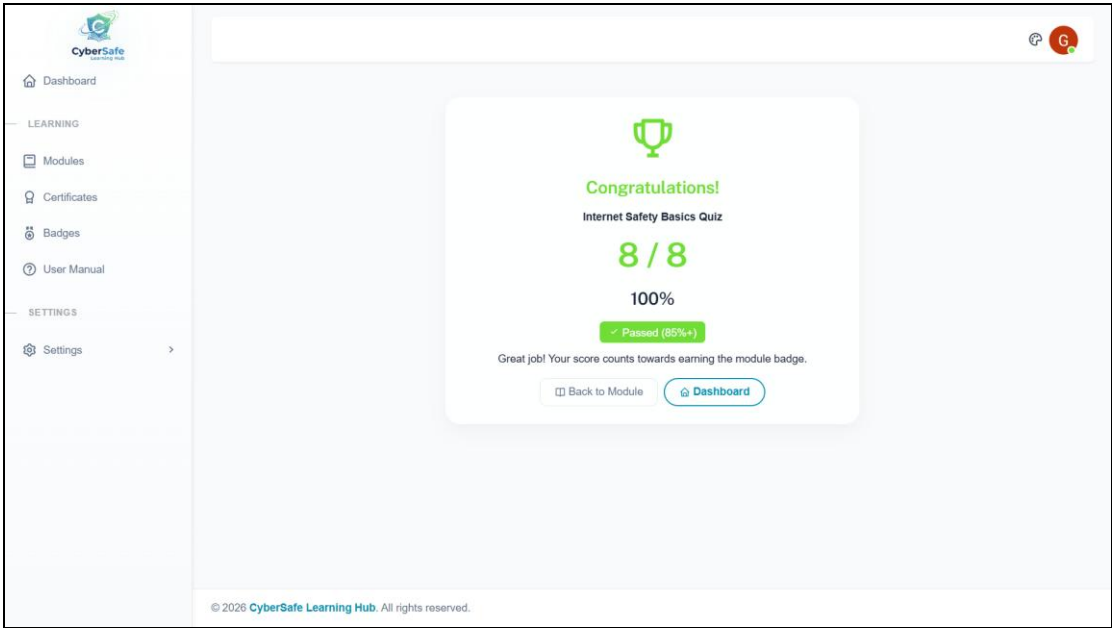


Figure 4.56: Quiz Result Page (Desktop View)

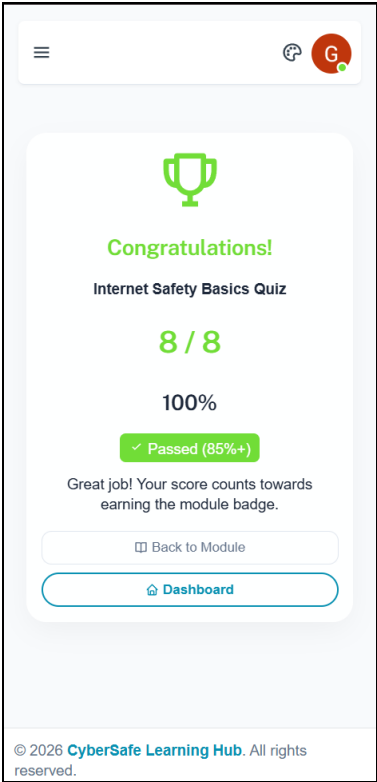


Figure 4.57: Quiz Result Page (Mobile View)

The Quiz Result page is displayed in desktop and mobile view in Figure 4.56 and Figure 4.57 respectively. It indicates the score of the student, percentage and pass/fail.

4.8.11 AI Chatbot (Quiz Page)

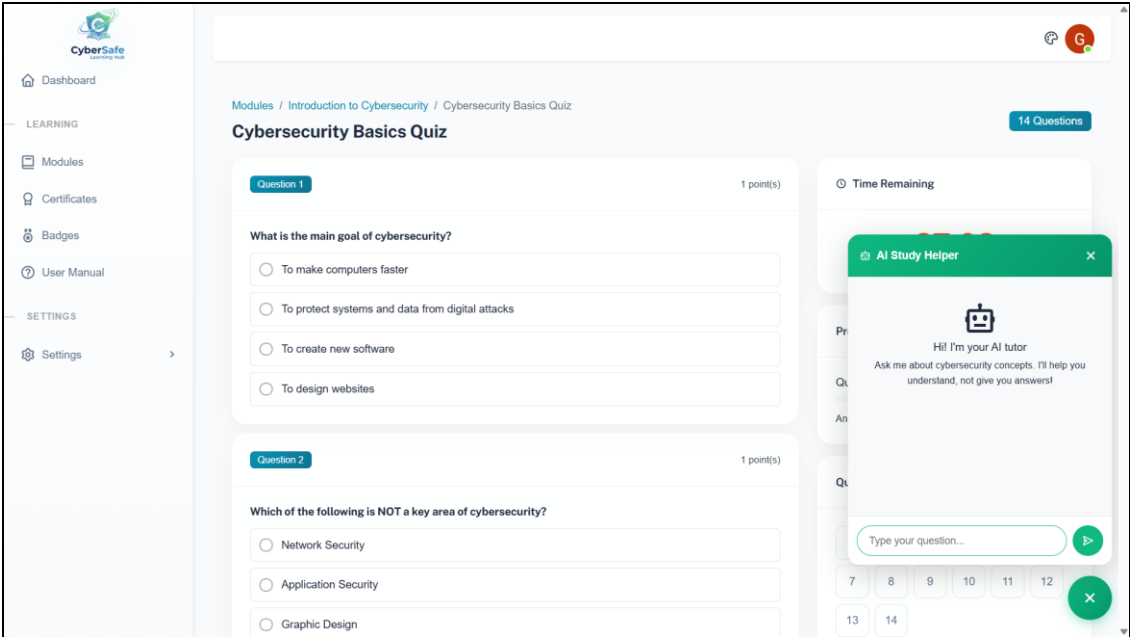


Figure 4.58: AI Chatbot – Cybersecurity Tutor Assistant (Desktop View)

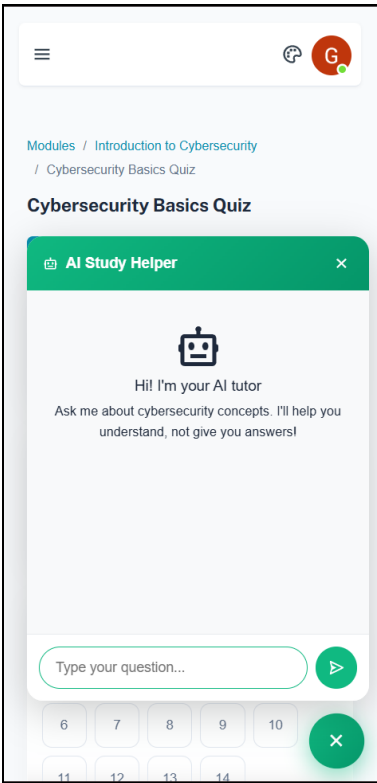


Figure 4.59: AI Chatbot – Cybersecurity Tutor Assistant (Mobile View)

Figure 4.58 and Figure 4.59 present the AI Chatbot assistant on the desktop and mobile platforms respectively. It is run by Llama 3. 3-70B by Groq to enable students to ask questions regarding cybersecurity when taking quizzes. The chatbot justifies the concepts and gives hints, but does not answer.

4.8.12 Badges Page (Student View)

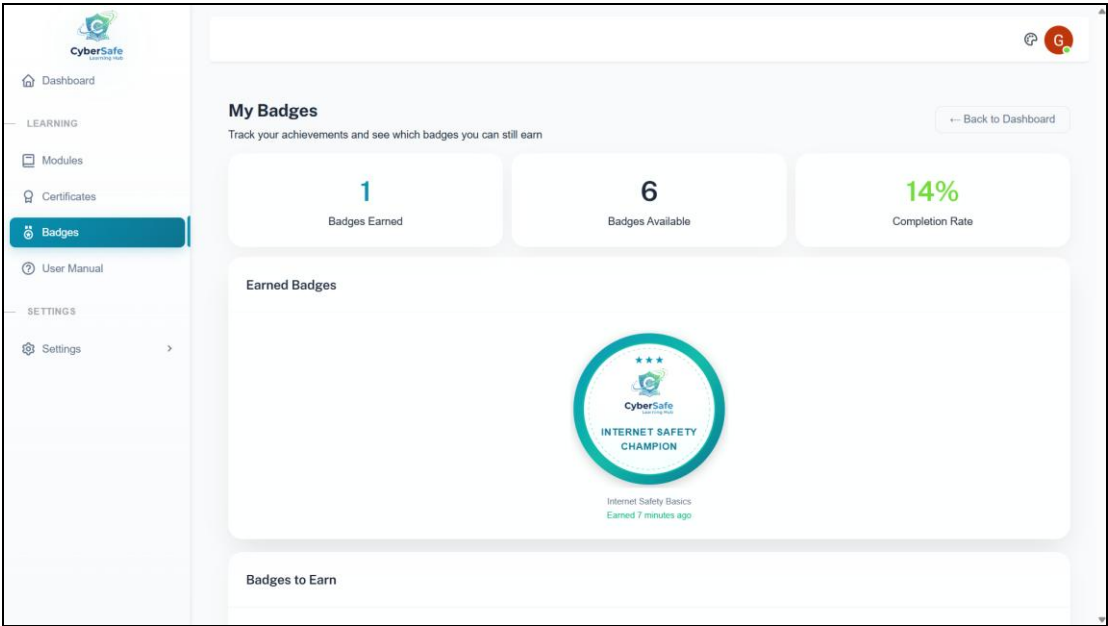


Figure 4.60: Student Badges Page (Desktop View)

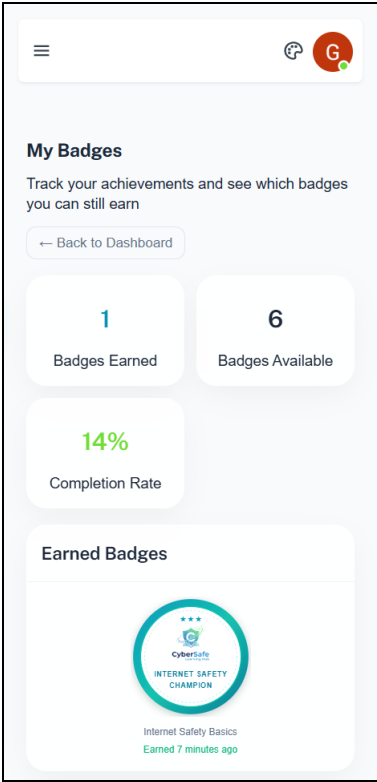


Figure 4.61: Student Badges Page (Mobile View)

Figure 4.60 and Figure 4.61 depict Badges page using desktop and mobile device respectively. Badges are automatically earned when a student passes all quizzes in a module with 85 percent or above marks. Every badge is a symbol of the competence in this or that cybersecurity module.

4.8.13 Certificates Page (Student View)

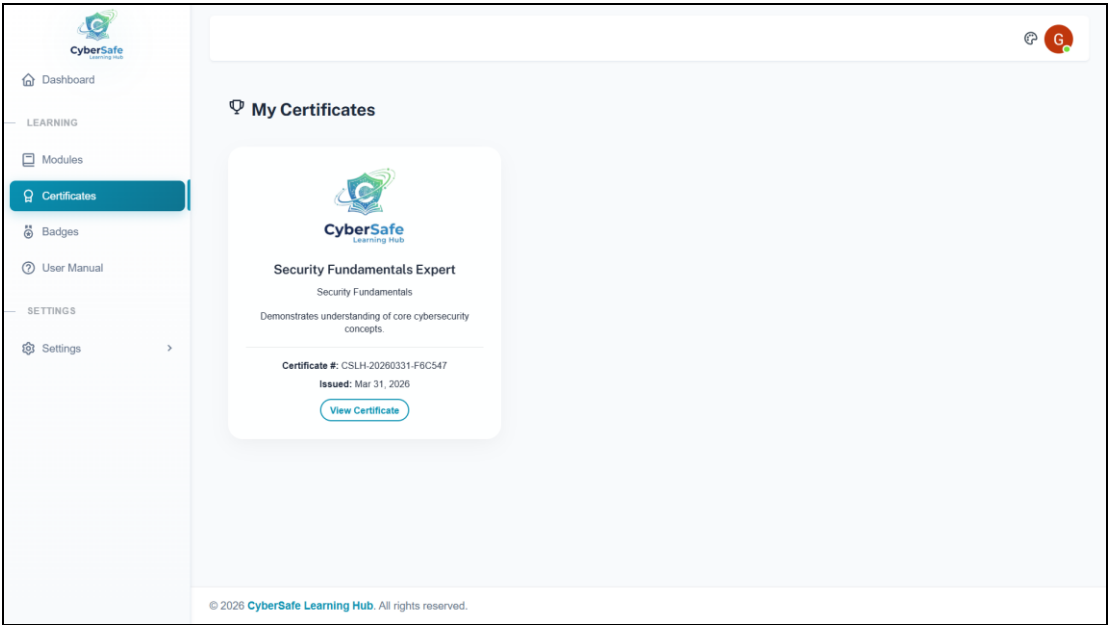


Figure 4.62: Student Certificates Page (Desktop View)



Figure 4.63: Student Certificates Page (Mobile View)

Figures 4.62 and 4.63 depict Certificates page on desktop and mobile respectively. Certificates would be automatically granted when one completes all the modules and passes all the quizzes in a category. Every certificate has its distinct certificate number, and date of issue.

4.8.14 Certificate Detail View (Student View)

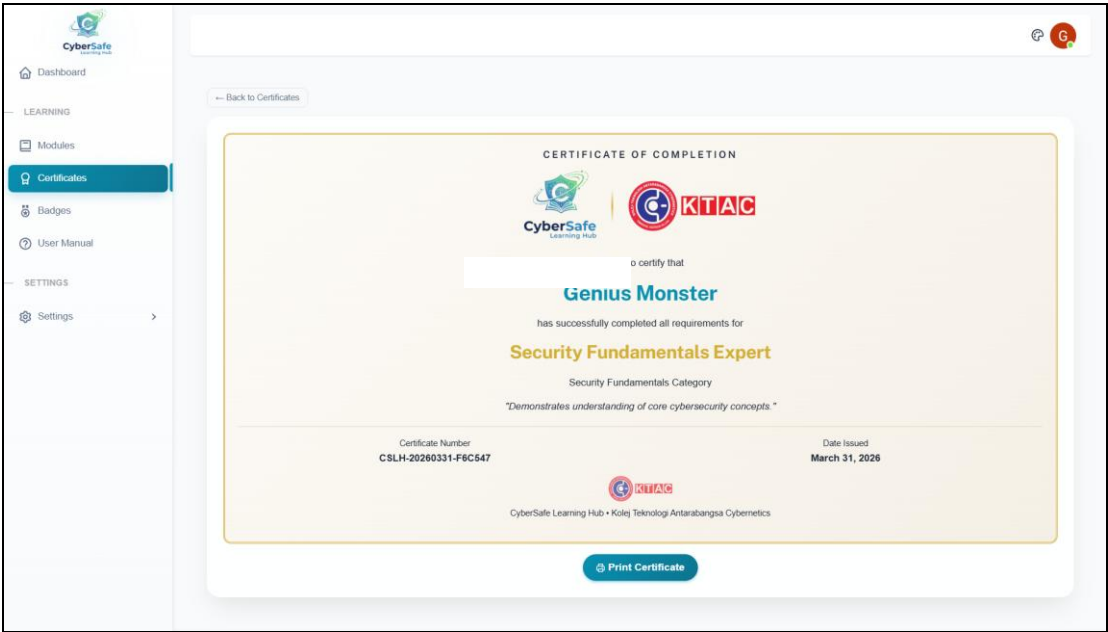


Figure 4.64: Certificate Detail View (Desktop View)

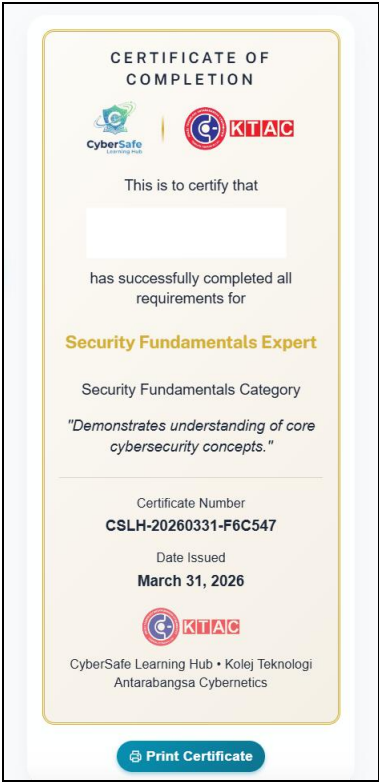


Figure 4.65: Certificate Detail View (Mobile View)

Figure 4.64 and Figure 4.65 present the Certificate Detail page at desktop and mobile respectively. Students are able to see the entire certificate with their name, category that they have completed, certificate number and date of issuance. The certificate is available in PDF format, that can be downloaded as personal records.

4.8.15 User Manual (Student View)

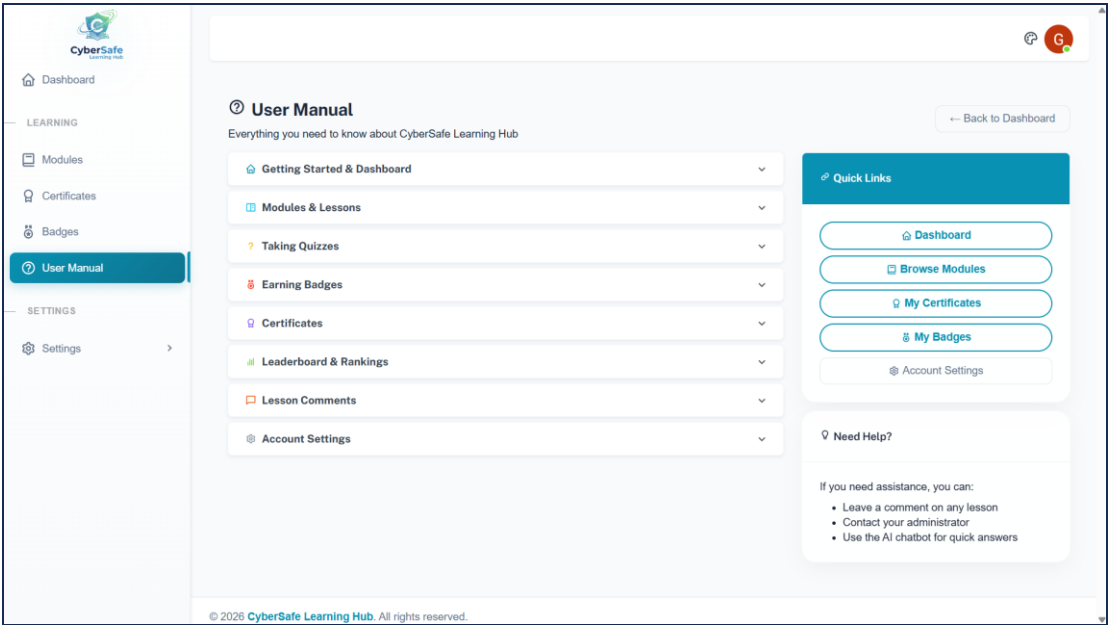


Figure 4.66: Student User Manual Page (Desktop View)

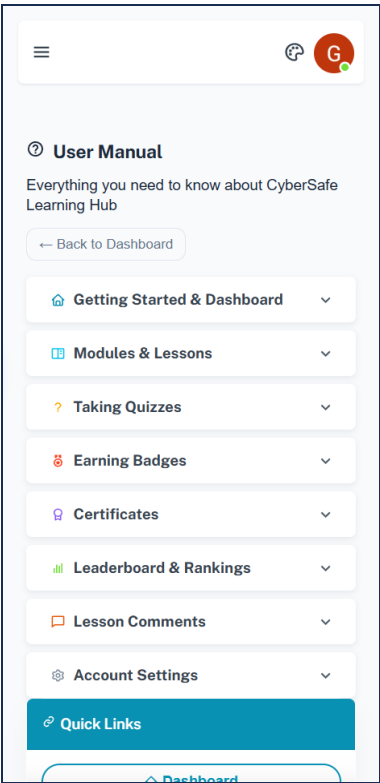


Figure 4.67: Student User Manual Page (Mobile View)

Figure 4.66 and Figure 4.67 present the User Manual page of desktop and mobile versions, respectively. The present page offers the students a step-by-step instruction on how to utilize the platform, including registering, working through modules and lessons, quizzes, and badges and certificates.

4.8.16 Admin Dashboard

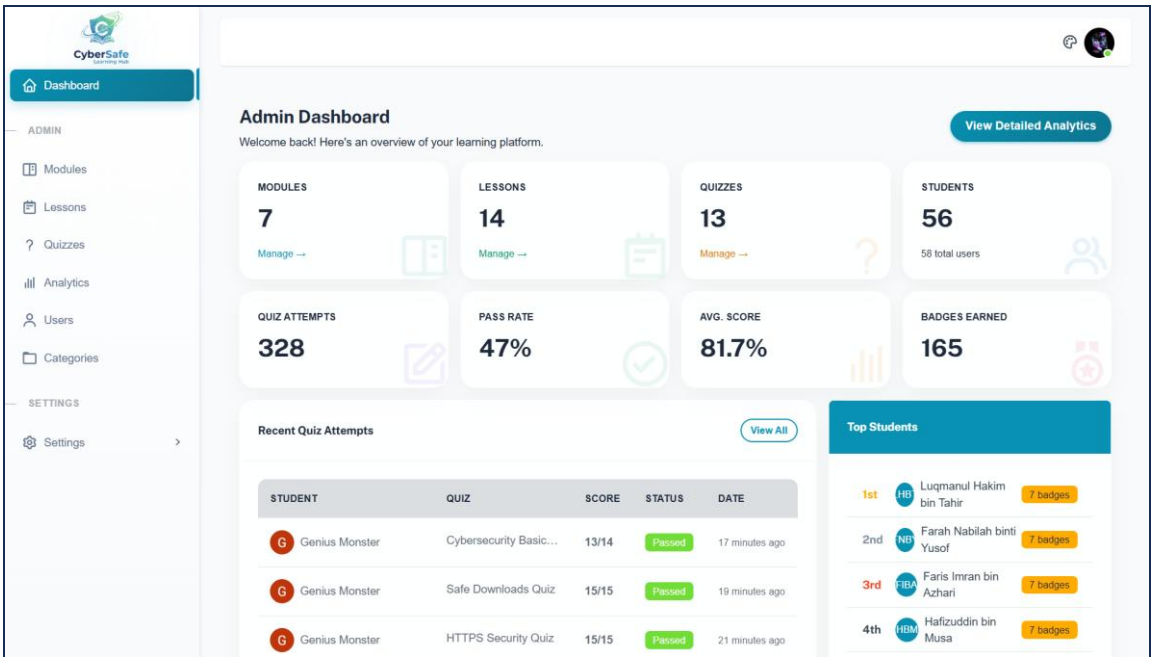


Figure 4.68: Admin Dashboard

The Admin Dashboard is displayed in figure 4.68. It shows the important platform statistics such as total number of registered students, total number of modules, total lessons, and quizzes, and the real time analytics charts that show how students are engaging, how many quizzes are being completed and the performance measures.

4.8.17 Admin Category Management

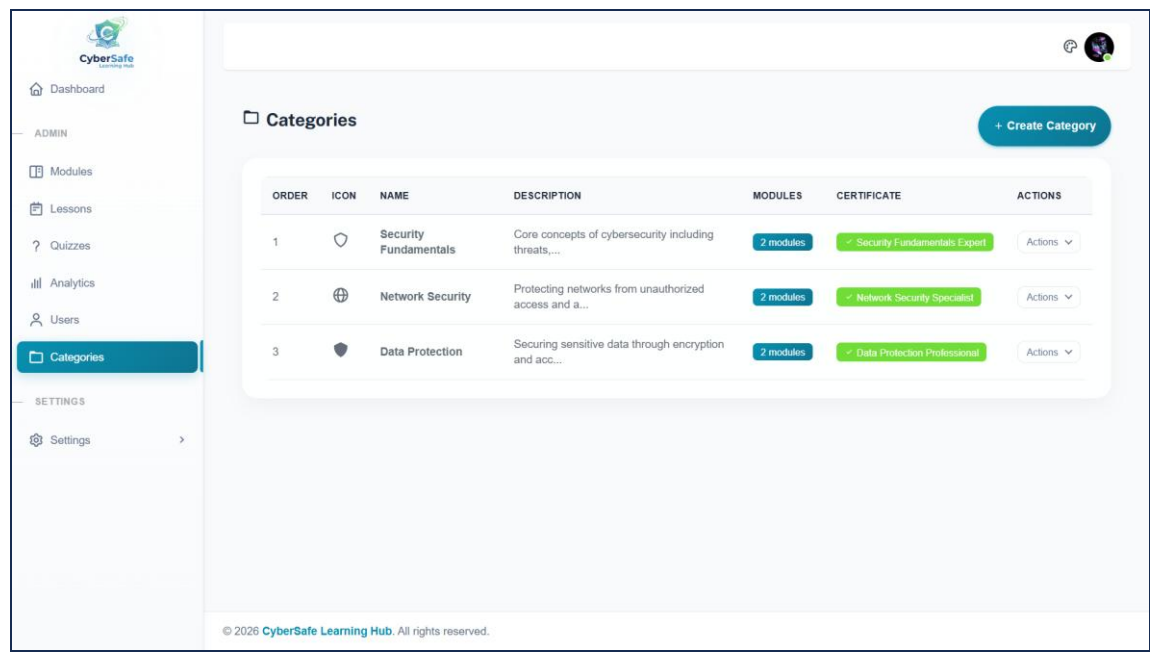


Figure 4.69: Admin Category Management

Figure 4.69 illustrates the interface of Admin Category Management. Administrators are allowed to see, add and remove cybersecurity categories that act as the highest grouping of learning modules. Each category is associated with a certificate that students obtain after passing all the modules in it.

4.8.18 Admin Create / Edit Category

The screenshot shows the 'Create Category' form in the CyberSafe Learning Hub. The left sidebar contains navigation links: Dashboard, ADMIN (Modules, Lessons, Quizzes, Analytics, Users, Categories), and SETTINGS (Settings). The main content area is titled 'Create Category' and includes a 'Back to Categories' link. The form fields are: 'Category Name *' (text input), 'Description' (text area), 'Icon' (dropdown with '+ Select Icon'), 'Display Order' (text input with value '0'), 'Create Certificate' (toggle switch), and a checkbox for 'Students who complete all modules in this category will earn this certificate'. Below the checkbox are 'Certificate Name' and 'Certificate Description' (text area) fields. The form concludes with 'Create Category' and 'Cancel' buttons.

Figure 4.70: Admin Category Create Form

Figure 4.70 shows the Admin Category Create form. The administrators complete the category name, description and icon and the system stores to the database to be displayed in the student module listing page.

4.8.19 Admin Module Management

The screenshot displays the 'Modules' management page. The left sidebar is identical to the previous figure. The main content area is titled 'Modules' and features a '+ Create Module' button. It contains a grid of six module cards. Each card includes an icon, a title, a brief description, a topic tag (e.g., 'Internet Saf.', 'Social Media', 'Privacy Prot.'), a list of associated topics, and counts for lessons and quizzes. At the bottom of each card are 'Edit' and delete icons. The modules shown are: Internet Safety Basics, Personal Data & Social Media Safety, Data Privacy & Protection, Phishing & Social Engineering, Safe Internet Browsing, and Introduction to Cybersecurity.

Figure 4.71: Admin Module Management

Figure 4.71 shows the Admin Module Management listing page. It displays all learning modules organised by category, with options to create new modules, edit existing ones, manage lessons within each module, and delete modules.

4.8.20 Admin Create / Edit Module

The screenshot shows the 'Edit Module: Internet Safety Basics' form. The left sidebar contains navigation links: Dashboard, ADMIN (Modules, Lessons, Quizzes, Analytics, Users, Categories), and SETTINGS (Settings). The main form area is divided into three sections: 'Module Details', 'Badge Settings', and 'Module Stats'. The 'Module Details' section includes fields for 'Module Title' (Internet Safety Basics), 'Description' (Learn the essential practices to stay safe online...), 'Cover Image' (Choose File, No file chosen), and 'Category' (No Category). The 'Badge Settings' section includes 'Badge Name' (Internet Safety Champion) and 'Badge Description' (Awarded for completing the Internet Safety Basics module...). The 'Module Stats' sidebar shows 'Lessons: 2', 'Quizzes: 1', and 'Badges Earned: 12'. At the bottom of the form are 'Update Module' and 'Cancel' buttons.

Figure 4.72: Admin Module Create / Edit Form

Figure 4.72 shows the Admin Module Create/Edit form. Administrators provide the module title, description, select its parent category, and upload a cover image. The module is then published and made available to students in the module listing.

4.8.21 Admin Lesson Management

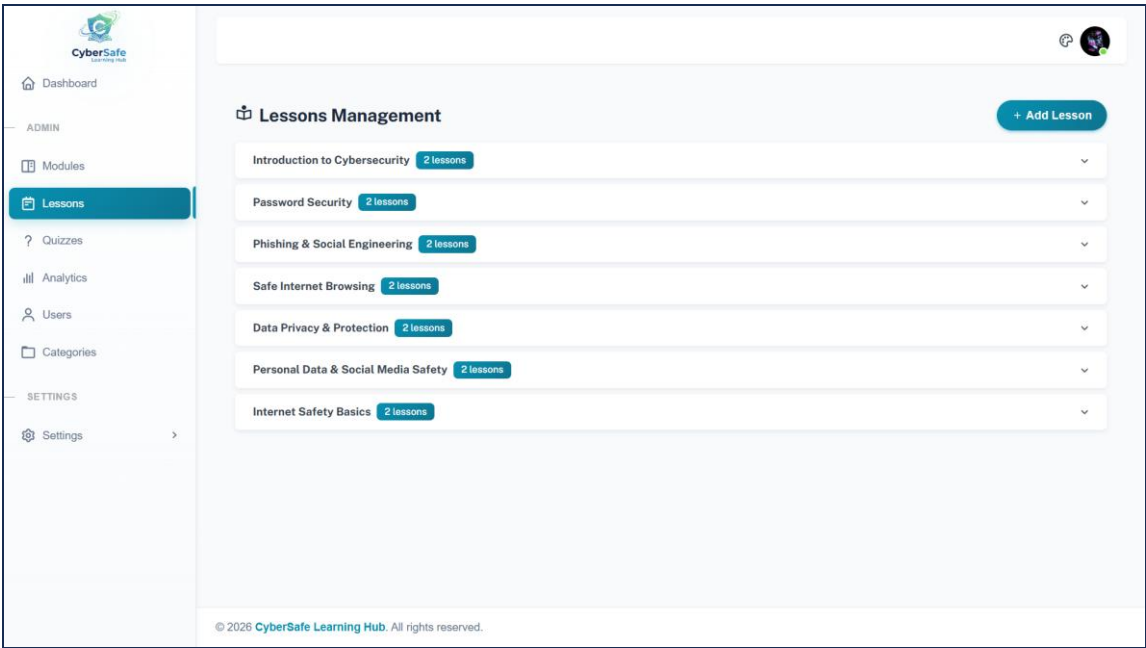


Figure 4.73: Admin Lesson Management

Figure 4.73 shows the Admin Lesson Management listing page. It lists all lessons belonging to a module, showing their title, position order, and whether a quiz is attached. Administrators can create new lessons, reorder them, edit content, or delete them.

4.8.22 Admin Lesson Content Editor

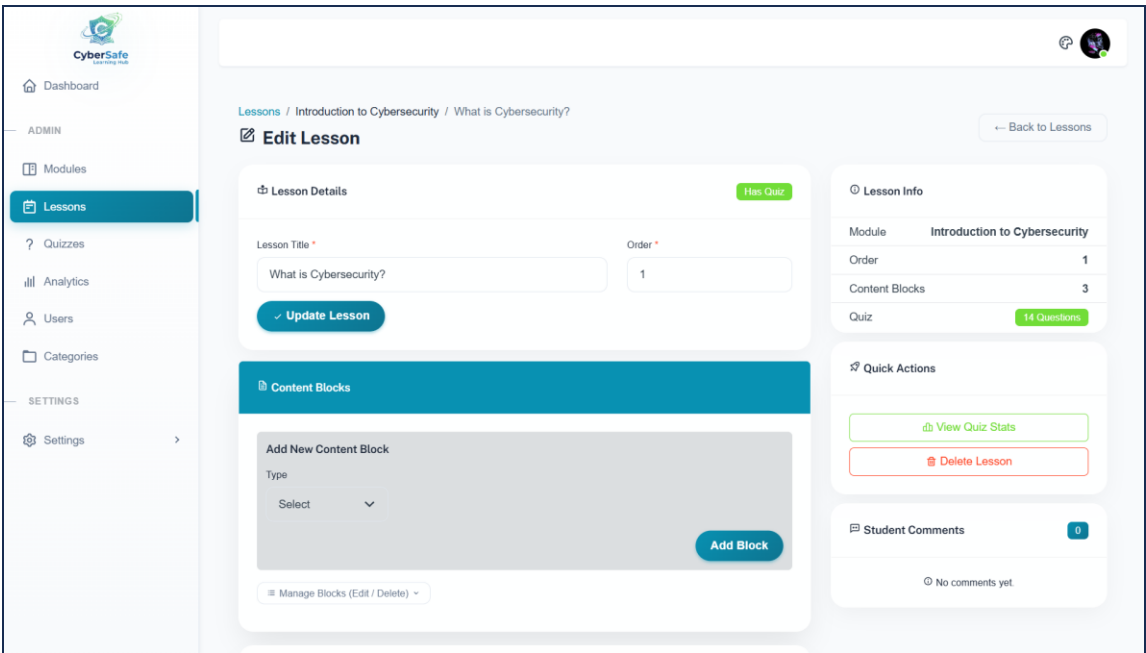
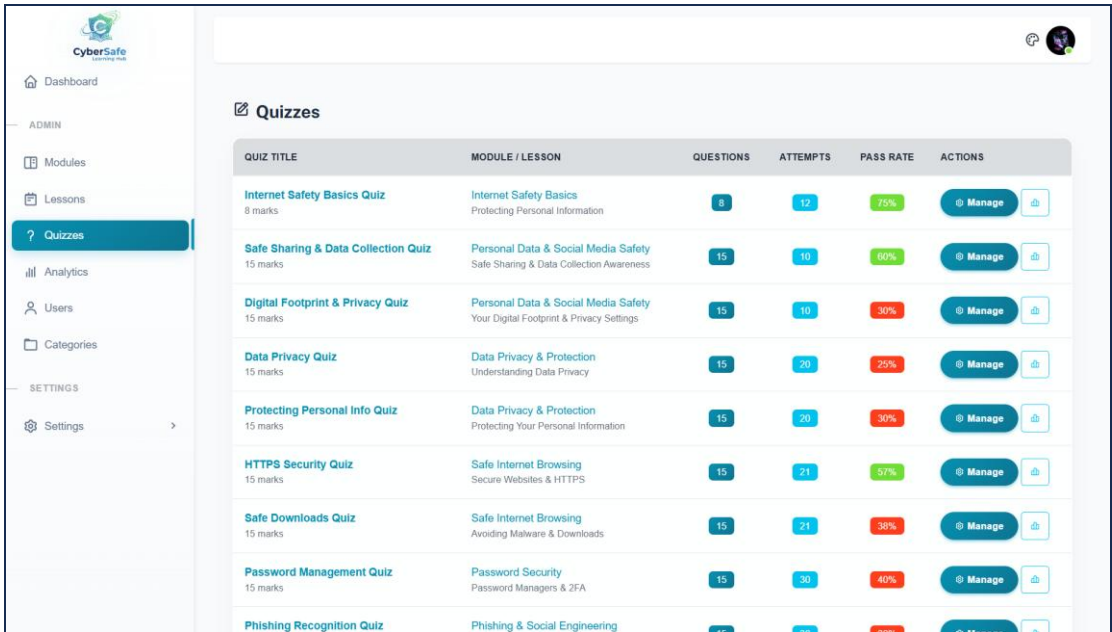


Figure 4.74: Admin Lesson Content Editor

Figure 4.74 shows the Admin Lesson Content Editor. This interface allows administrators to build lesson pages by adding, arranging, and editing content blocks. Each block can be a text paragraph or an image, with support for width and alignment customisation. Blocks can be reordered using drag-and-drop.

4.8.23 Admin Quiz Management



QUIZ TITLE	MODULE / LESSON	QUESTIONS	ATTEMPTS	PASS RATE	ACTIONS
Internet Safety Basics Quiz 8 marks	Internet Safety Basics Protecting Personal Information	8	12	75%	Manage Add
Safe Sharing & Data Collection Quiz 15 marks	Personal Data & Social Media Safety Safe Sharing & Data Collection Awareness	15	10	60%	Manage Add
Digital Footprint & Privacy Quiz 15 marks	Personal Data & Social Media Safety Your Digital Footprint & Privacy Settings	15	10	30%	Manage Add
Data Privacy Quiz 15 marks	Data Privacy & Protection Understanding Data Privacy	15	20	25%	Manage Add
Protecting Personal Info Quiz 15 marks	Data Privacy & Protection Protecting Your Personal Information	15	20	30%	Manage Add
HTTPS Security Quiz 15 marks	Safe Internet Browsing Secure Websites & HTTPS	15	21	57%	Manage Add
Safe Downloads Quiz 15 marks	Safe Internet Browsing Avoiding Malware & Downloads	15	21	38%	Manage Add
Password Management Quiz 15 marks	Password Security Password Managers & 2FA	15	30	40%	Manage Add
Phishing Recognition Quiz	Phishing & Social Engineering				Manage Add

Figure 4.75: Admin Quiz Management

Figure 4.75 represents the listing page of the Admin Quiz Management. It shows all quizzes within the system, each one of which is associated with a particular lesson, and the quantity of questions and choices available to view, edit, or remove the quiz.

4.8.24 Admin Quiz Question Management

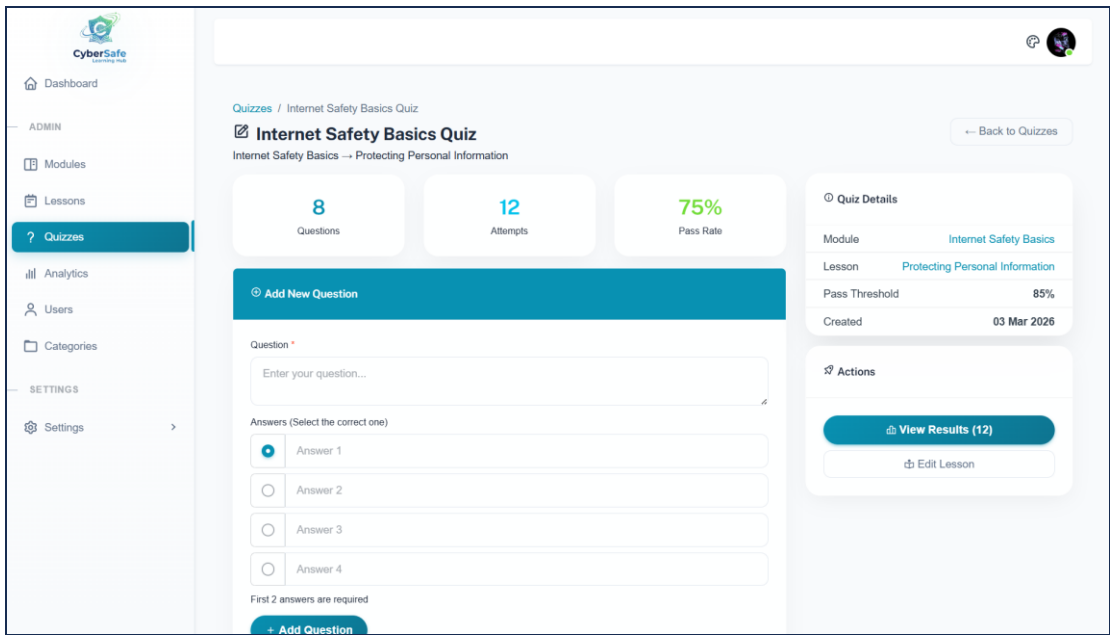


Figure 4.76: Admin Quiz Detail and Question Management

Figure 4.76 represents the Admin Quiz Detail page where administrators can control individual questions of a quiz. Administrators are also able to add multiple-choice questions, give options of answers, tick the right answer, and remove questions. Every quiz is associated with a single lesson and has a pass rate of 85%.

4.8.25 Admin Analytics Dashboard

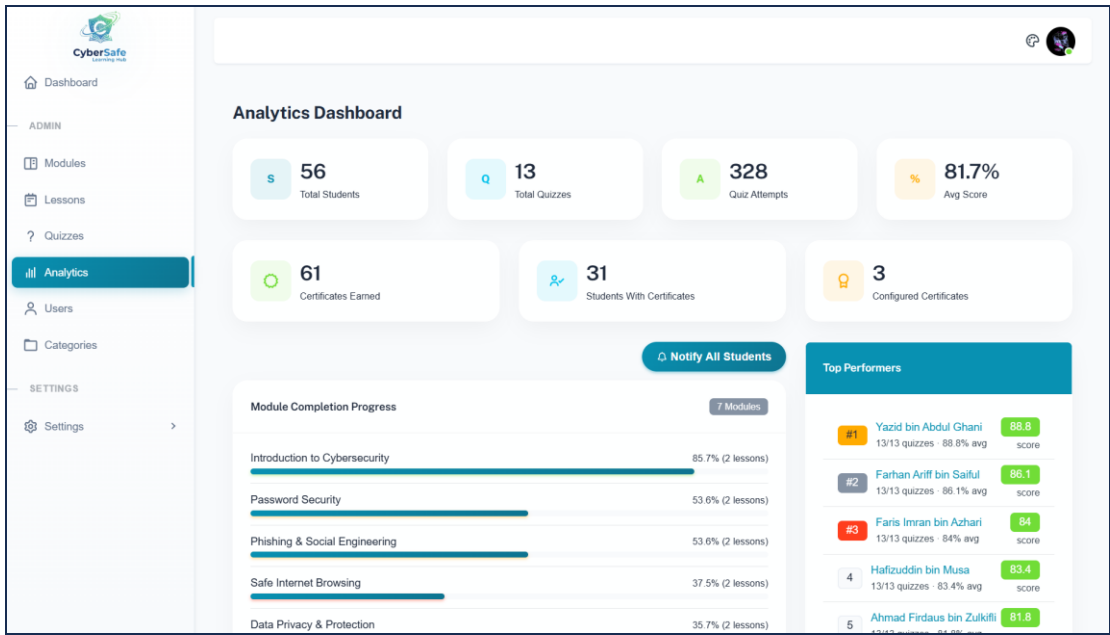


Figure 4.77: Admin Analytics Dashboard

In Figure 4.77, the overview page of the Admin Analytics is depicted. It gives a platform-wide overview of performance of students such as quiz completion rate, average score, best performing students and statistics of module engagement in the form of charts and tables.

4.8.26 Admin Student Analytics Drill-Down

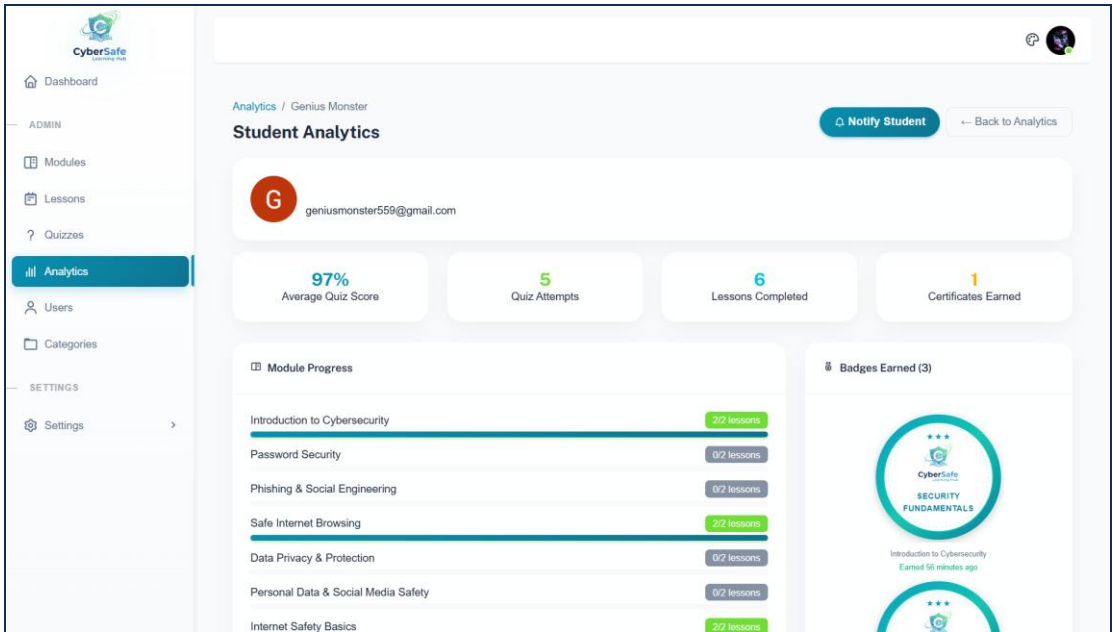


Figure 4.78: Admin Student Analytics – Individual Student View

Figure 4.78 displays the Admin Student Analytics drill-down page. Administrators may choose a single student and look at his/her entire learning profile, such as lessons attended, attempts and grades in quizzes per lesson, badges and certificates received, and total progress achieved in all modules.

4.8.27 Admin User Management

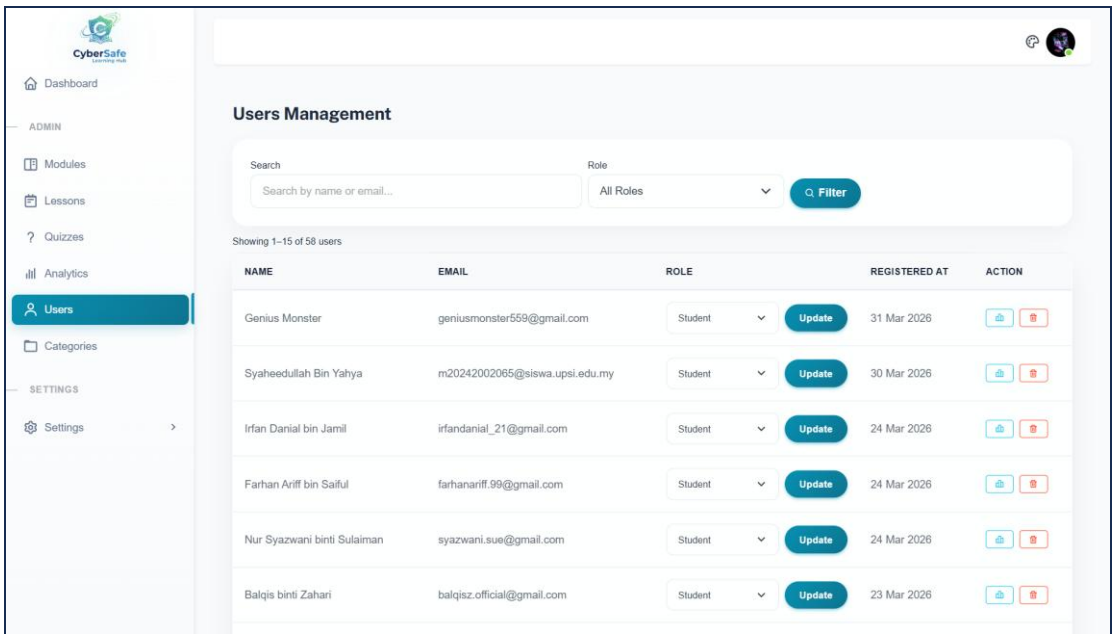


Figure 4.79: Admin User Management

Figure 4.79 represents the listing page of Admin User Management. It shows all the registered users including their name, email, role and date of registration. The administrators are allowed to search and filter users, promote or demote roles, edit user profile, or delete accounts.

4.9 Significant Functions

Security has been one of the priorities used in developing the CyberSafe Learning Hub. As the system is handling sensitive user data such as personal credentials, learning progress, quizzes performance and records of achievement among other significant functionality, various important functionality has been adopted to ensure the confidentiality, integrity and proper access of data in the system. There are some significant functionalities, which are discussed further in the following sections, as well as code snippets and explanation.

4.9.1 Significant Functions

The major functions are the key characteristics making the CyberSafe Learning Hub a working and efficient cybersecurity learning platform.

4.9.1.1 Google OAuth 2.0 Authentication

The system provides seamless authentication through Google OAuth 2.0 using the Laravel Socialite package, allowing users to sign in with their existing Google accounts.

```

19     public function callback()
20     {
21         $googleUser = Socialite::driver('google')->user();
22
23         // 1. Check if user exists by email FIRST
24         $user = User::where('email', $googleUser->email)->first();
25
26         if ($user) {
27             // 2. Attach google_id if missing
28             if (!$user->google_id) {
29                 $user->update([
30                     'google_id' => $googleUser->id,
31                     'avatar' => $googleUser->avatar,
32                 ]);
33             }
34         } else {
35             // 3. Create new user if email does not exist
36             $user = User::create([
37                 'name' => $googleUser->name,
38                 'email' => $googleUser->email,
39                 'google_id' => $googleUser->id,
40                 'avatar' => $googleUser->avatar,
41                 'password' => bcrypt(Str::random(16)),
42             ]);
43
44             // 4. Assign default student role
45             $studentRole = Role::where('name', 'student')->first();
46             $user->roles()->syncWithoutDetaching([$studentRole->id]);
47         }
48
49         Auth::login($user);
50
51         if ($user->hasRole('admin')) {
52             return redirect('/admin/dashboard');
53         }
54
55         return redirect('/student/dashboard');
56     }
57 }

```

Figure 4.80: Code Snippet – Google OAuth 2.0 Callback

Figure 4.80 shows the Google OAuth 2.0 callback implementation in the CyberSafe Learning Hub. It shows how the system authenticates the user through Google and verifies the existence of an account before creating a duplicate account, creates a new user with a secure random password, gives the user the role of a student, and redirects the user depending on the role after logging in.

4.9.1.2 Quiz Scoring and Validation

The quiz submission process implements thorough server-side validation to ensure fair and accurate assessment of student knowledge.

```

49 public function submit(Request $request, Quiz $quiz)
50 {
51     $request->validate([
52         'answers' => 'required|array',
53         'answers.*' => 'required|exists:answers,id',
54         'time_taken' => 'nullable|integer|min:0', // Time in seconds
55     ]);
56
57     $quiz->load('questions.answers');
58     $totalQuestions = $quiz->questions->count();
59
60     // Validate that all quiz questions are answered
61     if (count($request->answers) != $totalQuestions) {
62         if ($request->wantsJson() || $request->ajax()) {
63             return response()->json([
64                 'success' => false,
65                 'message' => 'Please answer all questions before submitting.',
66             ], 422);
67         }
68
69         return back()->withErrors(['answers' => 'Please answer all questions before submitting.']);
70     }
71
72     // Ensure each answer belongs to the correct question and quiz
73     $questionIds = $quiz->questions->pluck('id')->all();
74     $answerLookup = [];
75     foreach ($quiz->questions as $question) {
76         $answerLookup[$question->id] = $question->answers->pluck('id')->all();
77     }

```

Figure 4.81: Code Snippet – Quiz Submission and Validation

Figure 4.81 shows the quiz submission and validation logic in the CyberSafe Learning Hub. It shows how the system verifies a complete and correct response to the questions of the quiz, students who have already passed do not take the quiz again, and the system verifies that the response met 85 % of correct answer, which is verified by the server.

4.9.1.3 AI Chatbot Integration

The CyberSafe Learning Hub combines an AI-based chatbot with the Groq API and Llama 3.3-70B Versatile model that is used as a cybersecurity tutor assistant.

```

35 $systemPrompt = "You are a helpful cybersecurity tutor assistant for the CyberSafe Learning Hub.
36 You are helping a student who is currently taking a quiz about: {$quizContext}.
37
38 IMPORTANT RULES:
39 1. You are here to HELP students understand concepts, NOT give away answers directly.
40 2. If a student asks for a direct answer to a quiz question, politely decline and offer to explain the concept instead.
41 3. Provide educational explanations, hints, and guide students to think through problems.
42 4. Keep responses concise (2-3 paragraphs max) and student-friendly.
43 5. Focus only on cybersecurity topics. Politely redirect off-topic questions.
44 6. Be encouraging and supportive.";

```

Figure 4.82: Code Snippet – AI Chatbot System Prompt

The CyberSafe Learning Hub AI chatbot system prompt configuration is demonstrated in figure 4.82. It shows how the chatbot is coded with a set of strict regulations that will make it appear as a learning tool that will take students through the cybersecurity ideas and offer clues, but will not give direct answers to the questions, limiting the responses to cybersecurity-related topics only.

4.9.2 Security Elements

The security components will make sure that the CyberSafe Learning Hub is safe and secure in handling user data, unauthorised access, and ensuring system integrity.

4.9.2.1 Role-Based Access Control (RBAC) Middleware

Role-based access control is applied to the system with the help of a bespoke middleware that provides limited access to routes depending on the user role (admin or student).

```
11 class RoleMiddleware
12 {
13     /**
14      * Handle an incoming request.
15      *
16      * @param \Closure(\Illuminate\Http\Request): (\Symfony\Component\HttpFoundation\Response) $next
17      */
18     0 references | 0 overrides
19     public function handle(Request $request, Closure $next, ...$roles)
20     {
21         if (!Auth::check()) {
22             abort(403);
23         }
24         foreach ($roles as $role) {
25             if (Auth::user()->hasRole($role)) {
26                 return $next($request);
27             }
28         }
29         abort(403);
30     }
31 }
32
33 }
```

Figure 4.83: Code Snippet – Role-Based Access Control Middleware

Figure 4.83 indicates the custom RBAC middleware deployed in the CyberSafe Learning Hub. It shows the system to verify that an authenticated user has the necessary role to gain access to a route, any unauthorised access to the admin or student areas will result in a 403 Forbidden response.

4.9.2.2 Password Hashing and Data Protection

User passwords are hashed automatically by using the bcrypt algorithm and then stored in the database. Sensitive data is also hidden from API responses.

```

39     protected $hidden = [
40         'password',
41         'remember_token',
42     ];
43
44     /**
45      * Get the attributes that should be cast.
46      *
47      * @return array<string, string>
48      */
49     protected function casts(): array
50     {
51         return [
52             'email_verified_at' => 'datetime',
53             'password' => 'hashed',
54             'onboarded_at' => 'datetime',
55         ];
56     }

```

Figure 4.84: Code Snippet – Password Hashing and Hidden Fields

Figure 4.84 shows the password hashing and data protection configuration in the CyberSafe Learning Hub's User model. It shows how the hashed cast of Laravel will automatically hash passwords with bcrypt, and store them, and how the \$hidden property will not reveal sensitive fields like passwords or session tokens to API requests or in any JSON output.

4.9.2.3 CSRF Protection

Laravel provides built-in Cross-Site Request Forgery (CSRF) protection. The application is marked with a CSRF token on all forms that are automatically validated by the framework.

```

21     <div class="row">
22         {{-- Main Quiz Content --}}
23         <div class="col-lg-8 order-2 order-lg-1">
24             <form method="POST" action="{{ route('quiz.submit', $quiz) }}" id="quizForm">
25                 @csrf
26                 <input type="hidden" name="time_taken" id="timeTakenInput" value="0">

```

Figure 4.85: Code Snippet – CSRF Protection in Blade Form

Figure 4.85 depicts the CSRF protection in the CyberSafe Learning Hub. It shows the application of the @csrf Blade directive within HTML forms to produce a hidden session-specific token, which is automatically checked by Laravel on all POST, PUT, PATCH, and DELETE requests to prevent cross-site request forgery attacks.

4.9.2.4 Owner-Only Resource Access

The system ensures that users can only access their own data, implementing the principle of least privilege.

```
187 public function result(QuizAttempt $attempt)
188 {
189     // Security: only owner can view
190     if ($attempt->user_id !== auth()->id()) {
191         abort(403);
192     }
193
194     $attempt->load('quiz.questions.answers');
195
196     // Calculate percentage and pass/fail using question count
197     $totalQuestions = $attempt->quiz->questions->count();
198     $percentage = $totalQuestions > 0
199         ? ($attempt->score / $totalQuestions) * 100
200         : 0;
201
202     $passed = $percentage >= (self::PASS_THRESHOLD * 100);
203     $canRetake = !$passed;
204
205     return view('student.quizzes.result', compact('attempt', 'percentage', 'passed', 'canRetake'));
206 }
```

Figure 4.86: Code Snippet – Owner-Only Access Control

Figure 4.86 shows the owner-only resource access control implemented in the CyberSafe Learning Hub. It shows how the system will match the ID of the authenticated user with the stored user_id of a quiz attempt record and a 403 Forbidden response is issued when they are not equal, so that students can get access to their quiz results and personal information only.

4.10 Conclusion

The CyberSafe Learning Hub is a successful web based cybersecurity educational platform that is implemented. The system was built on a Laravel 12 framework with PHP 8.2 and with the use of the modern web technologies such as Livewire/Volt to create reactive components, Bootstrap 5.3 to create responsive design, and MySQL 8.0 to provide a stable data storage. The site runs on a DigitalOcean cloud server via Docker containers hosted by Coolify and is scaled and reliable.

The platform achieves its goal of delivering an interactive and engaging cybersecurity learning process through the integration of a number of important elements. The structured learning modules enable administrators to develop and administer categories, modules, lessons, and rich content blocks that enable them to have a well-organised cybersecurity curriculum. The interactive evaluation system that has an 85 percent pass mark is used to make sure that the students are fully comprehending the information before they move forward. Introducing the Groq Llama 3.3 AI chatbot will give students 24/7 access to a cybersecurity tutor that will explain concepts without providing the answer to quizzes, and this will encourage students to learn more. The gamification platform based on badges and certificates encourages students to go on with their learning process.

This being a cybersecurity education platform, the system has elaborate security controls such as role-based access control, Google OAuth 2.0 authentication and password hashing with bcrypt, CSRF controls, input validation on the server-side, and owner-only resources. These security measures ensure confidentiality, integrity, and equitable access of sensitive user data on the platform. The combination of the existing web technologies, the cloud-based deployment, and the effective security controls result in the development of a production ready e-learning solution that is capable of executing its mandate of educating the KTAC students on the issue of cybersecurity awareness and skills.

5 FINDING

5.1 Introduction

This chapter presents the findings obtained from the testing and evaluation phase of the CyberSafe Learning Hub system. Testing is an essential part of Software Development Life Cycle (SDLC) since it provides a system that works properly, satisfies the mentioned requirements, and provides a decent user experience.

The testing was organized into two categories: Non-Functional Testing and Functional Testing. The Non-Functional Testing was done initially to confirm that the system fulfills such quality attributes as performance, security, usability and reliability before ascertaining functional correctness. Functional Testing was then performed at three levels namely Unit Testing, Integration Testing, and System Testing which is to determine that individual parts and entire workflows function properly. Lastly, Acceptance Testing, which involved a Client Acceptance Test (CAT) and a User Acceptance Test (UAT), was a test of how the system would respond to the anticipation of the administrator and the target student users.

Results of each testing phase are recorded in the following sections with test cases, expected results, actual results and the pass or failed results.

5.2 Testing

This section documents the testing process of the CyberSafe Learning Hub system. The system is a web-based learning platform for cybersecurity topics developed using the Laravel 12 framework and for two types of users: administrator and student. The administrator will manage the learning content for the platform, while the student will be able to learn from the content and earn badges and certificates upon completing learning modules.

Testing was performed on the system for both non-functional and functional aspects of the application. Tests for non-functional aspects include performance, security, usability, and reliability of the system. Tests for functional aspects include unit, integration, system, and acceptance tests. Acceptance testing will ensure that the system meets the expectations of both administrator and student users of the application.

All testing was performed on the local machine on Laravel 12, MySQL, and PHP 8.2 environments as well as on the live production website: <https://cybersafelearninghub.app/>

Table 5.1: Testing Overview

Testing Category	Testing Type	Scope	Method
Non-Functional Testing	Performance	Page load speed and system responsiveness	Manual (browser timing)
Non-Functional Testing	Security	Authentication, access control, data protection	Manual browser + code review
Non-Functional Testing	Usability	Responsive design across devices	Manual (desktop & mobile)
Non-Functional Testing	Reliability	Data persistence and system stability	Manual verification
Functional Testing	Unit Testing	Individual controller methods and model functions	PHPUnit / Pest PHP
Functional Testing	Integration Testing	Module interactions and data flows	Manual + PHPUnit Feature Tests
Functional Testing	System Testing	Full system functionality end-to-end	Manual browser testing
Acceptance Testing	Client Acceptance Test	Admin/Lecturer interview evaluation	Structured interview
Acceptance Testing	User Acceptance Test	Student questionnaire (1–5 scale)	Google Form

5.3 Non-Functional Testing

5.3.1 Performance Testing

Performance testing ensures that the system is responsive to an acceptable operating time constraint.

Table 5.2: Performance Testing

Test ID	Test Description	Expected Result	Actual Result	Status
NFT-P01	Load the student dashboard and measure page load time under normal conditions	Page loads within 5 seconds	Page loaded in approximately 2–3 seconds	Pass
NFT-P02	Load the admin analytics dashboard (with charts and aggregated data)	Page loads within 5 seconds	Page loaded in approximately 3–4 seconds	Pass
NFT-P03	Submit a quiz (10 questions) and receive the results page	Response received within 5 seconds	Response received within 2–3 seconds	Pass
NFT-P04	Load a lesson page that includes text, images, infographics, and an embedded video block	Page loads within 5 seconds	Page loaded in approximately 3–4 seconds	Pass

5.3.2 Security Testing

Security testing ensures that the system keeps the user data secure, denies unauthorised users access, and withstands typical web vulnerabilities.

Table 5.3: Security Testing

Test ID	Test Description	Expected Result	Actual Result	Status
NFT-S01	Verify that all pages in production are served over HTTPS	All URLs use HTTPS; HTTP requests redirect to HTTPS	All URLs use HTTPS; HTTP redirects to HTTPS	Pass
NFT-S02	Attempt to access student-protected routes (e.g., /student/dashboard) without authentication	Redirect to login page	Redirect to login page	Pass
NFT-S03	Attempt to access admin-protected routes (e.g., /admin/dashboard) while logged in as a student	403 Forbidden response	403 Forbidden response returned	Pass
NFT-S04	Verify that CSRF tokens are present and validated on all POST forms	CSRF tokens included; invalid token rejected (419)	CSRF tokens present; invalid tokens rejected	Pass
NFT-S05	Inspect the database to confirm passwords are stored as bcrypt hashes, not plain text	Passwords stored as bcrypt hash strings	Passwords stored as bcrypt hashes	Pass
NFT-S06	Attempt to access another student's quiz result by manipulating the URL	403 Forbidden response; access denied	403 Forbidden response returned	Pass

5.3.3 Usability Testing

Usability testing evaluates the accessibility, consistency, and functionality of the interface of the system with various devices and screen sizes.

Table 5.4: Usability Testing

Test ID	Test Description	Expected Result	Actual Result	Status
NFT-U01	View the student dashboard on a desktop screen (1920×1080)	Layout renders correctly; no broken elements	Layout renders correctly	Pass
NFT-U02	View the student dashboard on a mobile screen (375×812)	Responsive layout adapts; navigation collapses	Responsive layout adapts correctly	Pass
NFT-U03	View the lesson content page on both desktop and mobile	Content readable; images scale correctly	Content readable; images scale correctly	Pass
NFT-U04	Complete a quiz on a mobile device	Quiz interface is usable; buttons are accessible	Quiz usable on mobile; no layout issues	Pass
NFT-U05	Navigate through the admin panel on a tablet screen (768×1024)	Admin interface adapts; no critical layout overflow	Admin interface adapts correctly	Pass

5.3.4 Reliability Testing

The reliability testing is used to ensure that the system still has data integrity and is still running as per the normal operating pattern.

Table 5.5: Reliability Testing

Test ID	Test Description	Expected Result	Actual Result	Status
NFT-R01	Complete a lesson and refresh the browser; check whether the lesson is still marked as complete	Progress retained; lesson shown as completed	Progress retained correctly	Pass
NFT-R02	Complete a quiz, close the browser, reopen, and verify that the score and attempt are saved	Quiz attempt and score persisted in the database	Quiz attempt and score correctly persisted	Pass
NFT-R03	Complete all lessons in a module; verify that the badge is awarded even after a full page reload	Badge remains visible on the profile page after reload	Badge persisted and displayed correctly	Pass
NFT-R04	Log out and log back in; confirm that all previously earned badges, points, and certificates are retained	All achievement data retained across sessions	All data retained correctly across login sessions	Pass

5.4 Functional Testing

Functional Testing ensures that the features and business logic of the system is functioning and that it is generating the desired outputs. Testing is structured into three stages, namely: Unit Testing, Integration Testing and System Testing.

5.4.1 Unit Testing

Testing individual components or small pieces of code to ensure that each unit works as intended is what it is called unit testing. Table 5.6 illustrates unit testing that was carried out on the CyberSafe Learning Hub project on the smallest functional components like student and admin dashboard access,

module and lesson creation, quiz management, user deletion, and role validation. Unit testing is meant to discover bugs as soon as possible and reduce future errors besides improving the quality of the code.

Table 5.6: Unit Testing

Test Case	Component	Test Steps	Expected Result	Actual Result	Status
Student Dashboard Access	Student Module	Log in as a student and navigate to /student/dashboard	Dashboard page loads with HTTP 200	Redirected successfully to dashboard	Pass
Student Lesson View	Student Module	Log in as a student and open a lesson page	Lesson content page loads correctly	Lesson content displayed correctly	Pass
Admin Dashboard Access	Admin Module	Log in as admin and navigate to /admin/dashboard	Admin dashboard loads with HTTP 200	Admin dashboard loaded successfully	Pass
Create Module	Admin Module	Fill in module details and submit the creation form	New module saved and listed in admin panel	Module created and displayed	Pass
Delete Module	Admin Module	Select a module and click delete	Module removed from the system	Module deleted successfully	Pass
Create Lesson	Admin Module	Fill in lesson details, link to module, and submit	Lesson saved and linked to the correct module	Lesson created and linked correctly	Pass
Create Quiz	Admin Module	Add quiz details and questions, then submit	Quiz and questions saved to the database	Quiz created successfully	Pass
Delete Student User	Admin Module	Select a student account and delete	User and all related data (progress, quiz attempts, certificates) removed	User and related data deleted	Pass
Role Check – Admin	User Model	Call isAdmin() on an admin user account	Returns true	Returned true	Pass

Test Case	Component	Test Steps	Expected Result	Actual Result	Status
Role Check – Student	User Model	Call isAdmin() on a student user account	Returns false	Returned false	Pass

5.4.2 Integration Testing

Integration testing is one that tests the behaviour of different modules or components within a system. In the CyberSafe Learning Hub project, integration testing is related to the verification of interaction and information exchange among the student module, the admin module, the gamification system, and the content management system. Table 5.7 demonstrates the process of ensuring that the lesson completion flow is connected with the progress tracking, the quiz submissions are connected with the points and badge systems and the activities of the administrators are displayed to students in real time.

Table 5.7: Integration Testing

Test Case	Modules Involved	Test Steps	Expected Result	Actual Result	Status
Registration to Login	Auth Module → Student Module	Register a new account, then log in with the same credentials	Redirected to onboarding page after successful login	Redirected successfully	Pass
Google OAuth Login	Google OAuth → Student Module	Click "Sign in with Google" and complete Google authentication	Logged in and redirected to student dashboard	Redirected successfully	Pass
Onboarding Name Confirmation	Onboarding Module → Student Module	First-time login triggers name prompt; submit confirmed name	Name saved, onboarded_at updated, redirected to dashboard	Completed successfully	Pass
Lesson Completion to Progress Update	Lesson Module → Progress Module	Open a lesson and click "Mark as Complete"	Lesson marked as completed in the progress table	Progress updated correctly	Pass
Quiz Submission to Points Award	Quiz Module → Points System	Answer all quiz questions and submit	Score calculated and points awarded to student profile	Points awarded correctly	Pass

Test Case	Modules Involved	Test Steps	Expected Result	Actual Result	Status
Module Completion to Badge Award	Quiz Module → Badge System	Pass all quizzes in a module with 85% or above	Badge awarded and displayed on student profile	Badge shown correctly	Pass
Module Completion to Certificate	Badge System → Certificate Module	Complete all lessons and pass all quizzes in a module	PDF certificate generated and available to download	Certificate generated and downloadable	Pass
Admin Creates Lesson, Student Views	Admin Module → Student Module	Admin creates a new lesson; student navigates to the module	New lesson visible to the student under the correct module	Lesson displayed correctly	Pass
Admin Deletes User, Data Removed	Admin Module → Database	Admin deletes a student account from the user management panel	User and all associated records removed with no orphaned data	All data deleted correctly	Pass
Admin Sends Notification, Student Receives	Admin Module → Notification Module	Admin sends a notification to a student	Notification appears in the student's notification panel	Notification received and displayed	Pass

5.4.3 System Testing

System testing refers to the process that involves testing a whole application as a complete system to determine whether all the components are acting in a desired manner when together. Table 5.8 demonstrates system testing in the CyberSafe Learning Hub project where the system integration between the student learning flow, gamification system, the admin management tools, and the delivery of the content is verified. This testing is used to ensure that every part of the system is functioning properly to the next. It is done after unit and integration testing, and it ensures that the system meets all the requirements of the users.

Table 5.8: System Testing

Test Scenario	Test Steps	Expected Result	Actual Result	Status
Full Registration and Login	Open registration page → Enter details → Register → Log in	Access granted to student dashboard	Successfully logged in	Pass
Google OAuth Sign-In	Click "Sign in with Google" → Authenticate via Google	Redirected to student dashboard	Login successful	Pass
Lesson Content Viewing	Navigate to a module → Open a lesson → View all content blocks	Text, images, infographics, and video rendered correctly	All content displayed correctly	Pass
Quiz Attempt and Scoring	Open quiz → Answer all questions → Submit	Score calculated and result page shown with correct/incorrect feedback	Score displayed accurately	Pass
Points Awarded After Quiz	Complete a lesson and pass a quiz → View dashboard	Points updated and visible on student profile	Points reflected correctly	Pass

Test Scenario	Test Steps	Expected Result	Actual Result	Status
Badge Awarded on Module Completion	Complete all lessons and pass all quizzes in a module → View profile	Badge displayed on the profile page	Badge shown correctly	Pass
Certificate Generation and Download	Complete all modules in a category → Navigate to certificates page → Download	PDF certificate generated with student name and module title	Certificate downloaded successfully	Pass
Leaderboard Display	Navigate to the leaderboard page	Students ranked correctly by total points	Rankings displayed accurately	Pass
AI Chatbot Assistance	Open chatbot during a quiz → Ask a cybersecurity concept question	Relevant explanation provided without giving the direct answer	Response shown correctly	Pass
Admin Module Management	Log in as admin → Create, edit, and delete a module	Changes reflected immediately in the system	Module operations successful	Pass
Admin Lesson Content Editor	Log in as admin → Open a lesson → Add text, image, infographic, and video blocks	All content blocks saved and rendered in the correct order	Content saved and displayed	Pass
Admin Quiz and Question Management	Log in as admin → Create a quiz → Add multiple-choice questions	Quiz and questions saved; available to students	Quiz created successfully	Pass

Test Scenario	Test Steps	Expected Result	Actual Result	Status
Admin Student Management	Log in as admin → View student list → Delete a student account	Student removed from the system with all associated data	Student deleted successfully	Pass
Admin Notification System	Log in as admin → Send notification to a student → Student views notification	Notification received and displayed in student's panel	Notification shown correctly	Pass
Admin Analytics Dashboard	Log in as admin → Open analytics page	Total users, completion rates, and active student data displayed accurately	Statistics loaded correctly	Pass

5.5 Acceptance Testing

The final stage of testing conducted to check if the system satisfies the client and targeted end user requirements is known as Acceptance Testing. There were two kinds of acceptance testing done. The first approach involves client acceptance testing (CAT). In this activity, the administrator or lecturer in charge of the system goes through an interview session conducted using a predetermined question set. The next step of the project is user acceptance testing (UAT) which distributing questionnaire to student user that use and test the system personally.

5.5.1 Client Acceptance Testing

A one-on-one interview with Mr. Syaheedullah Bin Yahya, a lecturer at Kolej Teknologi Antarabangsa Cybernetics (KTAC), who will be the manager of CyberSafe Learning Hub, was done as Client Acceptance Testing. The interview was divided into 15 formatted questions on project objectives three (Cybersecurity Awareness, Interactive Education, Motivation & Gamification) and both the functional and non-functional requirements.



Figure 5.1: Client Acceptance Testing Session with Mr.Syaheedullah bin Yahya

Table 5.9: Client Acceptance Testing: Interview Response Summary

Interview Question	Client's Response	Analysis / Outcome
Are the cybersecurity lessons and modules comprehensive and appropriate for the target student audience?	The modules are very comprehensive. The flow from basic to more advanced topics is just right for the students, easy for them to follow without feeling too heavy.	The lesson content is deemed comprehensive and appropriate for the target audience.
Does the platform cover all essential cybersecurity topics that students should learn?	Yes, it covers all the main topics like phishing, malware, and passwords, which are very important for students to learn so they know how to protect themselves in their daily lives.	All required cybersecurity topics are adequately covered.
Does the platform effectively bridge the knowledge gap for students with little to no prior cybersecurity awareness?	Very effective. The explanations are quite straightforward and do not use too much heavy jargon, making it really suitable for students who have zero background in cybersecurity.	The platform successfully bridges the cybersecurity knowledge gap for beginners.

Interview Question	Client's Response	Analysis / Outcome
Are the quizzes and interactive elements effective tools for reinforcing cybersecurity concepts?	The quizzes are quite good for testing understanding right after the lesson. It really helps students remember what they have just read.	Quizzes and interactive elements are effective for concept reinforcement.
Are the visual materials and multimedia content adequate to keep students engaged?	The visuals and videos are good and keep the students from getting bored reading too much text. More interactive infographics could be added in the future, but overall it is good enough.	Multimedia content is sufficient to maintain student engagement.
Does the platform provide sufficient feedback mechanisms for assessing student understanding?	Yes, the feedback is immediate. Students can see their quiz scores right away to know where their mistakes are, and it is easy for the lecturer to monitor their understanding as well.	Feedback mechanisms are adequate for both students and administrators.
Are the gamification features (points, badges, progress tracking) effective in motivating students?	The points and badges really help. Students enjoy this kind of gamification, it makes them more excited to finish the modules instead of just reading normal notes.	Gamification features are effective in motivating student participation.
Is the badge and milestone system meaningful enough to encourage continued participation?	Yes, the badges give students a sense of achievement. It is a good way to encourage them to keep logging in and complete the whole course.	The badge system provides meaningful incentives for continued learning.
Does the progress tracking dashboard give a clear and accurate picture of student progress?	The dashboard is very clear. It is easy to see which students are doing well and who is left behind, making it very convenient for tracking.	The dashboard accurately reflects student progress and is useful for monitoring.

Interview Question	Client's Response	Analysis / Outcome
Were you able to create, edit, and delete lessons, modules, and quizzes without errors?	No problems at all. Creating, editing, and deleting lessons is very smooth, with no bugs or errors experienced while using it.	Content management features function correctly without errors.
Does the admin dashboard provide all the information needed to monitor and review student performance?	Yes, the admin dashboard has all the information needed to monitor students' performance. It is quite neat and easy to view at a glance.	The admin dashboard provides comprehensive performance monitoring data.
Is the role-based access control working correctly for students and admins?	The access control is working fine. Students only see what they are supposed to see, and admins have full control. There has been no mix-up so far.	Role-based access control is functioning as intended.
Did you experience any performance issues while managing lessons or viewing the dashboard?	The system is quite stable. Loading time is fast and there was no lag or timeout experienced when navigating the dashboard.	No performance issues were encountered during admin usage.
Is the admin interface intuitive enough to manage all platform features without technical training?	Very user-friendly. The interface is simple to use, so even lecturers who are not very IT-savvy can manage it without needing much training.	The admin interface is intuitive and requires no technical training.
Are you confident that the system reliably stores all student data, progress, and credentials securely?	The system looks secure enough. The data saving and session management seem reliable, and there is confidence that students' progress will not suddenly go missing.	The system is deemed secure and reliable for storing sensitive student data.

5.5.2 User Acceptance Testing

The process of User Acceptance Testing (UAT) was carried out through the distribution of questionnaire through Google Forms to students who visited the platform of CyberSafe Learning Hub and explored it. There were 54 students who were involved in the evaluation. The participants were asked to rate each of the statements on a linear scale of 1 to 4, with: 1, Strongly Disagree, 2, Disagree, 3, Agree, 4, Strongly Agree.

The questionnaire contained 17 questions, beginning with demographic information and followed by evaluation of the platform's features in relation to the three project objectives which is cybersecurity awareness, interactive education, and student motivation through gamification as well as functional and non-functional requirements. The results from each question are presented below as chart images exported from Google Forms.

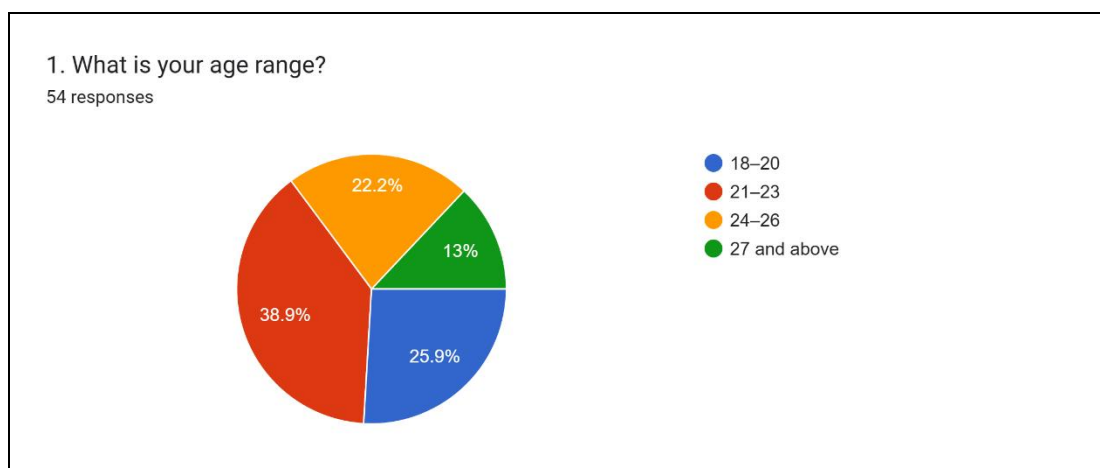


Figure 5.2: Age Range of Respondents

Figure 5.2 shows the age range distribution of the 54 student respondents who participated in the User Acceptance Testing. Most of the respondents were between the ages of 21 and 23 years (38.9%), then there was the 18 to 20 age group (25.9%), the 24 to 26 age group (22.2%), and the 27 and above age group (13.0). This distribution shows that the platform was mostly rated by students aged undergraduate, which also corresponds to the target audience of the CyberSafe Learning Hub. The diversity of the respondents in terms of age will give a fairly balanced view on the practicality and efficiency of the platform.

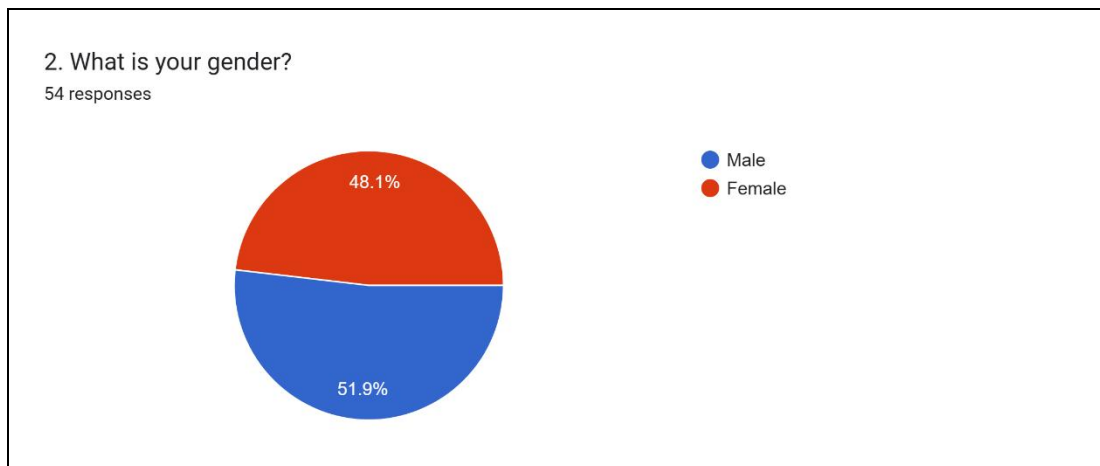


Figure 5.3: Gender of Respondents

Figure 5.3 presents the gender distribution of the respondents. A total of 54 participants were included in the study, of which 51.9% were male and 48.1% were female. The close balance between male and female respondents shows that there was a balance between genders in the UAT sample. It is a balance that makes sure that the results of the evaluation are not highly biased towards the preferences of a single gender and that the usability of the platform and educational content can be viewed as universal and applicable to the students of any gender.

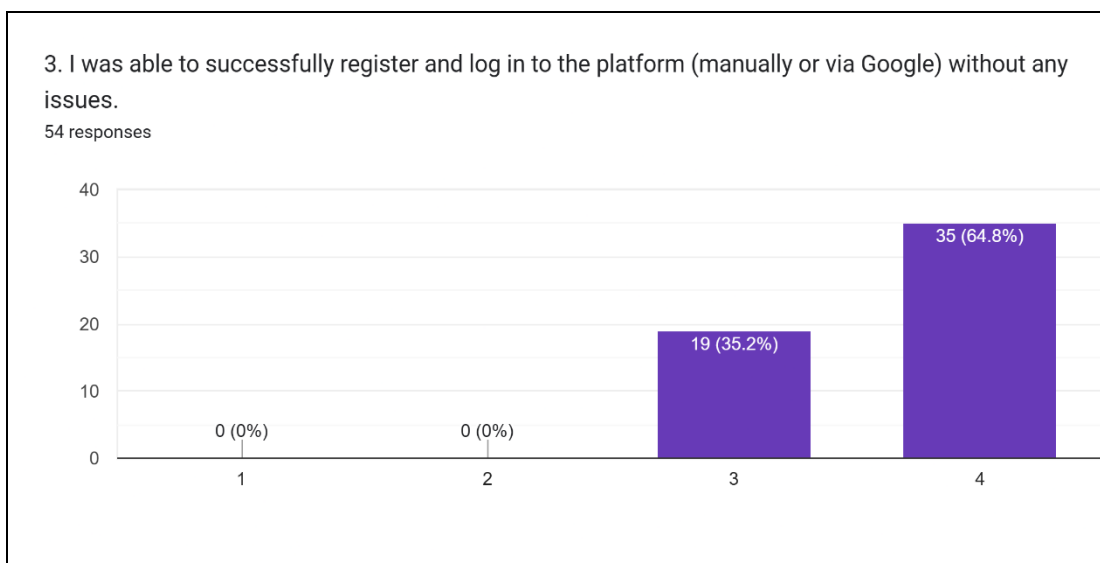


Figure 5.4: Registration & Login

Figure 5.4 presents the answers of the registration and the login assessment. The findings show that 35.2% of the respondents responded in the affirmative and 64.8% strongly affirmative such that the total response rate of 100% was obtained. The large percentage of the high level of agreement proves that both the manual email/ password registration and the Google OAuth 2.0 sign-in pathway were user friendly and effective to all student users. These findings verify that the authentication system is functioning properly and offers a pleasant onboarding experience without any technical obstacles.

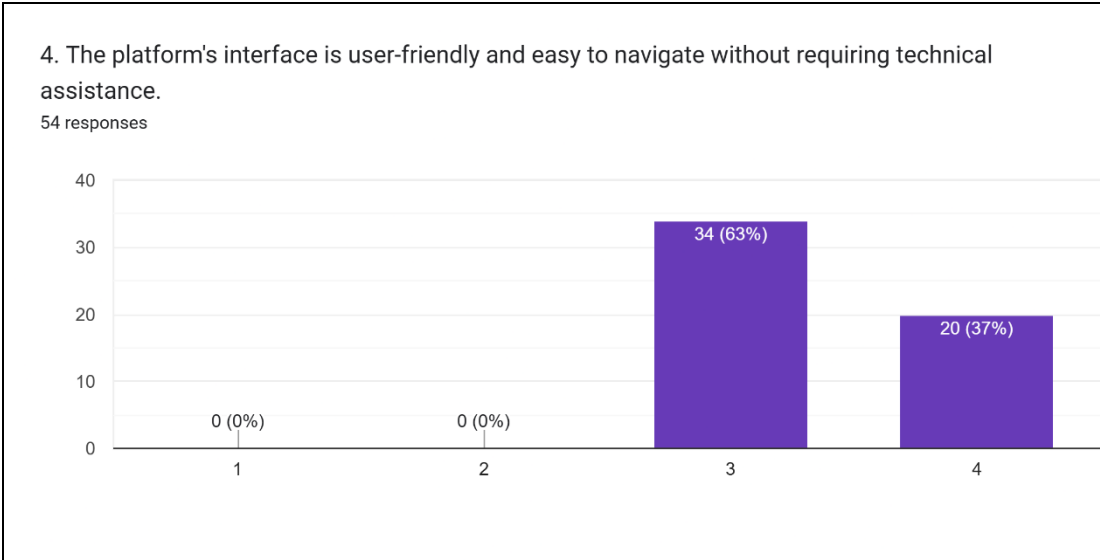


Figure 5.5: Navigation & Usability

Figure 5.5 presents the answers to the platform navigation and usability test. A total of 63.0% of respondents agreed and 37.0% strongly agreed, achieving a 100% positive response rate. The platform could be used individually by everyone, which implies that the interface design, menu, and page organisation could be comprehended as well as easily used by the individuals of various technical backgrounds. The results verify the design decision of clean and organised interface which is based on Bootstrap 5.3, so that non-IT students can use it without any difficulties.

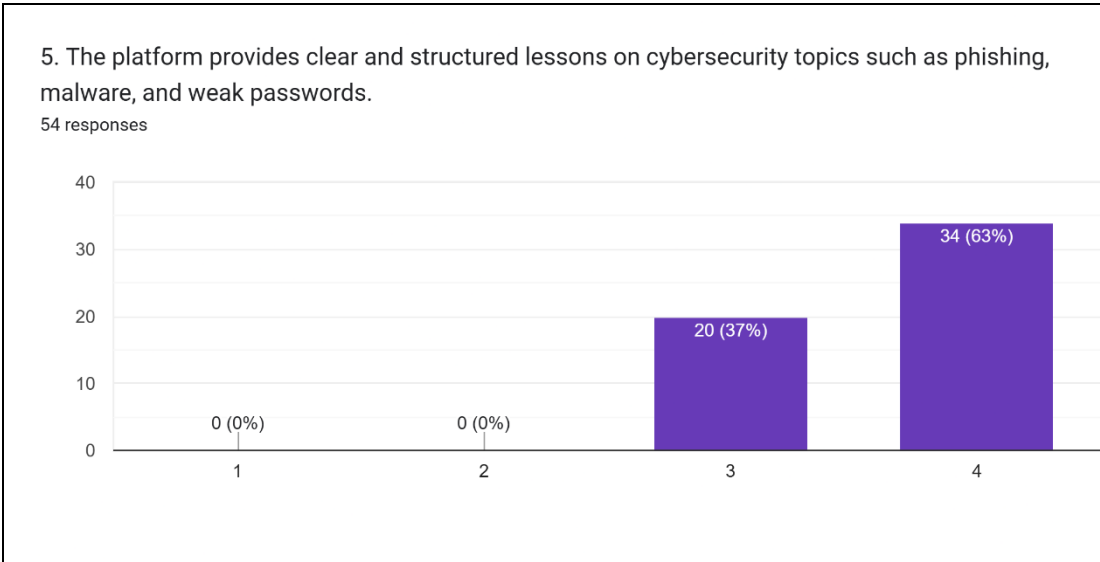


Figure 5.6: Cybersecurity Awareness (Lesson Structure)

Figure 5.6 shows the answers to the lesson structure and the cybersecurity awareness test. The findings indicate that 37.0% of participants concurred and 63.0% strongly concurred with a 100% positive response rate. The fact that the percentage of the respondents that strongly agreed is high points to the fact that the structured nature of presenting cybersecurity information, in categories, modules, and sequential lessons was an efficient way of offering a uniform and well-

organized learning process. This will validate the content structure of the platform to achieve the first goal of the project of raising cybersecurity awareness.

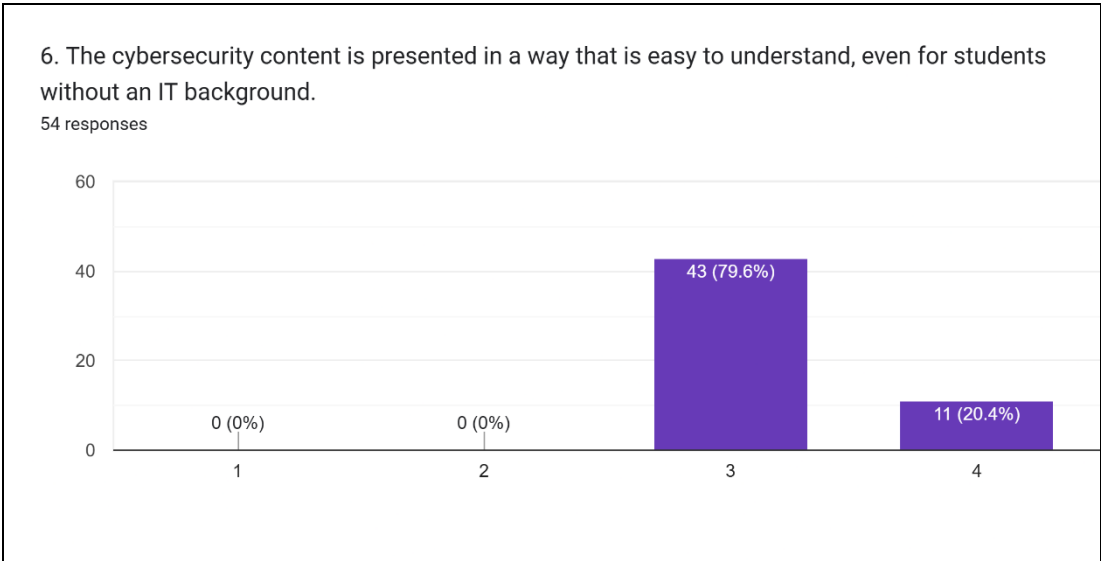


Figure 5.7: Cybersecurity Awareness (Content Clarity)

Figure 5.7 illustrates the answers obtained regarding the content clarity and accessibility assessment. A total of 79.6% of respondents agreed and 20.4% strongly agreed, resulting in a 100% positive response rate. Although most participants answered with agreement instead of strong agreement, the fact that there were no negative or neutral answers proves that the use of plain language, infographics, images, and real-life examples was effective in the process of rendering technical concepts of cybersecurity accessible to non-IT student audience. This finding justifies the objectives of the platform, which are to address the knowledge gap on cybersecurity among beginners.

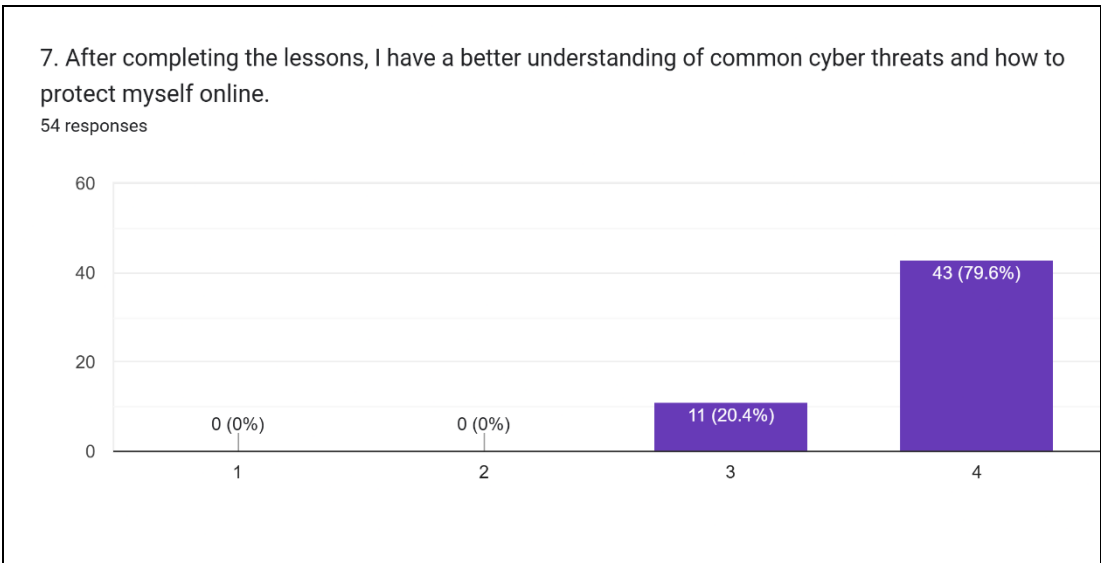


Figure 5.8: Cybersecurity Awareness (Learning Outcome)

Figure 5.8 indicates the answers to the learning outcome and cyber threat awareness test. One of the highest scores was obtained in this question, where 79.6% of the participants strongly agreed and 20.4% agreed, resulting in a 100% positive rate. The strong agreement rate means that the content of the learning was not only understandable but it was in fact useful in enhancing the knowledge and awareness of cybersecurity among students. This outcome is a direct indication that the platform is able to fulfill its initial goal of enhancing cybersecurity awareness in students.

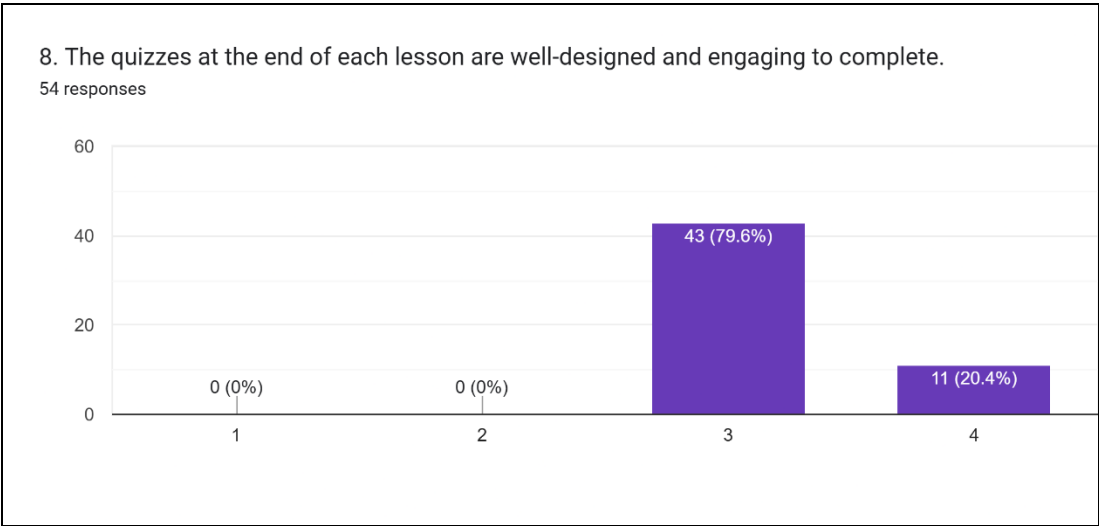


Figure 5.9: Interactive Education (Quiz Design)

Figure 5.9 shows the responses for the quiz design and engagement evaluation. The results show that 79.6% of respondents agreed and 20.4% strongly agreed, with all 54 respondents providing a positive response. The findings support that the quiz type of multiple choice, the 85 per cent threshold of passing, and instant feedback of the score were considered to be a well-organized and effective estimation mechanism. The fact that there is no disagreement whatsoever means that the quiz system is effective in promoting active involvement and knowledge reinforcement.

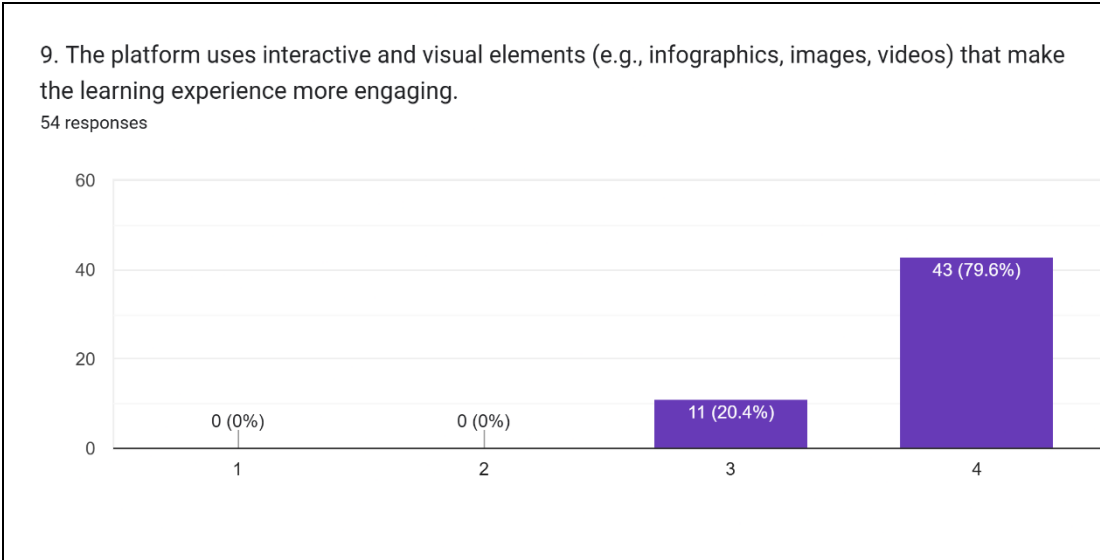


Figure 5.10: Interactive Education (Visual Elements)

Figure 5.10 presents the interactive and visual element evaluation responses. This question registered the highest score of strong agreement at 79.6% and the rest of the 20.4% agreed, making the question having 100 percent positive response. The high positive feedback of the multimedia content proves the fact that the combination of text, images, infographics, and embedded videos throughout the blocks of lesson content contributed to the increase in student engagement and made the process of learning more dynamic than reading a plain text does.

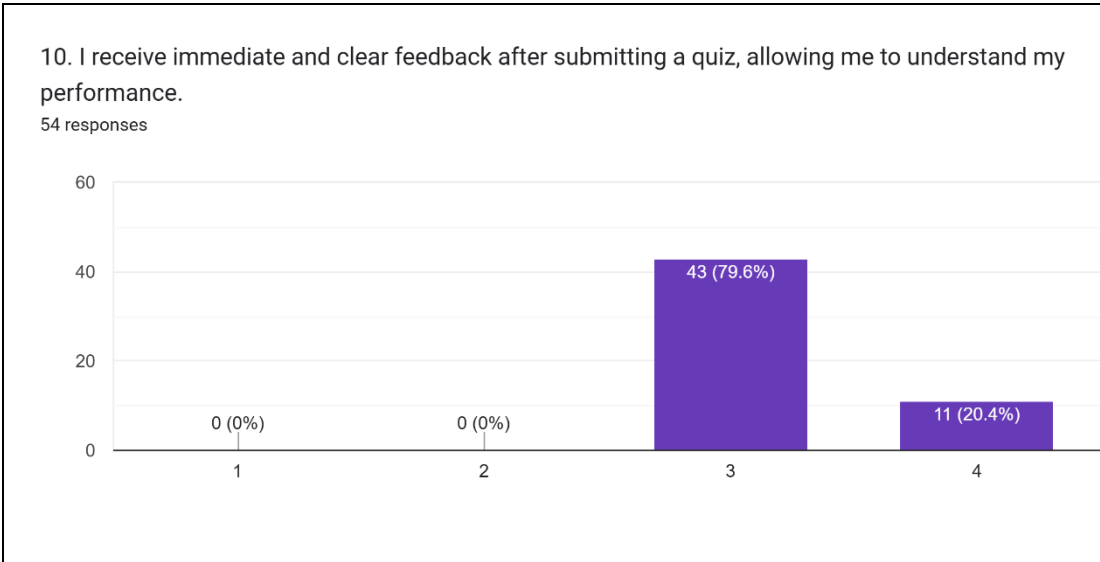


Figure 5.11: Interactive Education (Quiz Feedback)

Figure 5.11 shows the responses for the quiz feedback usefulness evaluation. A total of 79.6% of the respondents were in agreement with 20.4% strongly agreeing with no negative responses to this question. The outcome testifies that the quiz result page, showing the total score, percentage, pass or fail, time spent, and the feedback of the correct and incorrect answers per question, was understood as clear and helpful by all the participants. This is an instant feedback mechanism that

promotes the second goal of the platform to offer a level of interactive and engaging cybersecurity education.

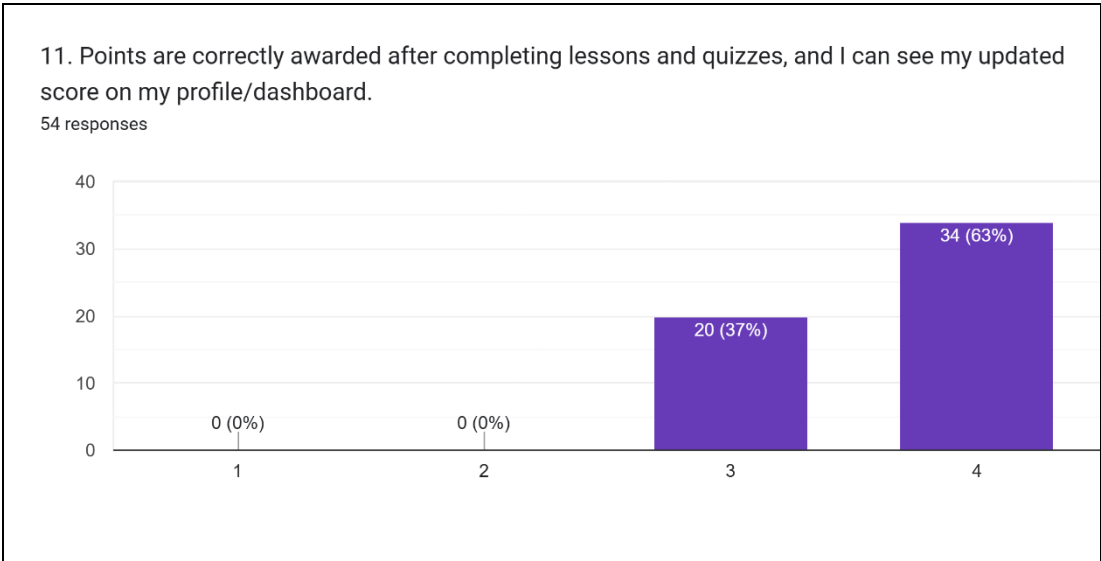


Figure 5.12: Motivation & Gamification (Points System)

Figure 5.12 shows the responses for the points system evaluation. The findings indicate that 37.0% of the respondents were in agreement and 63.0% strongly agreed, with a positive response rate of 100. Most of the strong agreement proves that students were satisfied that the points-awarding system was working properly and transparently. The feedback on the new scores on the student dashboard and profile page was well-received, which proves that the gamification mechanism is precise and encourages further interaction.

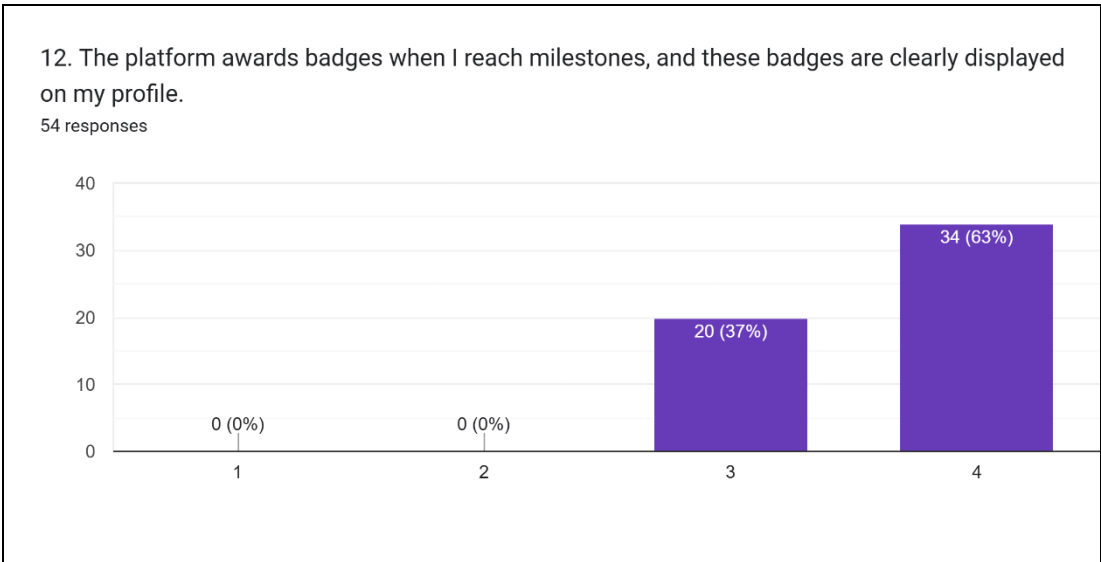


Figure 5.13: Motivation & Gamification (Badge System)

Figure 5.13 represents the responses to the evaluation of the badge system. As was the case with the points system, the respondents were equally positive with 37.0% agreeing and 63.0% strongly agreeing with a 100 percent positive response rate. The great positivity of the badge

system shows that students believed that the completion milestones of the module were significant and the display of the badge on their profile was easily seen and rewarding. The finding contributes to the third project goal of inspiring students using gamification in that the badge mechanism is operational to generate concrete achievement recognition.

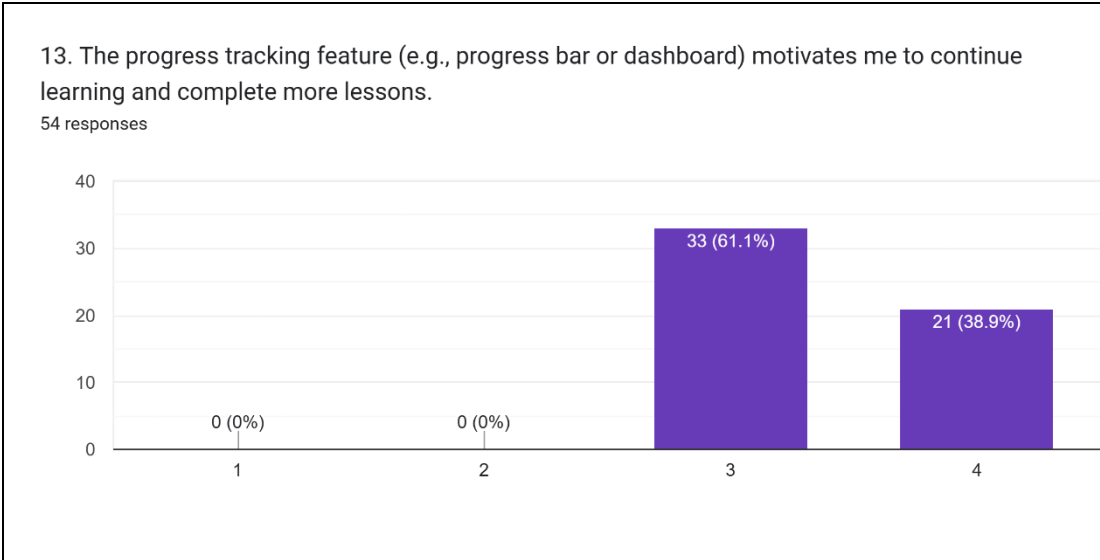


Figure 5.14: Motivation & Gamification (Progress Tracking)

Figure 5.14 presents the answers of progress tracking motivation evaluation. The positive response rate was 100% with 61.1% and 38.9% of respondents agreeing and strongly agreeing respectively. Each of the participants admitted that the aspects of tracking progress like module completion progress bars and the student dashboard overview were an incentive to learn. Although the percentage of strongly agreed answers is relatively less than other questions related to gamification, the fact that there are no negative answers proves that the progress tracking system is applicable across the board to encourage further engagement of students.

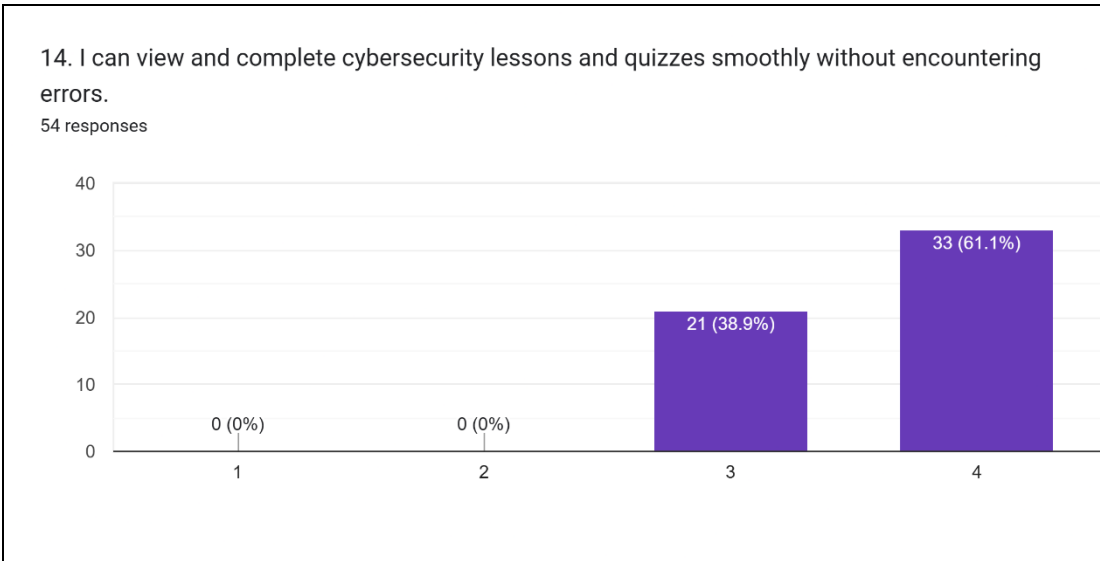


Figure 5.15: Functional Requirements (Lesson & Quiz Access)

Figure 5.15 shows the responses for the lesson and quiz functional access evaluation. The results show that 38.9% of respondents agreed and 61.1% strongly agreed, achieving a 100% positive response rate. Most of the strong agreement confirms that the key student-facing functionality, such as the content of the lesson viewing, the quiz attempt submission, and the display of the results, worked without errors throughout the timeframe of the evaluation. This is in line with the system testing results recorded in Table 5.8 where all 15 system-level test cases were successful.

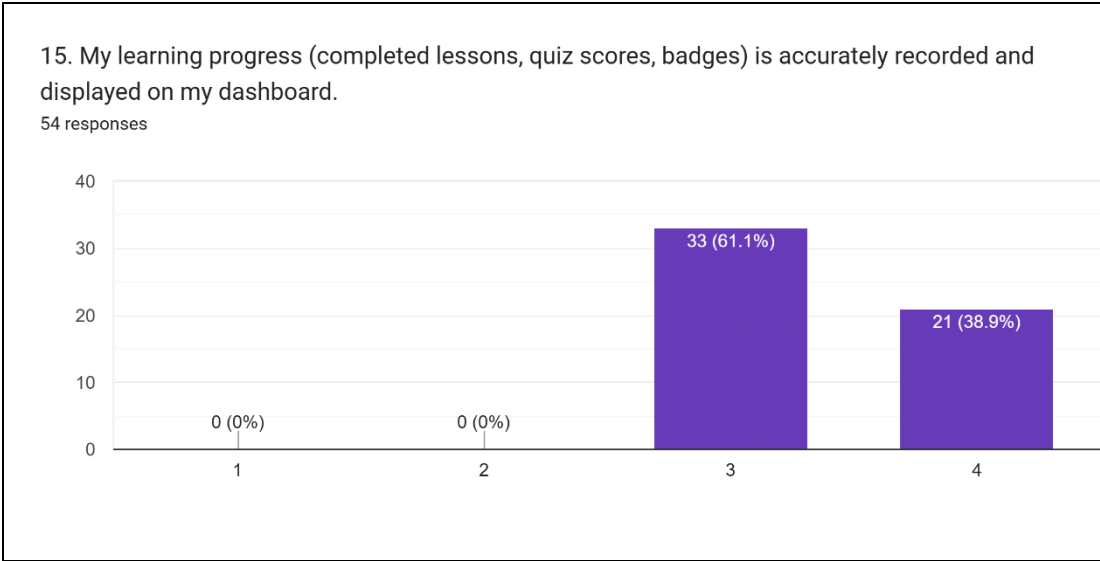


Figure 5.16: Functional Requirements (Progress Recording)

Figure 5.16 shows the responses for the progress recording accuracy evaluation. A total of 61.1% of respondents agreed and 38.9% strongly agreed, with a 100% positive response rate. All respondents agreed that the system was precise in tracking and showing their progress in all lessons and their quiz results and badges on the student dashboard. This confirms the consistency of the student progress and quiz attempt database tables and confirms that the progress tracking system is properly saving student data between sessions, which is also checked in the reliability testing (NFT-R01 through NFT-R04).

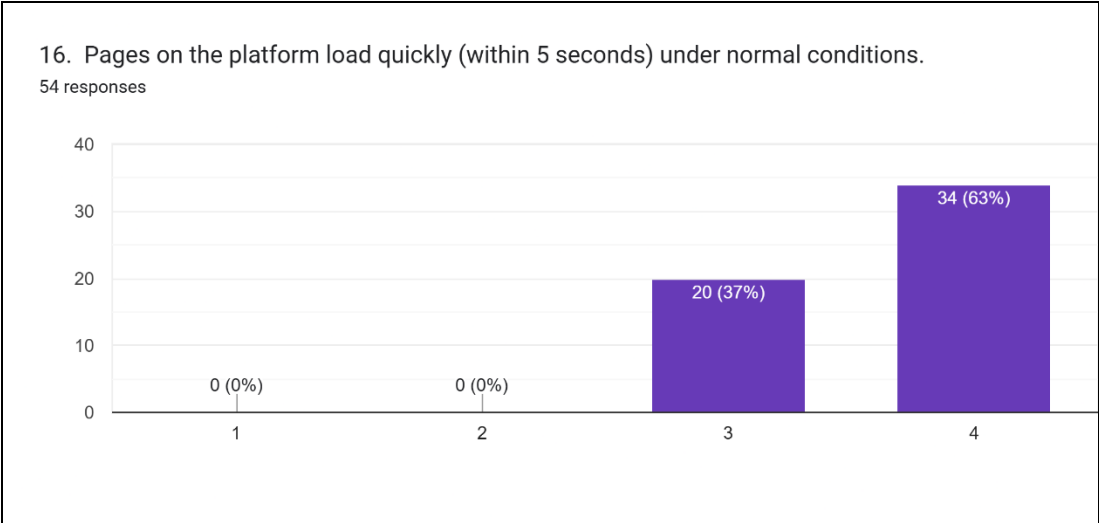


Figure 5.17: Non-Functional Requirements (Performance)

Figure 5.17 shows the responses for the page load performance evaluation. The analysis indicates that 37.0% of respondents agreed and 63.0% strongly agreed and 100% indicated with a positive response. The high majority of strong agreement proves that the performance of the platform that uses Nginx as a reverse proxy, Laravel and its query optimisation, and DigitalOcean as a cloud hosting provider provides an acceptable page load experience to all the users. This finding is in line with the performance testing findings (NFT-P01-NFT-P04) in which all pages loaded between 2 and 4 seconds in normal conditions.

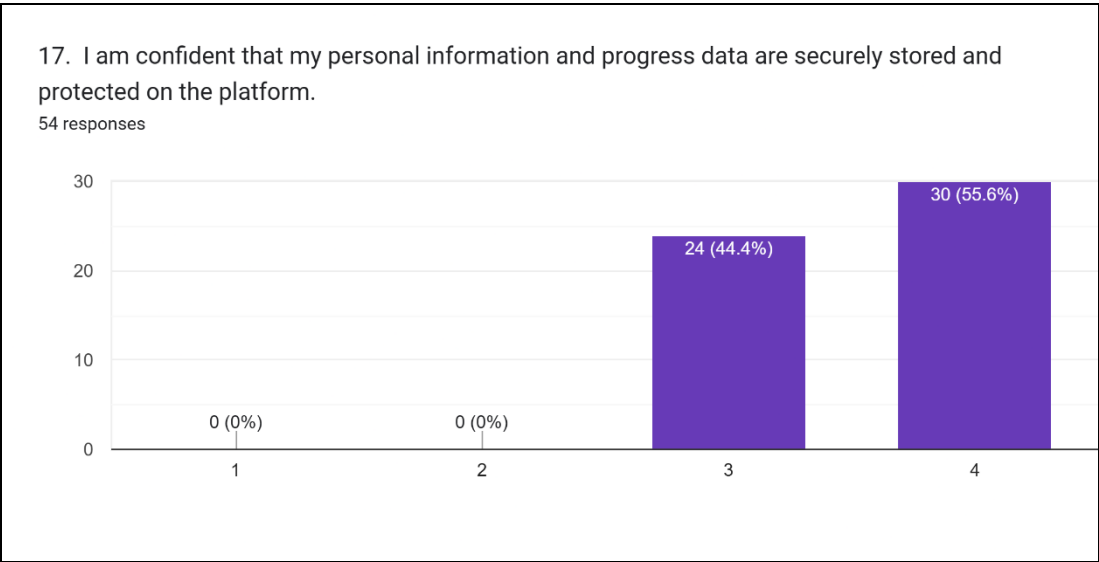


Figure 5.18: Non-Functional Requirements (Security)

Figure 5.18 shows the responses for the data security confidence evaluation. The proportion of respondents who agreed and strongly agreed was 44.4% and 55.6% respectively, which yields 100% positive response rate. Most of the strong agreement is an indicator of student trust in the security practices at the platform such as, HTTPS encryption, bcrypt password hashing, CSRF protection, and role-based access control. This good image is especially important considering that

the platform is a cybersecurity education tool - the fact that everyone involved in the process had no doubts about the security of their personal data confirms the validity and integrity of the CyberSafe Learning Hub as a security-conscious application.

5.6 Conclusion

This chapter contained the results of the extensive testing procedure that was performed on the CyberSafe Learning Hub system. Testing was divided into two large categories that comprised of Non-Functional Testing and Functional Testing followed by Acceptance Testing.

The first one was Non-Functional Testing which was performed to verify the quality properties of the system, and the second was functional correctness. All the 18 non-functional test cases of the Performance, Security, Usability, and Reliability were passed and this validated the fact that the system loads within acceptable time limits, has appropriate security controls (HTTPS, role based access control, CSRF protection and bcrypt password hashing), responsive interface irrespective of the device used, and the data integrity during user sessions.

Unit Level Functional Testing: this was carried out to verify that all the 10 single controller methods and model functions are working properly in isolation. Integration Testing was used to ensure that the 10 key system workflows, such as the Google OAuth login process, are fully functional up to modules, the issuance of badges and the creation of certificates, are fully functioning at the end. System Testing showed that all the 15 functional requirements were achieved and the test cases were all successful.

Acceptance Testing offered external verification between the client and the end users. The Client Acceptance Test had a 100 percent acceptance rate in all the 15 interview questions. The result of the User Acceptance Test that would be received once the data collection process is finished would provide certain quantitative data on the student satisfaction concerning the usability, educational value, gamification, and the reliability of the platform.

Overall, the findings of the testing made are that CyberSafe Learning Hub is a complete, functional, and technically feasible and quality-guaranteed system that effectively fulfills all the mentioned goals and specifications. These findings form the basis of findings in Chapter 6, which are compiled in the conclusions and recommendations.

6 CONCLUSION

6.1 Introduction

This chapter draws a close to the creation and testing of the CyberSafe Learning Hub, a web-based platform of cybersecurity education based on the Laravel platform. The chapter is a recap of the project as a whole in terms of the project schedule, the risk management measures and to what extent each of the described project objectives was achieved. Limitations and constraints, which were encountered in the development, are also discussed and suggestions made on the future work to expand and develop the platform further.

The CyberSafe Learning Hub is a program that has been developed to address a growing need of cybersecurity education accessibility, engagement, and effectiveness among students of universities. The platform can offer a complete-fledged learning management system that is founded on cybersecurity awareness by combining a structured lesson material, interactive quizzes, gamification tools, and role-based management.

6.2 Project Schedule

Project timeline is a road map, which is essential in planning, implementing, and monitoring development cycle of CyberSafe Learning Hub. It also helps to implement all the project activities in a systematic manner and within the stipulated time. This project schedule was built on the Agile approach and graphically presented with two different and yet complementary project management tools, which are the Work Breakdown Structure (WBS) and the Gantt chart.

The WBS serves as the project planning basis by subdividing the entire scope of the project into small and manageable and hierarchical elements (the what) without leaving out any of the critical activities. The Gantt chart then uses these components identified and plots them in a sequential fashion over a graphical time scale (the when) in a way that gives a clear picture of the duration of the tasks, overlaps and dependencies to monitor the overall project progress.

6.2.1 Work Breakdown Structure

The Work Breakdown Structure (WBS) breaks down the whole project into manageable work and sub-work, giving a clear picture of the hierarchy of the work needed to achieve the CyberSafe Learning Hub. The WBS was taken as the basis of planning the project timeline and prioritizing each stage of development.

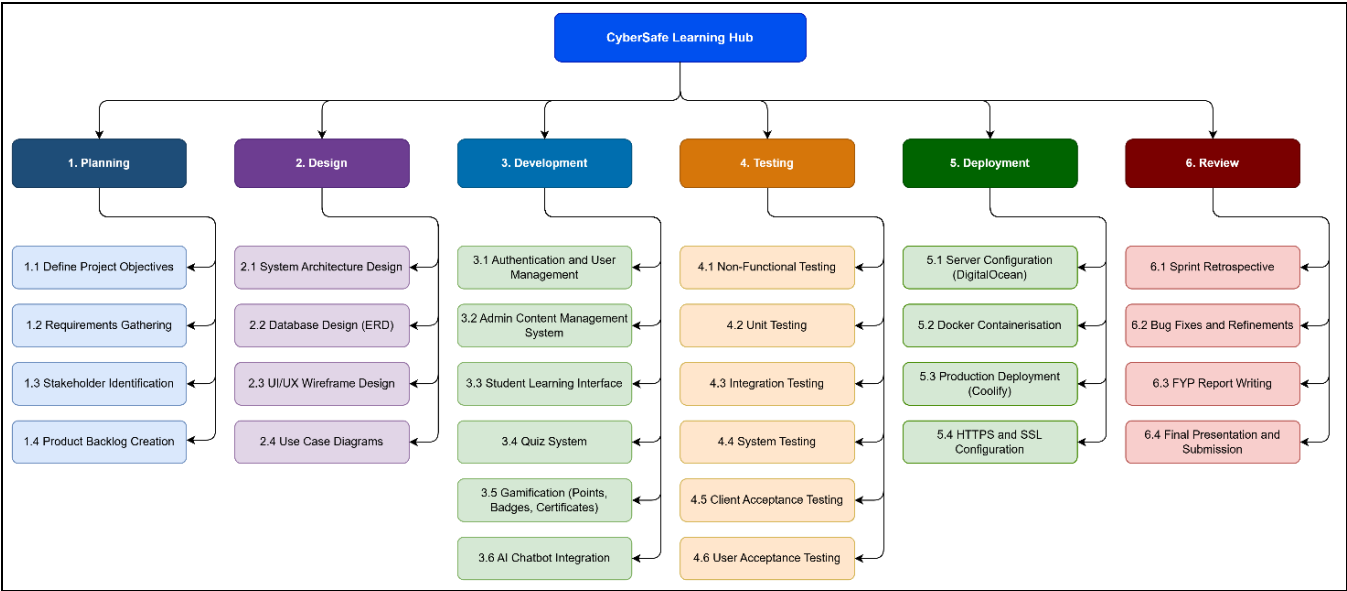


Figure 6.1: Work Breakdown Structure of the CyberSafe Learning Hub Project

Figure 6.1 presents the WBS of the CyberSafe Learning Hub that follows an Agile approach and breaks down the project lifecycle into six chronological steps. This starts with Planning to establish objectives and a product backlog, then Design to develop the system architecture, ERD, and wireframes of the UI. The Development phase includes the creation of the central part of the system, which includes the admin panel, the student interface, and the gamified quiz system. After the prototype is in place, there is intensive Testing (unit, system, and user acceptance testing) to assure quality. The Deployment phase will then process the configuration of the servers and make the application live through cloud hosting. Lastly, there is the Review phase where the emphasis is laid on sprint retrospectives, bug fixes and finalizing the final FYP documentation to be submitted.

6.2.2 Gantt Chart

The Gantt Chart illustrates the planned and actual timeline for each task defined in the WBS, showing the start date, duration, and completion status of all project activities across the development period.

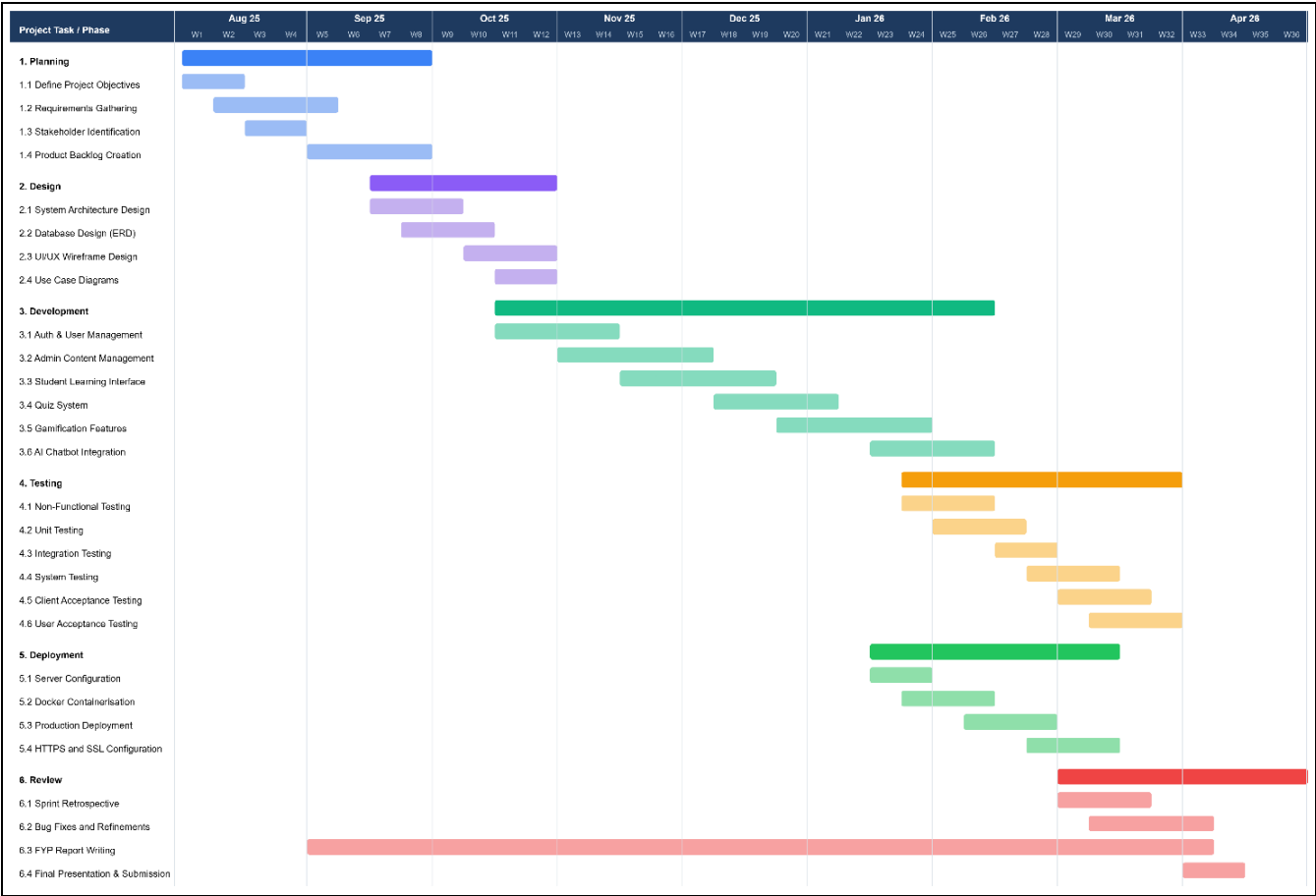


Figure 6.2: Gantt Chart of the CyberSafe Learning Hub Project Timeline

The Gantt chart, as demonstrated in Figure 6.2, is a graphic representation of the five Agile phases of the WBS over a 36-week period, between August 2025 and April 2026. Planning phase covers the first two months to define objectives whereas the Design phase overlaps in September to design system architecture before coding. The most intensive phase is the core Development phase which takes place between October to January and directly proceeds into the comprehensive testing. Testing and Deployment phases are executed simultaneously towards the end of the project so as to achieve quick bug fixes as the server environments are being configured. The Review phase that includes all FYP report documentation is constantly kept within the entire project lifecycle, which eventually results in final refinements and submission in April 2026.

Table 6.1: Project Task Timeline and Duration

ID	Task Name	Start	Finish	Duration
1.	Planning	August 2025 (Week 1)	September 2025 (Week 8)	8 Weeks
1.1	Define Project Objectives	August 2025 (Week 1)	August 2025 (Week 2)	2 Weeks
1.2	Requirements Gathering	August 2025 (Week 2)	September 2025 (Week 5)	4 Weeks
1.3	Stakeholder Identification	August 2025 (Week 3)	August 2025 (Week 4)	2 Weeks

ID	Task Name	Start	Finish	Duration
1.4	Product Backlog Creation	September 2025 (Week 5)	September 2025 (Week 8)	4 Weeks
2.	Design	September 2025 (Week 7)	October 2025 (Week 12)	6 Weeks
2.1	System Architecture Design	September 2025 (Week 7)	October 2025 (Week 9)	3 Weeks
2.2	Database Design (ERD)	September 2025 (Week 8)	October 2025 (Week 10)	3 Weeks
2.3	UI/UX Wireframe Design	October 2025 (Week 10)	October 2025 (Week 12)	3 Weeks
2.4	Use Case Diagrams	October 2025 (Week 11)	October 2025 (Week 12)	2 Weeks
3.	Development	October 2025 (Week 11)	February 2026 (Week 26)	16 Weeks
3.1	Auth & User Management	October 2025 (Week 11)	November 2025 (Week 14)	4 Weeks
3.2	Admin Content Management	November 2025 (Week 13)	December 2025 (Week 17)	5 Weeks
3.3	Student Learning Interface	November 2025 (Week 15)	December 2025 (Week 19)	5 Weeks
3.4	Quiz System	December 2025 (Week 18)	January 2026 (Week 21)	4 Weeks
3.5	Gamification Features	January 2026 (Week 20)	February 2026 (Week 24)	5 Weeks
3.6	AI Chatbot Integration	January 2026 (Week 23)	February 2026 (Week 26)	4 Weeks
4.	Testing	February 2026 (Week 24)	March 2026 (Week 32)	9 Weeks
4.1	Non-Functional Testing	February 2026 (Week 24)	February 2026 (Week 26)	3 Weeks
4.2	Unit Testing	February 2026 (Week 25)	March 2026 (Week 27)	3 Weeks
4.3	Integration Testing	March 2026 (Week 27)	March 2026 (Week 28)	2 Weeks
4.4	System Testing	March 2026 (Week 28)	March 2026 (Week 30)	3 Weeks
4.5	Client Acceptance Testing	March 2026 (Week 29)	March 2026 (Week 31)	3 Weeks
4.6	User Acceptance Testing	March 2026 (Week 30)	March 2026 (Week 32)	3 Weeks
5.	Deployment	January 2026 (Week 23)	March 2026 (Week 30)	8 Weeks
5.1	Server Configuration	January 2026 (Week 23)	February 2026 (Week 24)	2 Weeks
5.2	Docker Containerisation	February 2026 (Week 24)	February 2026 (Week 26)	3 Weeks
5.3	Production Deployment	February 2026 (Week 26)	March 2026 (Week 28)	3 Weeks

ID	Task Name	Start	Finish	Duration
5.4	HTTPS and SSL Configuration	March 2026 (Week 28)	March 2026 (Week 30)	3 Weeks
6.	Review	March 2026 (Week 29)	April 2026 (Week 36)	8 Weeks
6.1	Sprint Retrospective	March 2026 (Week 29)	March 2026 (Week 31)	3 Weeks
6.2	Bug Fixes and Refinements	March 2026 (Week 30)	April 2026 (Week 33)	4 Weeks
6.3	FYP Report Writing	September 2025 (Week 5)	April 2026 (Week 34)	29 Weeks
6.4	Final Presentation & Submission	April 2026 (Week 33)	April 2026 (Week 36)	4 Weeks

6.3 Risk Management

Risk management was undertaken during the project lifecycle in order to find out, evaluate and alleviate any risks that may be experienced to ensure that the CyberSafe Learning Hub achieves its successful completion. The table given below provides a summary of the major risks established, their rating of likelihood and impact, and the mitigation measures implemented.

Table 6.2: CyberSafe Learning Hub Risk Management

Risk	Likelihood	Impact	Risk Analysis	Mitigation Strategy
Data loss due to local development failure	Medium	High	Hardware failure or accidental deletion could erase weeks of code, causing severe project delays and jeopardising the submission deadline.	Used Git version control with regular commits pushed to a remote GitHub repository to ensure immediate code recoverability.
Production server downtime	Low	High	If the cloud server goes offline during UAT or evaluation, users cannot test, leading to incomplete feedback and perceived system unreliability.	Deployed on DigitalOcean with Coolify's automatic restart policy; monitored uptime manually to ensure immediate resolution of crashes.
Scope creep from additional feature requests	Medium	Medium	Attempting to build too many new gamification or learning features could stretch the timeframe, leaving core requirements unfinished or buggy.	Strictly followed the defined project objectives and WBS scope; deferred non-essential enhancements to the Future Work section.

Risk	Likelihood	Impact	Risk Analysis	Mitigation Strategy
Compatibility issues across browsers and devices	Medium	Medium	If the platform layout breaks on specific browsers or smaller screens, students may struggle to complete quizzes or view infographics properly.	Conducted continuous usability testing on multiple browsers (Chrome, Firefox, Edge) and various screen sizes throughout development.
Security vulnerabilities in the web application	Medium	High	Since this is a cybersecurity platform, any successful SQL injection or XSS attack would severely damage credibility and compromise student data.	Applied HTTPS, CSRF protection, bcrypt password hashing, strict role-based access control, and validated all user inputs.
Delayed student UAT response collection	Medium	Medium	If students take too long to complete the questionnaire, there will not be enough time left to properly analyse the data for Chapter 5.	Distributed the Google Form questionnaire early during the testing phase with a strict deadline to ensure sufficient time for result synthesis.
AI chatbot providing inaccurate responses	Low	Medium	An AI providing direct answers to quizzes or giving incorrect cybersecurity advice undermines the primary learning objective of the system.	Configured the Meta AI chatbot with a strict system prompt restricting it to cybersecurity guidance without revealing direct quiz answers.

Table 6.2 reveals that risk management process focuses on proactive identification as opposed to reactive problem-solving. The project continued to have a stable forward motion by foreseeing technical failures like, loss of data, server outage, etc. and creating respective recovery plans (such as Git version control and automatic server restart policies). Moreover, the risks associated with scope creep and UAT delays were addressed by following the schedule and showing the deadlines in the form of strict adherence. In the end, this constant check into the technical vulnerabilities as well as administrative bottlenecks made sure that no single risk event had a critical impact on the project timeline and the ultimate educational platform.

6.4 Achievement

The most basic parameter of success of any software development project is its capability to meet its original objectives. This part critically analyzes how the CyberSafe Learning Hub was able to meet the three main project objectives that were set at the first planning stage. The measurement of these successes is not only on how well the features in the Laravel framework were implemented technically, but what practical results would be realized during the functional system testing as well as the subsequent User Acceptance Testing (UAT) with the target student population.

6.4.1 To Improve Cybersecurity Awareness Among Students

The first objective was to enhance the knowledge of the basic cyber threats, such as phishing, malware, and weak passwords, among students through structured and easily accessible lesson material. This has been achieved in totality.

The CyberSafe Learning Hub offers cybersecurity learning modules addressing fundamental themes associated with cyber-attacks and internet security. Each module consists of several well-organized lessons. Each lesson includes numerous content block types like text blocks, images, infographic blocks, and embedded videos, thus allowing for varied learning strategies to cater to different learners' needs.

The admin panel lets the lecturer or administrator create, edit, and modify all modules, lessons and content blocks without any technical knowledge. The content management system allows the rich media uploads and flexibility in placing the content in order so that learning material is kept up to date and relevant.

This objective is heavily supported by the findings of the User Acceptance Testing that was carried out with 54 student respondents. On Q5 ("The platform provides clear and structured lessons on key cybersecurity topics"), the response rate of 37.0% agreed and 63.0% strongly agreed, and the response rate was 100%. On Q6 ("The content is easy to understand, even for students without an IT background"), 79.6% agreed and 20.4% strongly agreed (100% positive), which confirms that the plain language and visual aids used made technical information easy to read and comprehend by non-IT students. Most significantly, Q7 ("After completing the lessons, I have a better understanding of common cyber threats") recorded one of the highest levels of agreement, with 79.6% strongly agreeing and 20.4% agreeing (100% positive), directly confirming that the lesson material improved students' cybersecurity knowledge. The Client Acceptance Testing also ensured that the modules are all-inclusive, address all the key issues, and are as detailed as required by the target student audience.

6.4.2 To Provide Interactive and Engaging Cybersecurity Education

The second objective was to cease passive learning and offer interactive features, such as quizzes, multiple-choice questions, and visual data, such as infographics, that will motivate the students to actively engage in the process. This has been accomplished completely.

The platform has an in-built quiz system that accommodates multiple-choice questions that have adjustable correct answers. Learners are given instant feedback on every submission of quizzes, which is displayed as their score and the questions they answered correctly or incorrectly. The threshold to pass is 85% and the students can retake till they pass.

Lessons are designed to accommodate various learning requirements with the use of infographics, pictures, and embedded videos in addition to textual explanations. The site also features an AI-enhanced cybersecurity chatbot that students can chat with during quizzes to get clarification about the concepts, although the chatbot does not actually give out quiz answers. This promotes self-thinking and yet provides the guidance.

Integration and system testing ensured that all quiz workflows (including question display up to calculating scores and providing feedback) were working properly and free of errors. The reaction of the users to User Acceptance Testing also confirms that the design of the quiz and interactive features are effective in attracting the students.

The effectiveness of the interactive features is also affirmed by the results of the User Acceptance Testing. Regarding Q8 ("The quizzes are well-designed and engaging to complete"), 79.6% agreed and 20.4% strongly agreed (100% positive), supporting the view of the multiple-choice quiz format with an 85% pass threshold and immediate feedback as a well-structured assessment tool. On Q9 ("The platform uses interactive and visual elements that make learning more engaging"), 79.6% strongly agreed and 20.4% agreed (100% positive), one of the highest ratings in the survey, the integration of infographics, images and embedded videos played an important role in engaging students. On Q10, ("I receive immediate and clear feedback after submitting a quiz") 79.6% of the respondents agreed and 20.4% strongly agreed (100% positive), confirming the perceived transparency of the quiz result page as showing the score, a percentage, and the pass/fail status and feedback on each question was clear and useful to all the respondents.

6.4.3 To Motivate Students to Apply Cybersecurity Skills in Practice

The third objective was to maintain student attention and promote the continued use of cybersecurity knowledge by introducing the elements of gamification, including points, the ability to track progress, and badges upon the achievement of a milestone. This has been accomplished to the latter.

CyberSafe Learning Hub gives students points after every lesson and passing of a quiz. All students are ranked by a leaderboard based on the number of points, and it creates a healthy competition environment. After finishing all the lessons and passing all the quizzes in a module, the students get a module-specific badge, which is forever shown on their earned badge page.

After all modules in a category have been completed, the system automatically creates and sends out a PDF certificate with the full name of the student, category name, date of completion. The students are able to get their certificates on the certificate index page of the platform.

The lesson level is used to track progress with the `user_lesson_progress` table and students can see their individual progress on the student dashboard. The admin analytics page provides the administrator with the overall performance of the classes in terms of its completion and number of active students.

The User Acceptance Testing shows that the gamification features were received well. In case of Q11 ("Points are correctly awarded after completing lessons and quizzes, and I can see my updated score"), 37.0% strongly agreed and 63.0% agreed (100% positive) it can be said that students were satisfied that the points system was working properly and motivated them. In case of Q12 ("The platform awards badges when I reach milestones, and these badges are clearly displayed on my profile"), 37.0% answered yes, and 63.0% answered strongly yes (100% positive), which means that the badge milestones are seen as meaningful and visible by students. In the case of Q13 ("The progress tracking feature motivates me to continue learning and complete more lessons"), 61.1% respondents agreed and 38.9% strongly agreed (100% positive), which confirms that the dashboard progress tracking motivated them to keep learning and take more lessons. Client Acceptance Testing also confirmed that the points and badges are actually useful, that students are more eager to complete the modules with it and that badges provide students with the feeling that they have achieved something.

6.5 Constraint and Limitation

Although the CyberSafe Learning Hub was able to meet its set goals and objectives and provide an operational educational platform, there is no software development project that is boundless. It is important to note the limitations that the project faced during the lifecycle in order to effectively assess the current capabilities of the system. The main cause of these restrictions was the strong time limitations of the Final Year Project (FYP) schedule, the scope of the initial requirements, and the reliance on the free or third-party external services. The main limitations that characterized the scope of the created prototype are outlined below:

6.5.1 Limited Cybersecurity Topic Coverage

As it stands now, the platform focuses on a range of fundamental cybersecurity issues that have practical implications on digital safety for everyday internet users. Although they constitute a wide range of commonly encountered cyber threats for regular people, the learning materials do not go into advanced topics like network security or cryptography, nor do they explore any sophisticated social engineering techniques. The reasons for such a limited scope are mainly connected to the severe time limitations within which one is supposed to develop a minimum viable product (MVP) during a final year project.

6.5.2 No Real-Time Collaboration or Discussion

The existing platform encourages simple communication in form of asynchronous lesson comments, where students are able to pose inquiries on individual content blocks. It however lacks real time collaboration features like live chat interfaces, active group discussion boards, and peer to peer communications. This is a weakness of the social learning dimension of the site, which may diminish the community feeling among students enrolled in the course at the same time.

6.5.3 English-Only Content

At present, every component of the platform such as lesson material, quiz questions, navigation within the interface, and responses of the chatbot are all exclusively in English. This creates a possible language barrier to students who might feel more at ease learning complicated technical aspects in Bahasa Melayu or their own language, and this could influence the rate of comprehension among non-native speakers of English.

6.5.4 Manual Content Management

Although the administrative panel has a user-friendly drag and drop content editor, the administrator is required to create and input all new lesson content, quizzes and modules manually. The site does not have any bulk-import options (csv, or json import) or content templates. This limitation renders the initial big course population tiresome and time consuming to lecturers.

6.5.5 Dependency on Third-Party AI API

The AI chatbot that is deployed inside the platform depends on a third-party, external AI service (via the Groq API with the use of the Meta Llama 3.3 70B Versatile model). As a result, any unexpected service failures, the rate limits of the API being changed unpredictably, or the model being degraded by the provider would immediately and directly affect the availability and behaviour of the chatbot. This brings on board the element of failure which is not directly under the control of the developer.

6.6 Future Work and Recommendation

Software development is a highly iterative process and the initial release of the CyberSafe Learning Hub is one of the pillars around which a more robust ecosystem can be formed. According to the limitations that were determined in the section above, and the positive feedback that was provided by both the project supervisor and the students in the process of User Acceptance Testing, a number of areas have been identified as requiring improvement.

6.6.1 Expand Cybersecurity Content

To expand the educational reach and applicability of the platform, more learning modules ought to be created to span a broader range of digital threats. Some of the future subjects might be social engineering psychology, network security fundamentals, threats to a public Wi-Fi, mobile device security, and cloud data protection. Diversifying the curriculum would make the platform a comprehensive cybersecurity learning platform to the students.

6.6.2 Multilingual Support

It would be strongly suggested to implement a powerful localisation system (such as the native Localisation functionalities of Laravel with specific lang files). The introduction of the Bahasa Melayu language would instantly make the site more inclusive. This would make sure that proficiency in language is not a bottleneck to gaining the important cybersecurity knowledge and thus the platform could be made available to a significantly broader population of students.

6.6.3 Live Discussion and Peer Interaction

In order to improve the social learning experience, real-time collaboration features should be implemented in the future. This may be in the form of an integrated discussion board, specific student group chats or a more sophisticated peer commenting system on separate lesson blocks. Creating an atmosphere in which students are able to talk about the latest cyber threats or seek the assistance of other students would go a long way into improving active participation and retention of knowledge.

6.6.4 Adaptive Learning Pathways

The most effective future improvement would be the introduction of an algorithm that can dynamically examine the performance of a student in his quizzes to determine the most vulnerable points in his knowledge. On the basis of such data, the platform would suggest particular lessons or create specialized revision quizzes automatically. Such a move towards adaptive, individualised learning would radically enhance the individual knowledge retention as opposed to a rigid curriculum.

6.6.5 Bulk Content Import

In order to reduce the workload on the lecturers, it is important to develop a bulk content import feature. The option of uploading complete modules, lessons and quiz question bank using standardised CSV or JSON files would also save a lot of time on manual data entry. The feature is essential in case the platform is to be scaled to dozens of courses in various faculties of universities.

6.6.6 Mobile Application

Although the existing web platform is responsive, it is suggested to make a specific companion mobile application (iOS and Android-based) based on a cross-platform framework like Flutter or React Native. The cybersecurity content would be immediately available on the go in a native mobile application, and students could use their free time on the platform (micro-lessons or quizzes) as they are commuting to college, which would also mean spending more time on the platform.

6.6.7 Advanced Analytics and Reporting

The existing administrator analytics dashboard should be expanded to include much deeper insights. The next version must include more detailed reporting of individual student performance, an option to export the data in CSV format, and graphical trends of the progress of the classes over time. The availability of granular data to the lecturers will also allow them to detect students who are struggling promptly and modify their teaching methods.

6.6.8 Gamification Enhancements

The gamification system of the platform should be improved and extended to achieve even greater motivation of the students and ensure long-term attraction. The next league of mechanics may include streaks of daily logins, time-limited challenges on weekends or challenges inside a team related to physical campus activities. Moreover, the achievement levels (e.g. Bronze, Silver, Gold badges) should also be introduced so that the students can have a constant set of goals even when the core curriculum is already finished.

6.7 Conclusion

CyberSafe Learning Hub was created, tested, and implemented successfully as a fully working web-based cybersecurity awareness training program. The system is developed on the Laravel framework and has structured lesson information, interactive quizzes with real-time feedback, gamification elements (points, badges, leaderboards, and certificates), an AI-driven cybersecurity chatbot, and an extensive administrator management dashboard.

All three project objectives were met in full: the platform provides organized and available cybersecurity awareness material, introduces an interactive and engaging education system, and manages to encourage student engagement through gamification and progress tracking systems. The outcomes of the testing will make the system technologically sound, complete and will meet the expectations of the administrator and the end users.

Though some drawbacks were noted such as the absence of coverage of numerous issues, the use of English only, and the use of external APIs, they are largely the scope and time constraints that can be addressed in the next versions. The recommendations provided in section 6.6 present a reasonable overview of how the platform can be further developed and improved when compared to the existing version.

To conclude, the CyberSafe Learning Hub is a significant addition to cybersecurity education in the university setting, and it proves that an interactive, engaging, and gamified learning environment can be successfully applied to sensitize cybersecurity awareness among students.

Appendix A – Questionnaire & Interview Questions

i. Questionnaire Question (Pre-Development)

CyberSafe Learning Hub Questionnaire

Assalamualaikum and hi, my name is Muhammad Imran Bin Mohd Hanifah from University Poly-Tech Malaysia.

This questionnaire is part of my Final Year Project (FYP) titled "CyberSafe Learning Hub", which aims to develop an interactive, web-based platform to improve cybersecurity awareness among college students.

The purpose of this survey is to understand students' current level of cybersecurity awareness, learning preferences, and expectations for an educational platform that includes gamified and interactive learning elements.

Your responses will help guide the development of a more engaging and effective cybersecurity awareness system.

All responses are anonymous and will be used strictly for academic purposes.

kl2408016649@student.upm.edu.my [Switch account](#)

Not shared

** Indicates required question*

1. Age *

☐ 18–20

☐ 21–23

☐ 24–26

☐ Above 26

2. Gender *

☐ Male

☐ Female

3. Program of Study *

☐ IT-related

☐ Non-IT related

4. Frequency of Internet Use *

☐ Less than 2 hours per day

☐ 2-4 hours per day

☐ 5-8 hours per day

☐ More than 8 hours per day

5. What is your current level of knowledge regarding basic cybersecurity practices *
(e.g., strong passwords, phishing awareness)?

- ☐ Very Low
- ☐ Low
- ☐ High
- ☐ Very high

6. Have you ever experienced a cybersecurity incident such as phishing, malware infection, or data breach? *

- ☐ Yes
- ☐ No

7. How often do you participate in cybersecurity awareness programs or training? *

- ☐ Never
- ☐ Rarely
- ☐ Occasionally
- ☐ Frequently

8. Do you believe cybersecurity awareness is important for university students? *

- ☐ Yes
- ☐ No

9. How confident are you in protecting your personal data and online accounts? *

- ☐ Not confident
- ☐ Slightly confident
- ☐ Confident
- ☐ Very confident

10. What type of learning method do you prefer when learning about cybersecurity? (Select one or more) *

- ☐ Videos
- ☐ Articles
- ☐ Interactive modules
- ☐ Gamified learning
- ☐ Quizzes
- ☐ Other: _____

11. How often do you apply safe online practices *

- ☐ Never
- ☐ Rarely
- ☐ Sometimes
- ☐ Often
- ☐ Always

12. Are you aware of practices such as two-factor authentication and regular password updates? *

- ☐ Yes
- ☐ No

13. Would you be interested in using an online platform that provides cybersecurity awareness and educational content? *

- ☐ Yes
- ☐ No

14. How important do you think user authentication is for such a platform? *

☐ Not important

☐ Slightly important

☐ Moderately important

☐ Important

☐ Very important

15. How motivating would gamification features (points, badges, challenges) be for your learning experience? *

☐ Not motivating

☐ Slightly motivating

☐ Motivating

☐ Very motivating

16. Which features would you find most useful to be implemented in Cybersafe Learning Hub? (Select one or more) *

☐ Quizzes

☐ Tutorials

☐ Gamified lessons

☐ Progress tracking

☐ Leaderboards

☐ Other: _____

17. How useful do you think it would be if the platform allowed students to track their learning progress and achievements? *

☐ Not useful

☐ Slightly useful

☐ Moderately useful

☐ Useful

☐ Very useful

18. How important is it that the web platform loads quickly? *

☐ Not important

☐ Slightly important

☐ Moderately important

☐ Important

☐ Very important

19. The interface should be simple and user-friendly, even for non-IT students. *
How much do you agree?

☐ Strongly disagree

☐ Disagree

☐ Agree

☐ Strongly agree

20. Do you think your learning data should be encrypted and securely stored? *

☐ Yes

☐ No

ii. Interview Question (Pre-Development)

Question
1. In your opinion, how important is cybersecurity awareness for college students?
2. What are the most common cybersecurity challenges or issues you observe among students?
3. Have you encountered any cases where students were affected due to a lack of cybersecurity knowledge?
4. How effective do you think the university's current cybersecurity awareness efforts are?
5. What learning methods do you find most effective in teaching students about cybersecurity?
6. Do you think a platform such as the CyberSafe Learning Hub could improve students' understanding of cybersecurity?
7. What specific features or functions would you recommend to make the platform more engaging for students?
8. From an administrative perspective, how important is Role-Based Access Control (RBAC) in managing lecturer and student permissions within the system?
9. Should cybersecurity awareness be integrated across all academic disciplines, or only within IT-related courses?
10. What advice would you give to ensure the CyberSafe Learning Hub supports learning and long-term awareness?

iii. Questionnaire Questions (Post-Development)

CyberSafe Learning Hub – User Acceptance Testing (UAT)

Thank you for participating in the User Acceptance Testing for the CyberSafe Learning Hub. Before answering this questionnaire, please visit the platform using the link below, log in, and explore all the features available. Once you have had a chance to use the platform, please evaluate each statement based on your experience.

Platform Link: <https://cybersafelearninghub.app/>

geniusmonster559@gmail.com [Switch account](#) 

 Not shared

* Indicates required question

1. What is your age range? *

☐ 18–20

☐ 21–23

☐ 24–26

☐ 27 and above

2. What is your gender? *

☐ Male

☐ Female

Next

Clear form

CyberSafe Learning Hub – User Acceptance Testing (UAT)

geniusmonster559@gmail.com [Switch account](#)

Not shared

* Indicates required question

For the following questions, please rate each item on a scale of 1 to 4.

Response Scale (Linear Scale 1–4):

- 1 = Strongly Disagree
- 2 = Disagree
- 3 = Agree
- 4 = Strongly Agree

3. I was able to successfully register and log in to the platform (manually or via Google) without any issues. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

4. The platform's interface is user-friendly and easy to navigate without requiring technical assistance. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

5. The platform provides clear and structured lessons on cybersecurity topics such as phishing, malware, and weak passwords. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

6. The cybersecurity content is presented in a way that is easy to understand, even for students without an IT background. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

7. After completing the lessons, I have a better understanding of common cyber threats and how to protect myself online. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

8. The quizzes at the end of each lesson are well-designed and engaging to complete. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

9. The platform uses interactive and visual elements (e.g., infographics, images, videos) that make the learning experience more engaging.

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

10. I receive immediate and clear feedback after submitting a quiz, allowing me to understand my performance. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

11. Points are correctly awarded after completing lessons and quizzes, and I can see my updated score on my profile/dashboard. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

12. The platform awards badges when I reach milestones, and these badges are clearly displayed on my profile. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

13. The progress tracking feature (e.g., progress bar or dashboard) motivates me to continue learning and complete more lessons. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

14. I can view and complete cybersecurity lessons and quizzes smoothly without encountering errors. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

15. My learning progress (completed lessons, quiz scores, badges) is accurately recorded and displayed on my dashboard. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

16. Pages on the platform load quickly (within 5 seconds) under normal conditions. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

17. I am confident that my personal information and progress data are securely stored and protected on the platform. *

1 2 3 4

Strongly Disagree ☐ ☐ ☐ ☐ Strongly Agree

iv. Interview Questions (Post-Development)

Interview Question
Are the cybersecurity lessons and modules comprehensive and appropriate for the target student audience?
Does the platform cover all essential cybersecurity topics that students should learn?
Does the platform effectively bridge the knowledge gap for students with little to no prior cybersecurity awareness?
Are the quizzes and interactive elements effective tools for reinforcing cybersecurity concepts?
Are the visual materials and multimedia content adequate to keep students engaged?
Does the platform provide sufficient feedback mechanisms for assessing student understanding?
Are the gamification features (points, badges, progress tracking) effective in motivating students?
Is the badge and milestone system meaningful enough to encourage continued participation?
Does the progress tracking dashboard give a clear and accurate picture of student progress?
Were you able to create, edit, and delete lessons, modules, and quizzes without errors?
Does the admin dashboard provide all the information needed to monitor and review student performance?
Is the role-based access control working correctly for students and admins?
Did you experience any performance issues while managing lessons or viewing the dashboard?
Is the admin interface intuitive enough to manage all platform features without technical training?
Are you confident that the system reliably stores all student data, progress, and credentials securely?

Appendix B – User Manual



CyberSafe Learning Hub

USER MANUAL

MUHAMMAD IMRAN BIN MOHD HANIFAH

BIT (HONS) IN CYBER SECURITY

**FACULTY OF COMPUTING AND MULTIMEDIA
UNIVERSITY POLY-TECH MALAYSIA**

9TH MARCH 2026

Table of Contents

1. Introduction	4
2. Accessing the System	5
3. Admin Guide	6
3.1 Admin Login.....	6
3.2 Admin Dashboard	7
3.3 Managing Categories	8
3.4 Managing Modules	10
3.5 Managing Lessons	13
3.6 Managing Lesson Content.....	15
3.7 Managing Quizzes.....	19
3.8 Managing Questions & Answers	22
3.9 Managing Users	24
3.10 Analytics	26
3.11 Sending Notifications to Students	28
4. Student Guide	30
4.1 Registration & Login	30
4.2 Onboarding.....	32
4.3 Student Dashboard.....	33
4.4 Browsing Modules	35
4.5 Viewing a Lesson	37
4.6 Completing a Lesson	38
4.7 Taking a Quiz.....	39
4.8 AI Chatbot.....	41
4.9 Viewing Quiz Results.....	42
4.10 Badges	44
4.11 Certificates.....	45
4.13 Account Settings.....	47
5. System Requirements.....	48

1. Introduction

CyberSafe Learning Hub is a web-based cybersecurity education platform designed to help students learn about cybersecurity topics through structured lessons, interactive quizzes, and gamification features. The system supports two types of users:

- **Administrator** — responsible for managing all platform content, monitoring student progress, and configuring the system.
- **Student** — accesses learning content, completes lessons and quizzes, and earns badges and certificates.



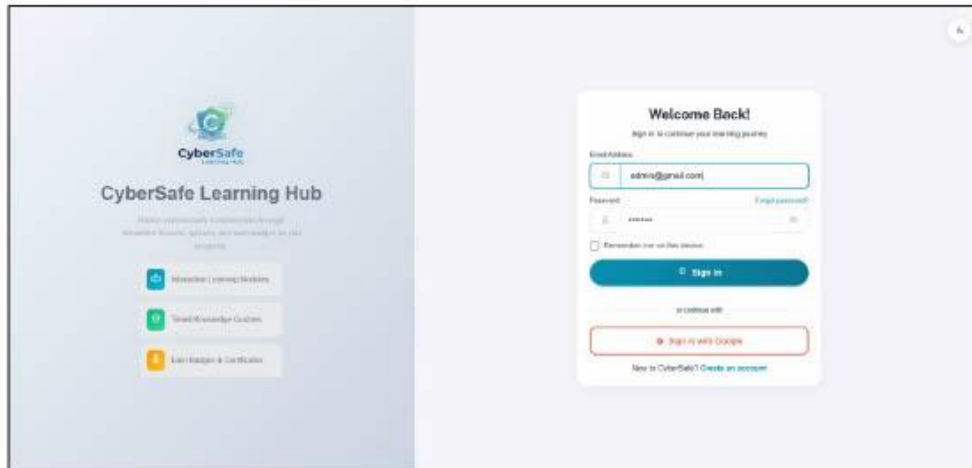
2. Accessing the System

1. Open a web browser (Google Chrome, Firefox, or Microsoft Edge recommended).
2. Navigate to <https://cybersafelearninghub.app/>.
3. The landing page will be displayed, showing an overview of the platform.
4. Click **Sign In** to proceed to the login page.



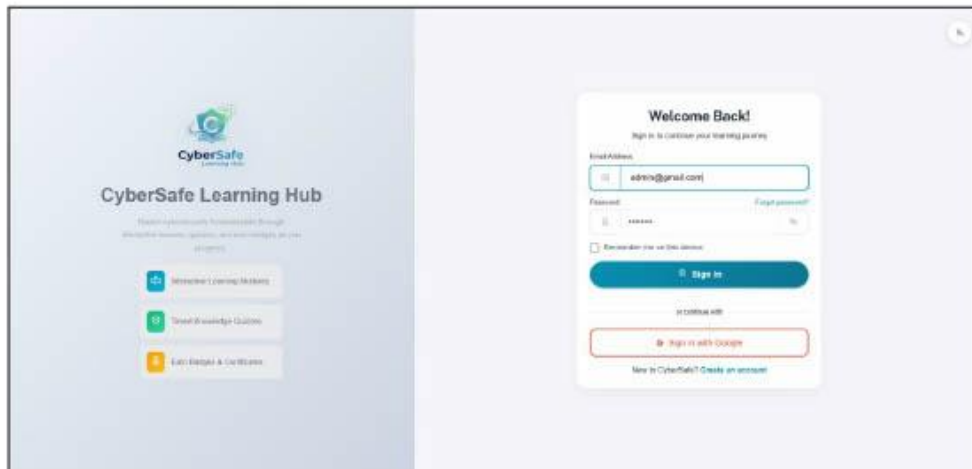
3. Admin Guide

3.1 Admin Login



1. On the login page, enter your **email address** and **password**.
2. Click **Sign In**.
3. The system will verify your credentials. If your account has the **Admin** role, you will be automatically redirected to the **Admin Dashboard**.

3.2 Admin Dashboard



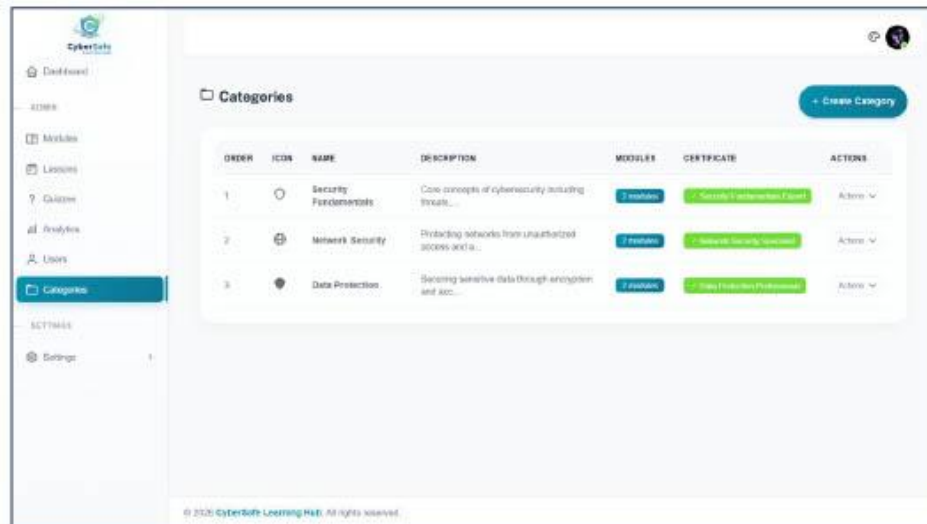
The Admin Dashboard provides a summary of the platform's current state. The following information is displayed:

Section	Description
Total Students	Number of registered student accounts
Total Modules	Number of learning modules created
Total Lessons	Number of lessons across all modules
Total Quizzes	Number of quizzes created
Pass Rate	Percentage of quiz attempts that scored 85% or above
Average Score	Average quiz score percentage across all attempts
Badges Earned	Total badges awarded to students
Recent Quiz Attempts	Latest 10 quiz submissions with student name and score
Top Performing Students	Top 5 students ranked by number of badges earned
Recent Student Activity	Latest 5 lesson completions by students

3.3 Managing Categories

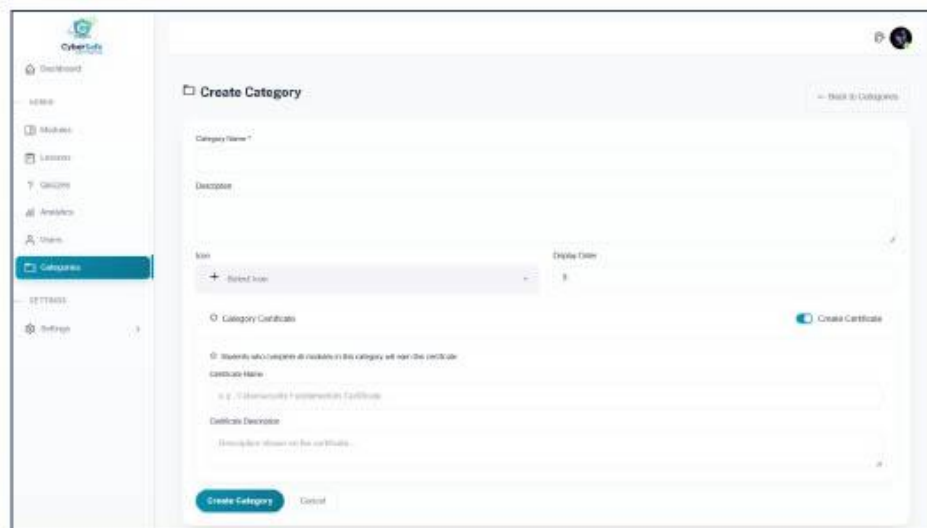
Categories are the top-level groupings for learning content. Each category can contain multiple modules and has one associated certificate.

- View All Categories



1. Click **Categories** in the sidebar.
2. A list of all categories is displayed with their name, icon, and description.

- Create a New Category



1. Click **Categories** → **Create Category**.
2. Fill in the following fields:
 - **Name** — the category title (e.g., *Security Fundamentals*)
 - **Description** — a brief explanation of the category
 - **Icon** — an emoji to represent the category (e.g., 🛡️)
3. Click **Save**.

- **Edit a Category**

1. In the category list, click **Edit** next to the category you want to update.
2. Modify the fields as needed.
3. Click **Update**.

- **Delete a Category**

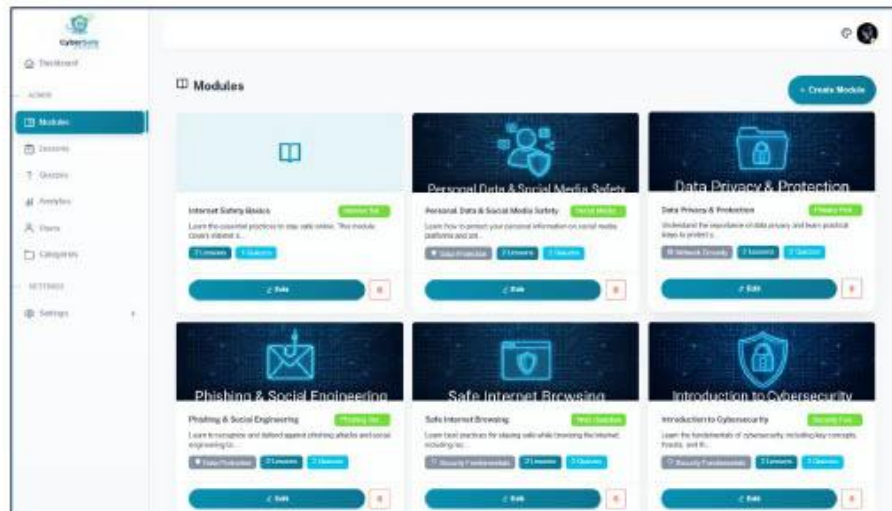
ORDER	ICON	NAME	DESCRIPTION	MODULES	CERTIFICATE	ACTIONS
1	🛡️	Security Fundamentals	Give concepts of cybersecurity including threats,...	2 modules	Security Fundamentals E-quest	Edit Delete
2	🔒	Network Security	Protecting networks from unauthorized access and a...	2 modules	Network Security E-quest	Edit Delete
3	🔑	Data Protection	Securing sensitive data through encryption and acc...	2 modules	Data Protection E-quest	Edit Delete

1. In the category list, click **Delete** next to the category.
2. Confirm the deletion. All modules, lessons, quizzes, and the associated certificate will also be removed.

3.4 Managing Modules

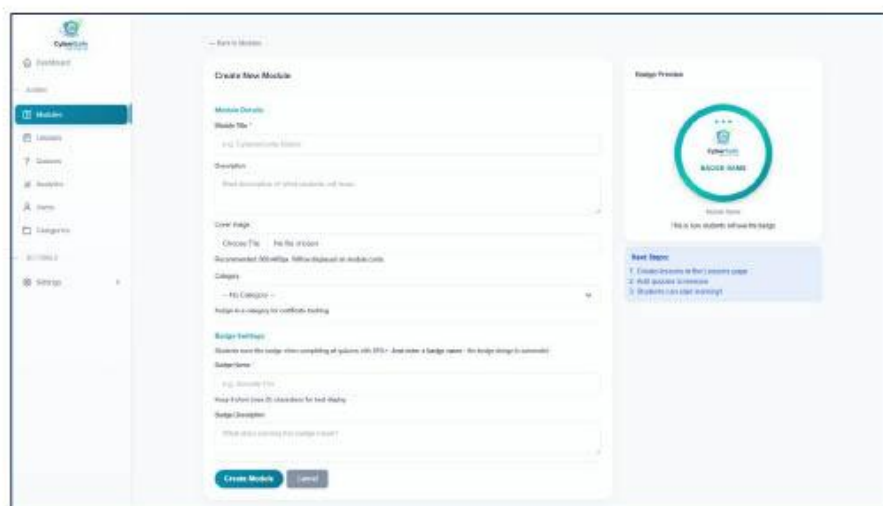
Modules are learning units within a category. Each module contains multiple lessons and has one associated badge that is awarded to students upon completion.

- View All Modules



1. Click **Modules** in the sidebar.
2. All modules are listed with their category, number of lessons, and associated badge.

- Create a New Module

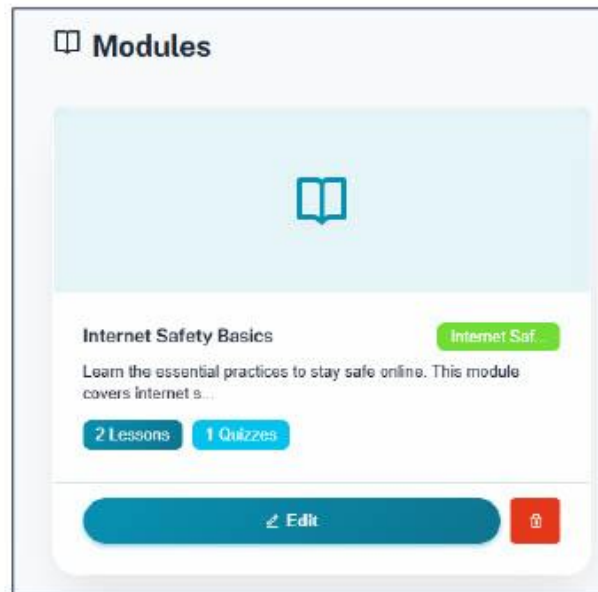


1. Click Modules → Create Module.
2. Fill in the following fields:
 - **Category** — select the parent category from the dropdown
 - **Title** — the module name
 - **Description** — a summary of what the module covers
 - **Cover Image** — *(optional)* upload an image to represent the module
 - **Badge Name** — the name of the badge students will earn
 - **Badge Description** — *(optional)* a description of the badge
 - **Badge Icon** — an emoji for the badge (defaults to 🏆 if left blank)
 - **Badge Image** — *(optional)* upload a custom badge image
3. Click **Save**. The module and its badge are created simultaneously.

- **Edit a Module**

1. In the module list, click **Edit** on the module you want to update.
2. All module and badge fields can be updated.
3. Click **Update**.

- Delete a Module

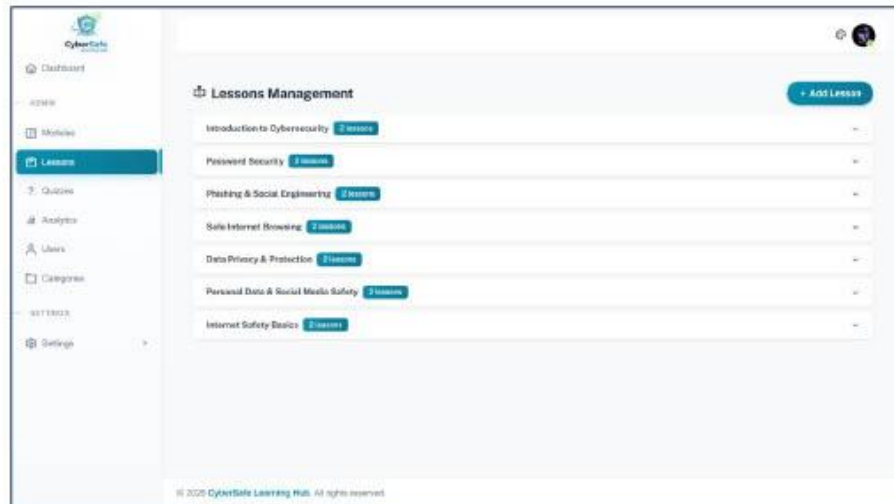


1. Click **Delete** next to the module.
2. Confirm the deletion. All associated lessons, quizzes, and the badge will also be removed.

3.5 Managing Lessons

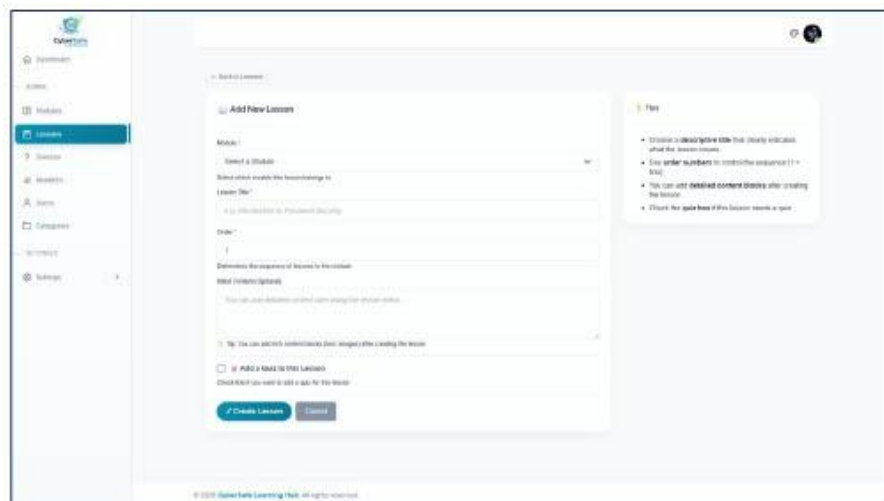
Lessons are the individual pieces of educational content within a module.

- View All Lessons



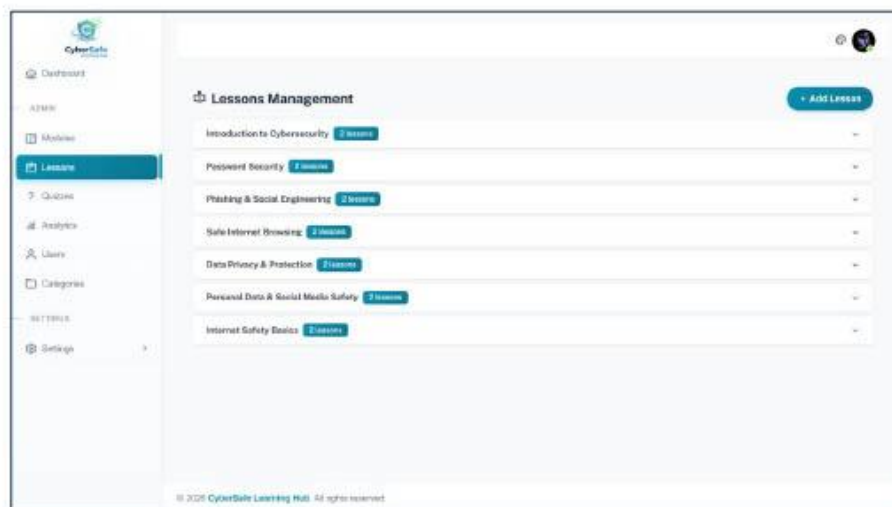
1. Click **Lessons** in the sidebar.
2. All lessons are listed with their module, title, and order.

- Create a New Lesson



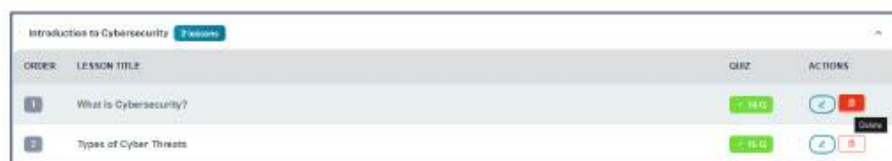
1. Click **Lessons** → **Create Lesson**.
2. Fill in the following fields:

- **Module** — select the parent module from the dropdown
 - **Title** — the lesson name
 - **Order** — the display order of the lesson within the module (lower number = appears first)
3. Click **Add a Quiz to this Lesson** checkbox to add a quiz under the lesson.
 4. Click **Save**. The lesson is created and will be listed under the selected module.
- **Edit a Lesson**



1. In the lesson list, click **Edit** on the lesson.
2. Update the title, module, or order as needed.
3. Click **Update**.

- **Delete a Lesson**

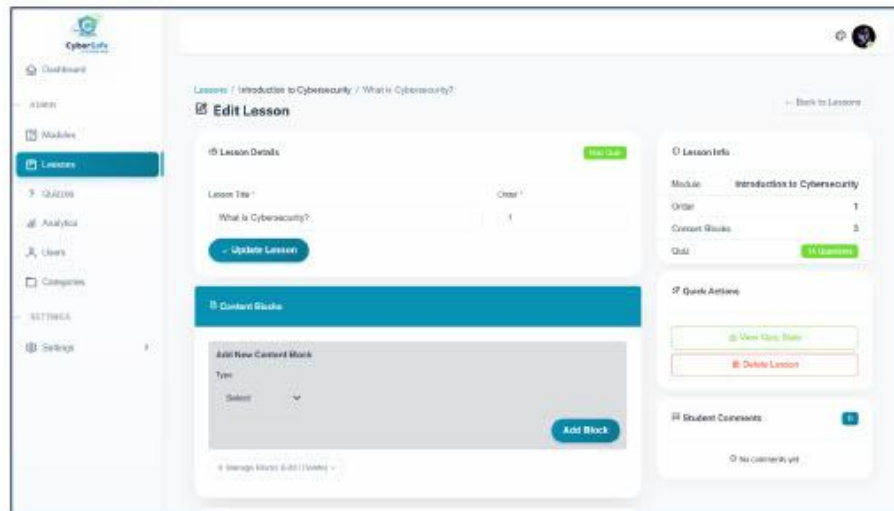


1. Click **Delete** next to the lesson.
2. Confirm the deletion. All associated lesson content and the attached quiz will also be removed.

3.6 Managing Lesson Content

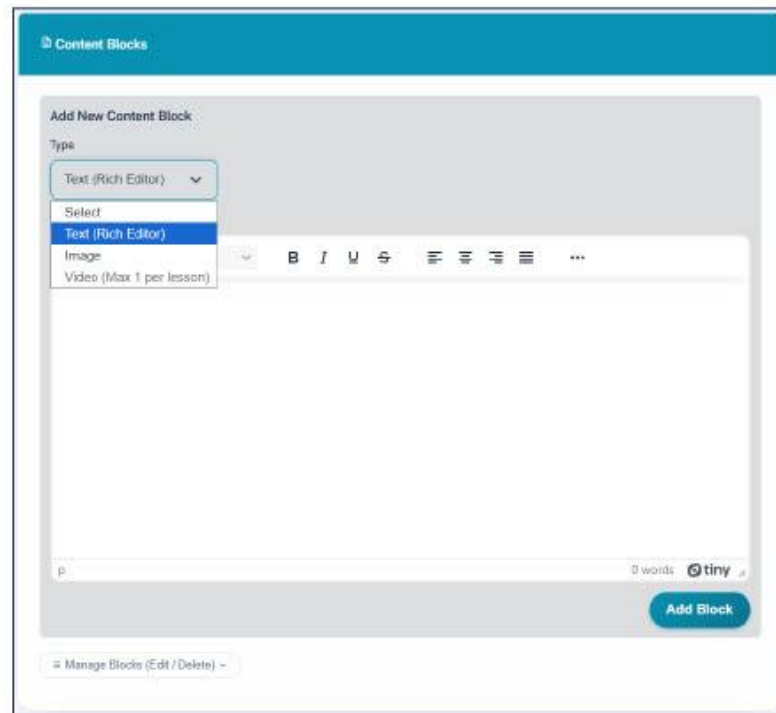
Lesson content refers to the actual educational material displayed to students. Each lesson can contain multiple content blocks of different types.

- Access the Lesson Content Editor



1. Go to **Modules** → click the module title → click the lesson name. Or go to **Lessons** → click Edit on a lesson.
2. The lesson content editor page will open.

- Add a Content Block



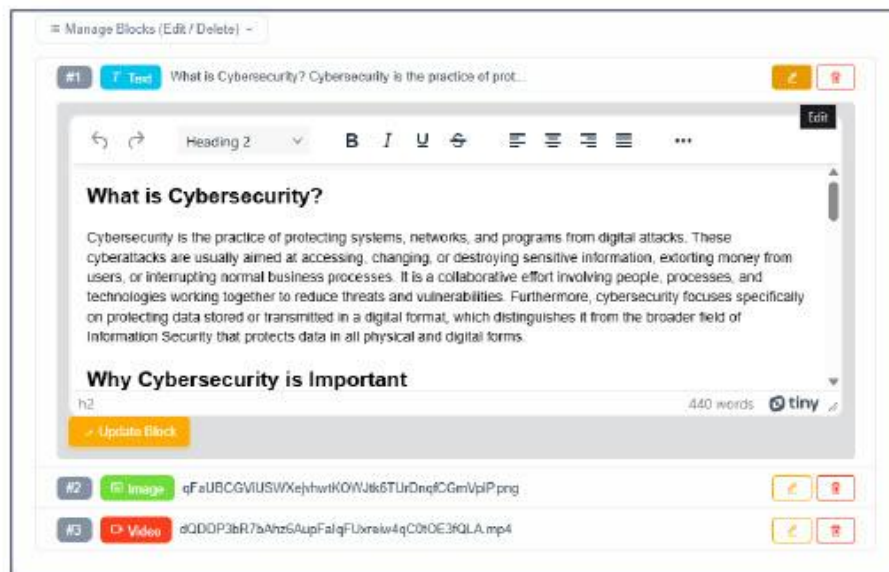
1. On the lesson content editor, click **Type** dropdown.
2. Select the block type:
 - **Text** — rich HTML text content
 - **Image** — upload an image file
 - **Video** — embed a video URL
3. Enter the content for the block.
4. Click **Add Block**.

- Reorder Content Blocks



1. Drag and drop blocks to reorder them.

- Edit a Content Block



1. Click **Edit** on the block you want to modify.
2. Update the content.
3. Click **Save**.

- Delete a Content Block



1. Click **Delete** on the block.
2. Confirm the deletion.

3.7 Managing Quizzes

Each lesson has one associated quiz. The quiz is automatically linked to the lesson when created.

- View All Quizzes

QUIZ TITLE	MODULE / LESSON	QUESTIONS	ATTEMPTS	PASS RATE	ACTIONS
Internet Safety Basics Quiz (8 marks)	Internet Safety Basics Protecting Personal Information	8	15	93%	Manage
Safe Sharing & Data Collection Quiz (15 marks)	Personal Data & Social Media Safety Safe Sharing & Data Collection Awareness	15	16	94%	Manage
Digital Footprint & Privacy Quiz (15 marks)	Personal Data & Social Media Safety Your Digital Footprint & Privacy Settings	15	16	94%	Manage
Data Privacy Quiz (15 marks)	Data Privacy & Protection Understanding Data Privacy	15	16	94%	Manage
Protecting Personal Info Quiz (15 marks)	Data Privacy & Protection Protecting Your Personal Information	15	16	94%	Manage
HTTPS Security Quiz (15 marks)	Safe Internet Browsing Secure Websites & HTTPS	15	16	94%	Manage
Safe Downloads Quiz (15 marks)	Safe Internet Browsing Avoiding Malware & Unwanted	15	16	94%	Manage
Password Management Quiz (15 marks)	Password Security Password Managers & 2FA	15	16	94%	Manage
Phishing Recognition Quiz (15 marks)	Phishing & Social Engineering	15	16	94%	Manage

1. Click **Quizzes** in the sidebar.
2. All quizzes are listed with their linked lesson and total number of questions.

- Create a New Quiz

 Add New Lesson

Module *

Select a Module

Select which module this lesson belongs to

Lesson Title *

e.g. Introduction to Password Security

Order *

1

Determines the sequence of lessons in the module

Initial Content (Optional)

You can add detailed content later using the lesson editor...

Tip: You can add rich content blocks (text, images) after creating the lesson

☒ Add a Quiz to this Lesson

Check this if you want to add a quiz for this lesson

Quiz Title *

e.g. Password Security Quiz

You can add questions to the quiz after it's created

✓ Create Lesson

Cancel

1. Quizzes are created by checking the **Add a Quiz to this Lesson** checkbox on the create lesson page.
2. Then, the quiz will appear on the quizzes list page.

- View Quiz Results

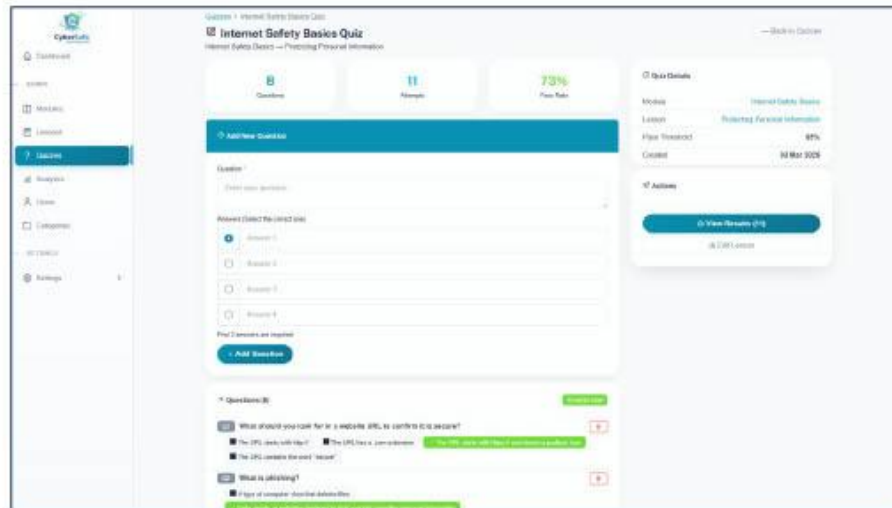
HTTPS Security Quiz			
Lesson: Secure Websites & HTTPS			
STUDENT	SCORE	STATUS	ATTEMPTED AT
Ahmad Firdaus bin Zulkifli	15/15	Passed	19 Mar 2020, 11:40
Nurul Aina binti Hanisah	10/15	Failed	21 Mar 2020, 15:23
Shi Nur Aayyah binti Kamal	15/15	Passed	20 Mar 2020, 19:42
Farah Nabillah binti Yusoff	13/15	Passed	21 Mar 2020, 06:52
Nur Hidayah binti Mohd Nizar	15/15	Failed	20 Mar 2020, 04:57
Khalid Anwar bin Ismail	15/15	Failed	22 Mar 2020, 08:36
Halizuddin bin Musa	15/15	Failed	20 Mar 2020, 20:59
Razli Aqmar bin Zenuddin	13/15	Passed	20 Mar 2020, 08:38
Chenah Arfan bin Mohd Razli	12/15	Failed	20 Mar 2020, 10:23
Luzmanul Hakim bin Tahir	12/15	Failed	19 Mar 2020, 22:40
Muhammad Zikri bin Nordin	12/15	Passed	19 Mar 2020, 13:50

1. In the quiz list, click **Results** on a quiz.
2. A summary of all student attempts is displayed, including scores and pass/fail status.

3.8 Managing Questions & Answers

Questions and their answer choices are managed directly from the quiz detail page.

- Access the Quiz Detail Page



1. Go to **Quizzes** → click on the quiz title.

- Add a Question

1. On the quiz detail page, go to **Add New Question** form.

2. Enter the question text.
3. Add at least **2 answer choices**. For each choice:
 - Enter the answer text
 - Tick the checkbox to mark it as the **correct answer**
4. Click Add Question.

Important: Each question must have exactly one correct answer marked.

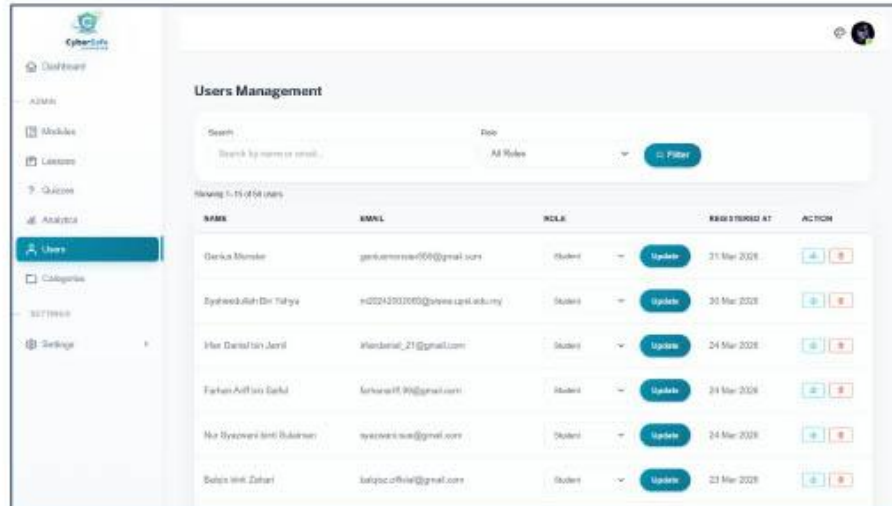
- Delete a Question



1. On the quiz detail page, click **Delete** next to the question.
2. Confirm the deletion. All answer choices for that question will also be removed.

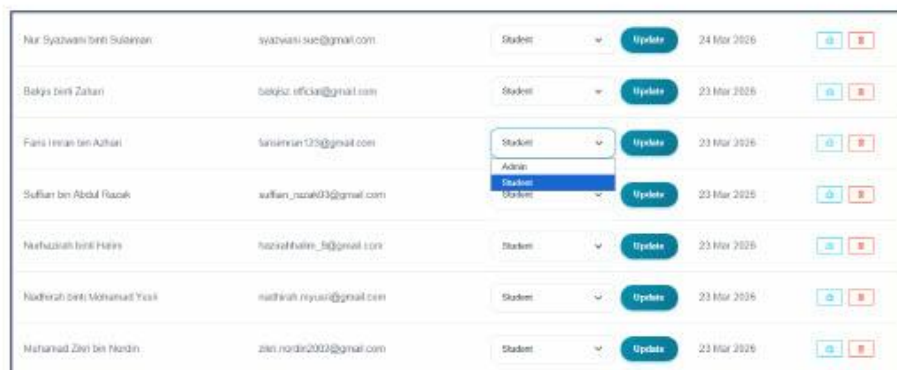
3.9 Managing Users

- View All Users



1. Click **Users** in the sidebar.
2. All registered users are listed with their name, email, role, and registration date.
3. Use the **search bar** to find a user by name or email.
4. Use the **role filter** to display only Admins or only Students.

- Change a User's Role



1. In the user list, locate the user.
2. In the **Role** dropdown next to the user, select the new role (**Admin** or **Student**).
3. Click **Update Role**. The change takes effect immediately.

- Delete a User

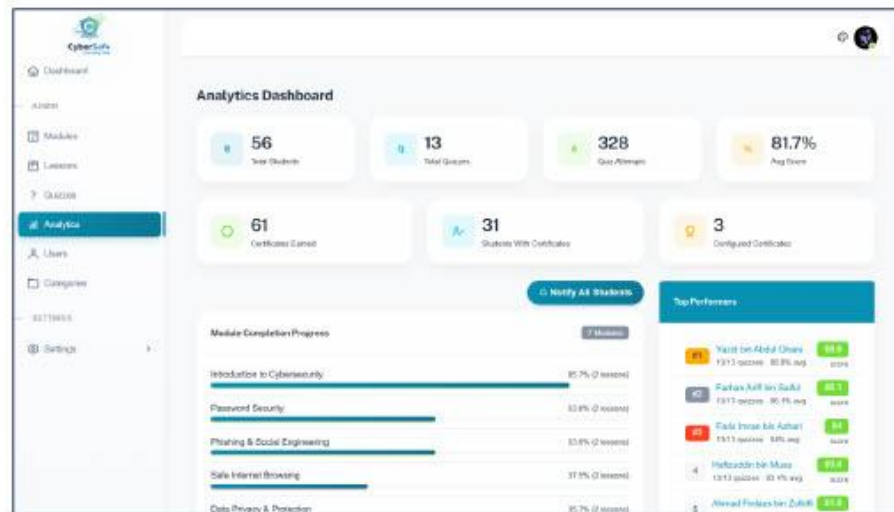
Nur Syazwani binti Sulaiman	syazwanisul@gmail.com	Student	Update	24 Mar 2025	 
Rafiqz binti Zahari	rafiqz_official@gmail.com	Student	Update	23 Mar 2025	 
Fahri Izzah bin Azhari	fahriahad23@gmail.com	Student	Update	23 Mar 2025	 
Soffian bin Abdul Razak	soffian_razak02@gmail.com	Student	Update	23 Mar 2025	 
Nurhanisah binti Habin	nurhanisah_hb@gmail.com	Student	Update	23 Mar 2025	 
Nadhrash binti Mohamad Yusli	nadhrash_nyusli@gmail.com	Student	Update	23 Mar 2025	 
Muhamad Zeki bin Nordin	zeki.nordin2002@gmail.com	Student	Update	23 Mar 2025	 

1. Click Delete next to a user.
2. Confirm the deletion. All of the user's progress, quiz attempts, badges, and certificates will also be permanently removed.

3.10 Analytics

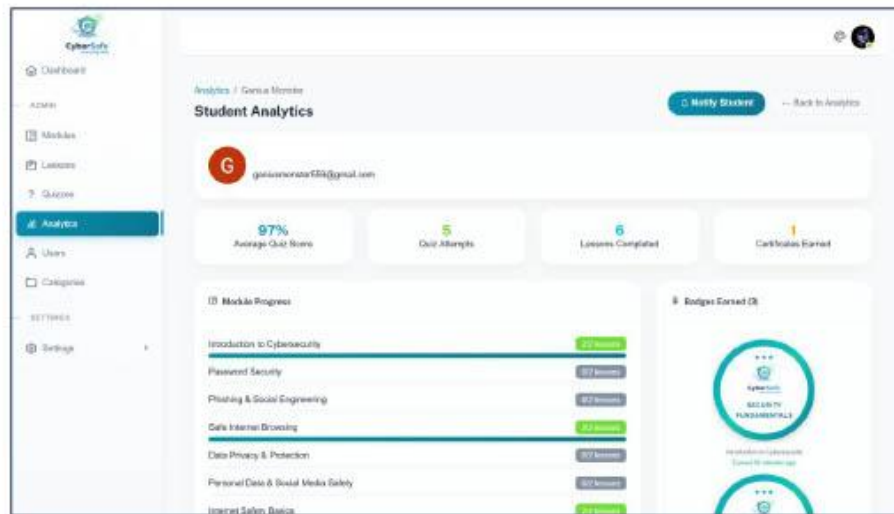
The Analytics section provides detailed reports on student and quiz performance.

- Platform Analytics Overview



1. Click **Analytics** in the sidebar.
2. The overview displays:
 - Total quiz attempts and pass rate
 - Average score across all students
 - Module completion statistics
 - Top performing students

- Individual Student Report

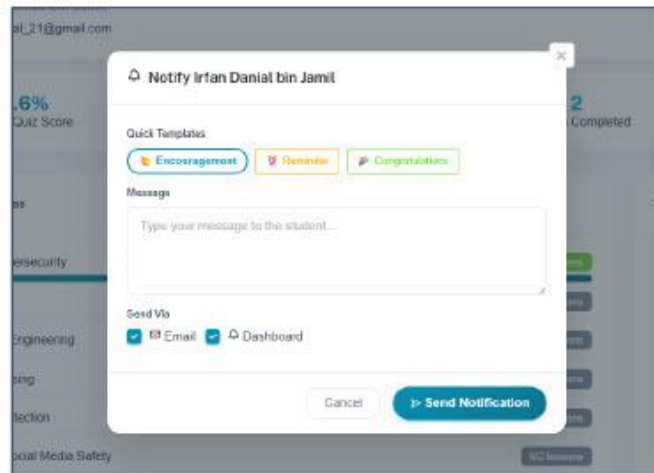


1. On the Users page, click **View** next to a student name.
2. The student's profile displays:
 - Total lessons completed
 - Total quiz attempts and average score
 - All badges earned with dates
 - All certificates earned with dates
 - Quiz-by-quiz performance breakdown

3.11 Sending Notifications to Students

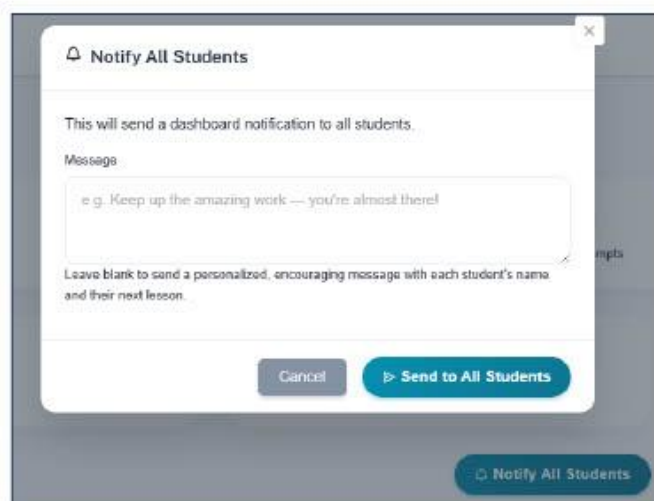
Administrators can send announcements directly to student accounts as in-platform notifications.

- Send a Notification to One Student



1. On the student's profile, click **Notify Student**.
2. Enter a **message**.
3. Click **Send**. The notification will appear in the student's notification bell immediately.

- Send a Notification to All Students



1. On the Analytics page, click **Notify All Students**.
2. Enter a **title** and **message**.
3. Click **Send**. All registered students will receive the notification.

4. Student Guide

4.1 Registration & Login

- Register with Email and Password

1. Go to <https://cybersafelearninghub.app/>.
2. Click Sign In → Register.
3. Fill in:
 - Full Name
 - Email Address
 - **Password** (minimum 8 characters)
 - Confirm Password
4. Click **Register**. You will be logged in and redirected to your dashboard.

- Register / Login with Google

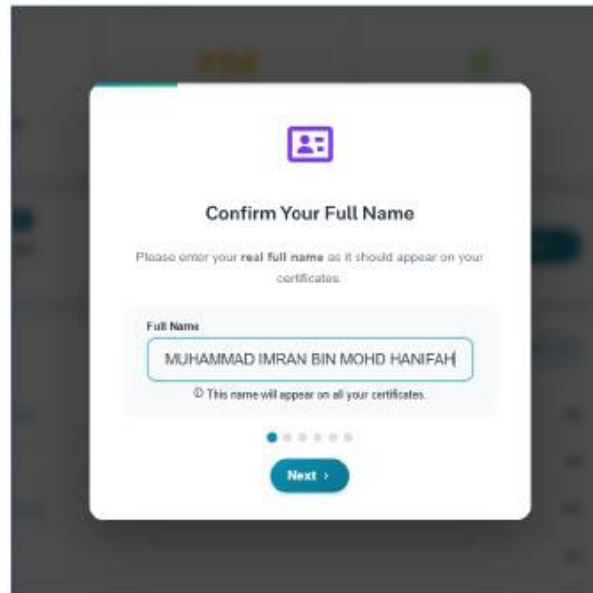
1. On the Login or Register page, click **Continue with Google**.
2. Select your Google account and grant permission.
3. You will be automatically registered (if first time) and logged in.

- Login with Email and Password

1. Click **Sign In**.
2. Enter your email address and password.
3. Click **Sign In**. You will be redirected to your Student Dashboard.

4.2 Onboarding

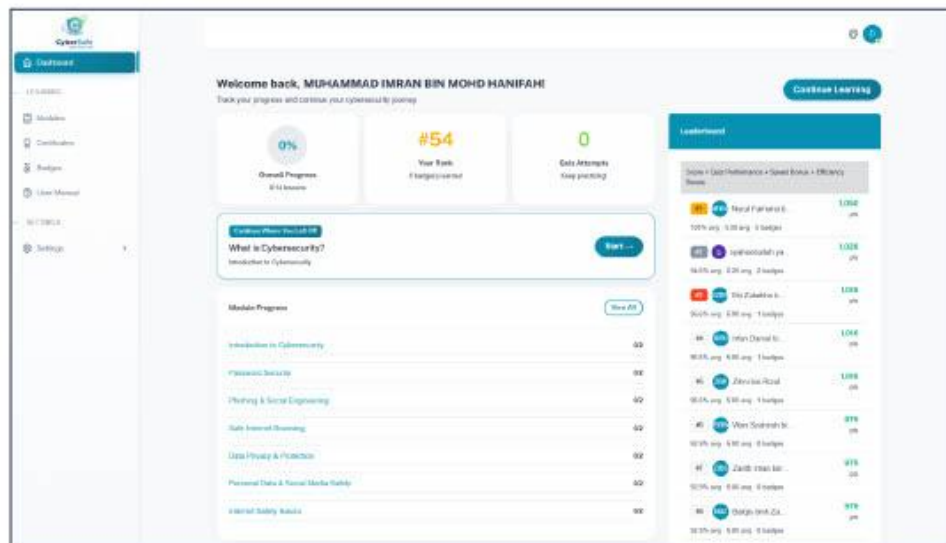
When logging in for the first time, a welcome screen will appear asking you to confirm your **full name**. This name will be printed on your certificates.



1. Review the pre-filled name in the input field.
2. Edit it if needed to match your official full name.
3. Click **Next**. Your name is saved and the dashboard will load.

Note: Onboarding only appears once. You can update your name later in Account Settings.

4.3 Student Dashboard



The dashboard provides an overview of your learning progress.

Section	Description
Progress Bar	Shows the percentage of all lessons you have completed
Continue Learning	A quick link to your next uncompleted lesson
Module Progress	Progress percentage for each module
Recent Quiz Attempts	Your last 10 quiz results with scores and pass/fail status
Badges Earned	Badges you have earned so far
Leaderboard	Top 10 students ranked by leaderboard score
Your Rank	Your current position on the leaderboard

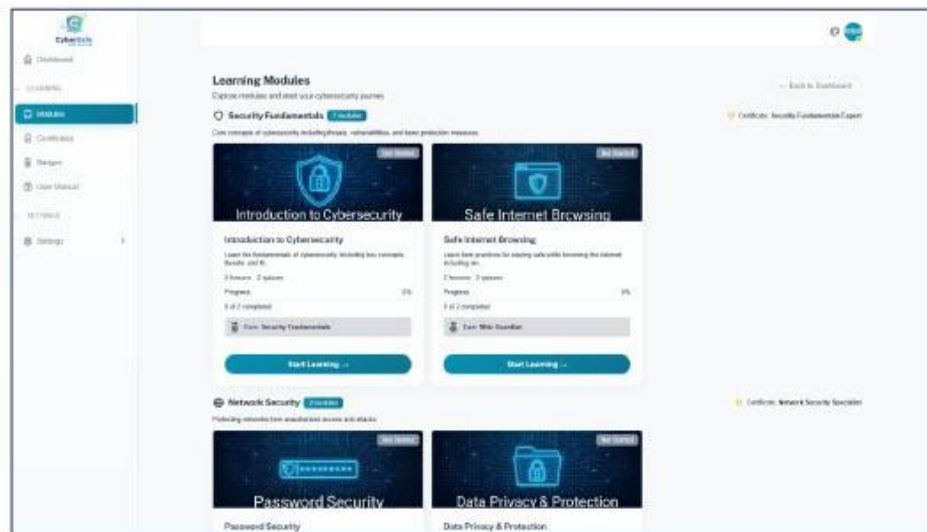
- **Leaderboard Score Formula**

Leaderboard			
Score = Quiz Performance + Speed Bonus + Efficiency Bonus			
#1	NFBG	Nurul Farhana b...	1,050 pts
100% avg - 5:00 avg - 0 badges			
#2	b	syaheedullah ya...	1,028 pts
94.6% avg - 2:26 avg - 2 badges			
#3	SZBR	Siti Zulaikha b...	1,016 pts
96.6% avg - 5:00 avg - 1 badges			
#4	IDBJ	Irfan Danial bi...	1,016 pts
96.6% avg - 5:00 avg - 1 badges			
#5	ZBR	Zihni bin Rizal	1,016 pts
96.6% avg - 5:00 avg - 1 badges			
#6	SBW	Wan Syahirah bi...	979 pts
92.9% avg - 5:00 avg - 0 badges			
#7	ZBS	Zarith Iman bin...	979 pts
92.9% avg - 5:00 avg - 0 badges			
#8	BBZ	Balqis binti Za...	979 pts
92.9% avg - 5:00 avg - 0 badges			
#9	NSB	Noor Syarifah b...	947 pts
89.7% avg - 5:00 avg - 1 badges			
#10	YBAC	Yazid bin Abdul...	926 pts
88.8% avg - 5:00 avg - 7 badges			
Your rank: #54			

Your leaderboard score is calculated based on:

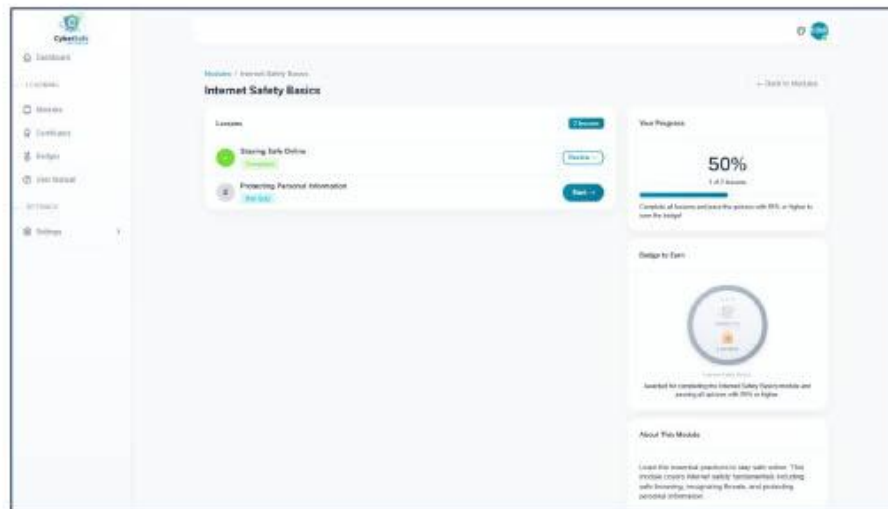
- **Average quiz score** (higher = more points)
- **Time bonus** — faster quiz completion earns bonus points
- **Efficiency bonus** — passing more quizzes on fewer attempts earns bonus points

4.4 Browsing Modules



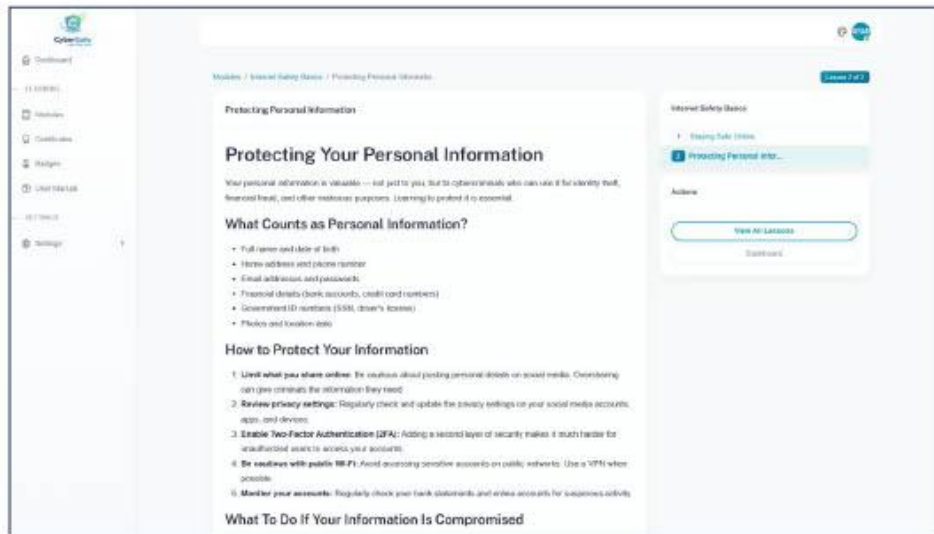
1. Click **Modules** in the navigation menu.
2. All available modules are displayed, grouped by category.
3. Each module card shows:
 - Module title and description
 - Number of lessons
 - Your completion progress
 - The badge you can earn
4. Click on a module to view its lessons.

- **Module Detail Page**



- All lessons within the module are listed in order.
- A  tick appears at the lessons you have completed.
- Click any lesson name to open it.

4.5 Viewing a Lesson



1. Click on a lesson from the module page or from the **Continue Learning** shortcut on the dashboard.
2. The lesson page displays the full content, which may include:
 - Text explanations
 - Images and infographics
 - Embedded videos
3. Use the **Previous** and **Next** buttons at the bottom to navigate between lessons in the same module.
4. Your current position in the module is shown.

- Discussion Comments



Discussion (0)

Share your thoughts or ask a question...

Post Comment

No comments yet. Be the first to share your thoughts!

- Below the lesson content, there is a **Discussion** section where you can leave a comment or question.
- To post a comment, type your message and click **Post**.
- To delete your own comment, click the **Delete** button next to it.

4.6 Completing a Lesson



← Previous Lesson

Mark as Complete

Back to Module

1. After reading through the lesson content, click the **Mark as Complete** button.
2. Your progress is saved. The lesson will be marked as  in the module overview.
3. If there is a quiz under the lessons you can answer it and if you passed you will earn the module badge.

4.7 Taking a Quiz

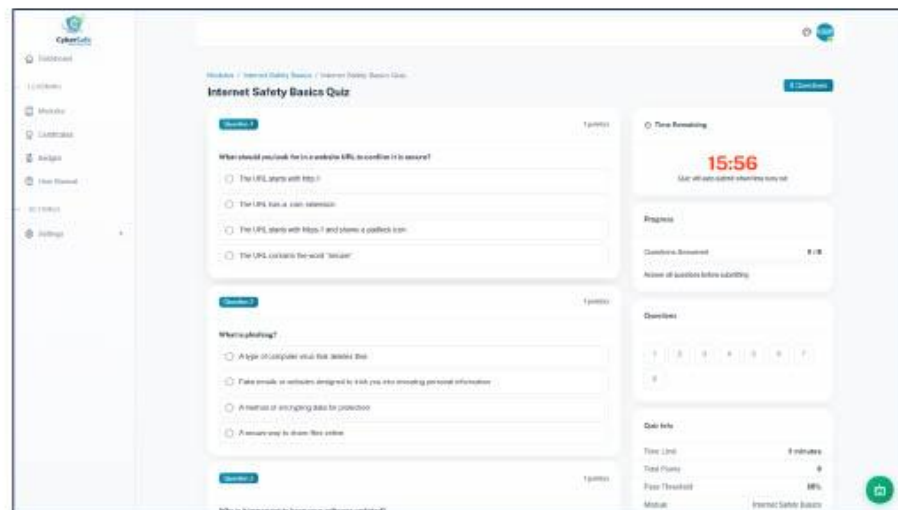
Each lesson has one associated quiz that must be passed with a score of **85% or above**.

- Starting a Quiz



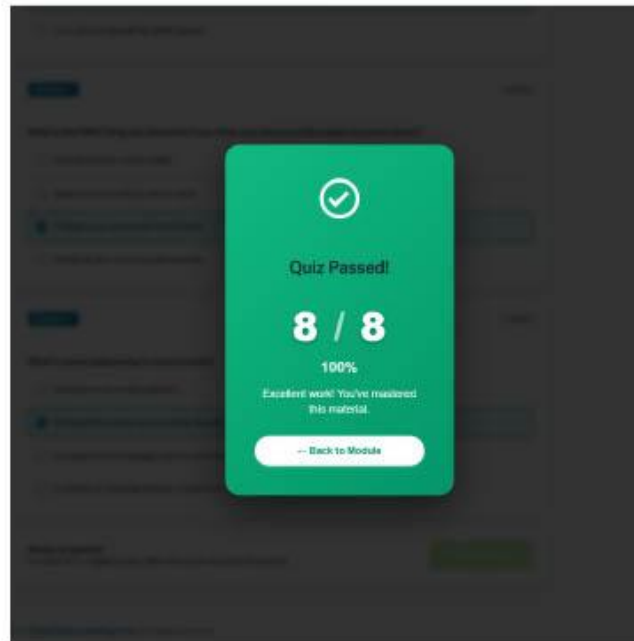
- At the lesson content page, click **Take Quiz**.
- You will be taken to the quiz page.

- Quiz Interface



- All questions are displayed with **multiple-choice answer options** (select one answer per question).

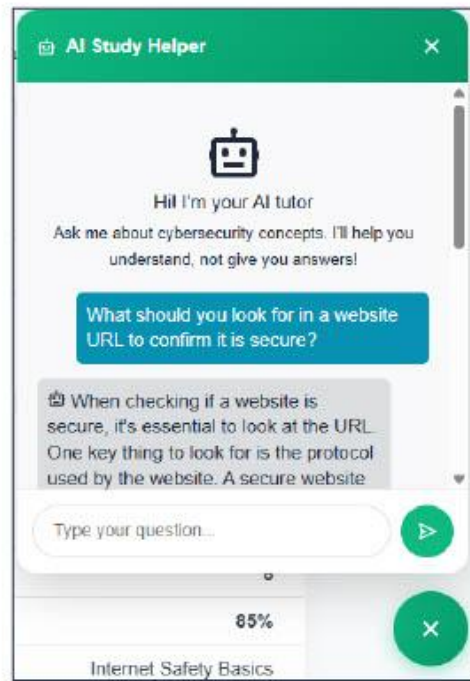
- A **countdown timer** tracks the time you spend on the quiz.
 - A **question navigator** on the side shows which questions you have and have not answered.
 - A **progress bar** shows how many questions you have answered.
- Submitting a Quiz



1. Answer all questions. You must answer every question before submitting.
 2. Click Submit Quiz.
 3. A result popup will appear showing your score and whether you passed or failed.
- Retaking a Quiz
 - If you score below 85%, you may retake the quiz.
 - If you have already passed a quiz, retaking is not allowed.

4.8 AI Chatbot

The AI Chatbot is available during a quiz to help you understand concepts without giving away direct answers.



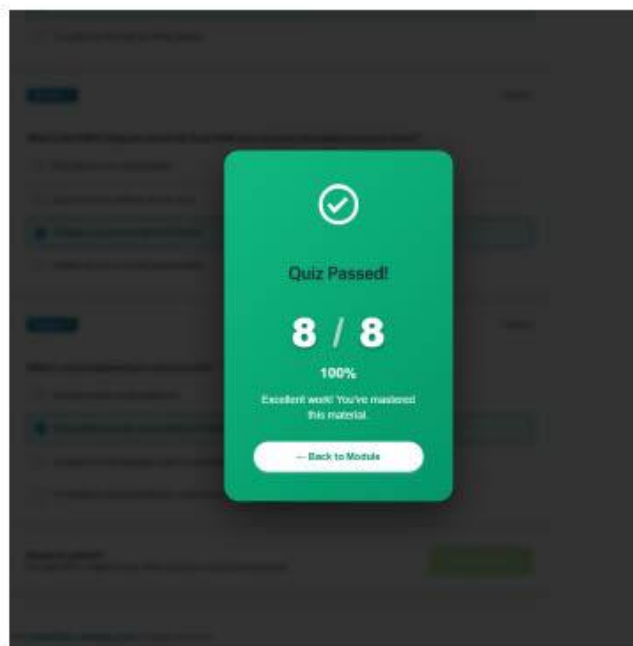
1. While on the quiz page, click the **chatbot icon** (usually located at the bottom corner of the screen).
2. Type your question.
3. The chatbot will provide an explanation based on cybersecurity knowledge.

Note: The chatbot is designed to explain concepts only. It will not tell you which answer to select for a quiz question.

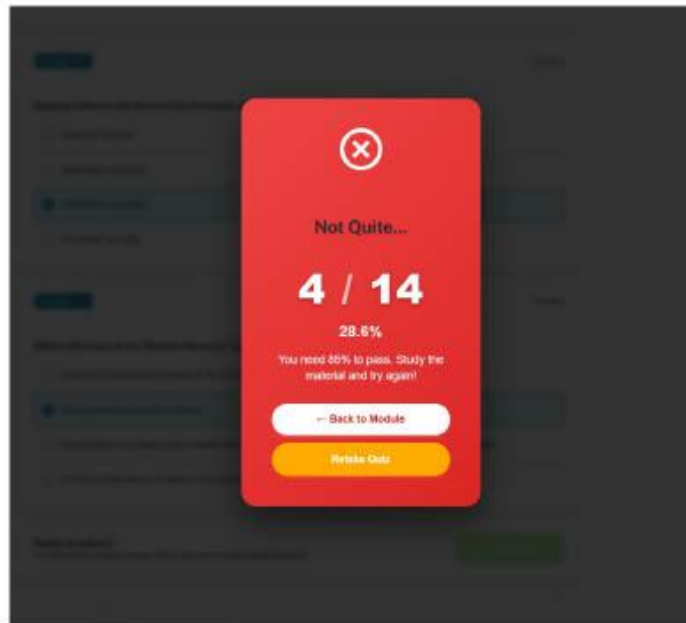
4.9 Viewing Quiz Results

After submitting a quiz, the result page shows:

Field	Description
Score	Number of correct answers out of total questions
Percentage	Your score as a percentage
Pass / Fail	Whether you reached the 85% passing threshold



- If you **passed**: a success animation is shown. You can return to the module or continue to the next lesson.



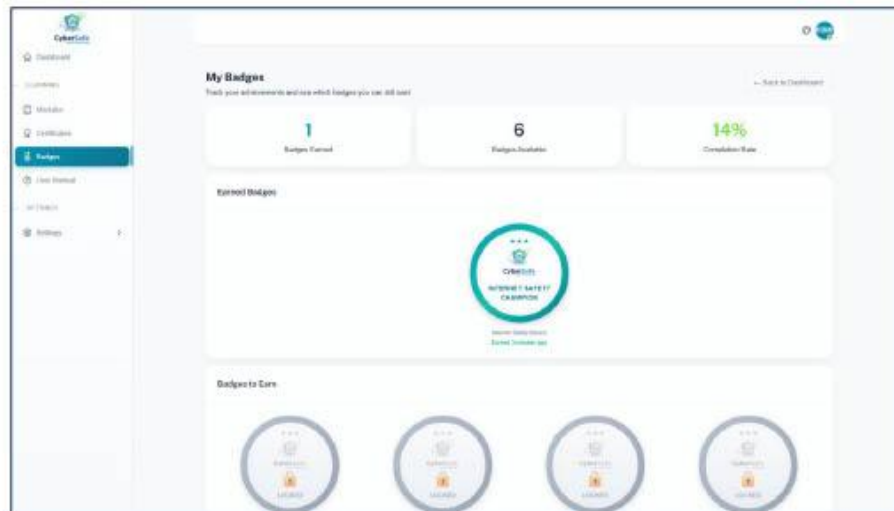
- If you failed: a retry option is shown. Click **Retake Quiz** to try again.

You can also view your quiz result history from the **Dashboard** under *Recent Quiz Attempts*.

4.10 Badges

Badges are awarded automatically when you pass all quizzes in a module with a score of 85% or above.

- View Your Badges



1. Click **Badges** in the navigation menu.
2. All earned badges are displayed with the module name and date earned.

How badges are awarded: After each quiz submission, the system checks whether you have passed all quizzes in the module. If all quizzes are passed at 85%+, the badge is automatically awarded and a notification is sent.

4.11 Certificates

Certificates are awarded when you complete **all modules** within a category.

- View Your Certificates



1. Click **Certificates** in the navigation menu.
2. All earned certificates are listed with the category name, certificate number, and date issued.

- View or Download a Certificate



1. Click **View Certificate** next to the certificate.
2. Your certificate is displayed with your full name, the category, and the date issued.
3. Click **Download PDF** to save a copy of your certificate.

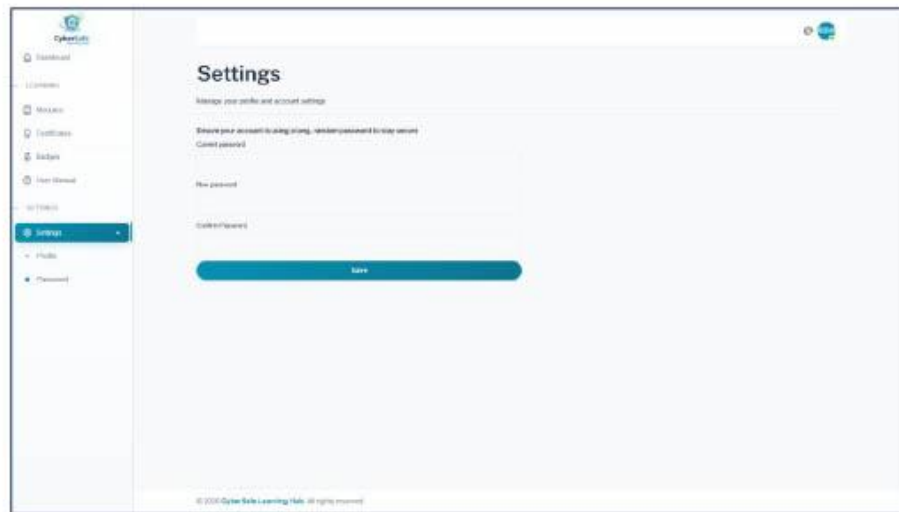
4.13 Account Settings

- Update Your Profile



1. Click your **profile name or avatar** in the top navigation bar.
2. Select Settings → Profile.
3. Update your **name or email address**.
4. Click **Save**.

- Change Your Password



1. Go to Settings → Password.
2. Enter your current password.
3. Enter and confirm your **new password**.
4. Click Update Password.

Note: If you registered using Google Sign-In, the password change option may not be available. Manage your password through your Google account instead.

5. System Requirements

Requirement	Recommended
Browser	Google Chrome 110+, Firefox 110+, Microsoft Edge 110+
Internet Connection	Required (stable broadband recommended)
Screen Resolution	1280 × 720 or higher (mobile-responsive)
PDF Viewer	Required for viewing/downloading certificates

Appendix C – Turnitin Result

i. Turnitin Result FYP1 (Chapter 1-3)


Page 1 of 67 - Cover Page
Submission ID trnoid::1:3412295277

FYP Report Chapter 1-3.pdf

Document



Document Details

Submission ID	trnoid::1:3412295277	62 Pages
Submission Date	Nov 15, 2025, 7:21 PM GMT-5	12,733 Words
Download Date	Nov 15, 2025, 7:22 PM GMT-5	73,992 Characters
File Name	tmpxtt1l_ka.pdf	
File Size	2.6 MB	


Page 1 of 67 - Cover Page
Submission ID trnoid::1:3412295277



Page 2 of 67 - Integrity Overview

Submission ID: tmcoid:1:3412295277

2% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

-  **24 Not Cited or Quoted 2%**
Matches with neither in-text citation nor quotation marks
-  **3 Missing Quotations 0%**
Matches that are still very similar to source material
-  **1 Missing Citation 0%**
Matches that have quotation marks, but no in-text citation
-  **0 Cited and Quoted 0%**
Matches with in-text citation present, but no quotation marks

Top Sources

-  **2% Internet sources**
-  **1% Publications**
-  **1% Submitted works (Student Papers)**

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.



Page 2 of 67 - Integrity Overview

Submission ID: tmcoid:1:3412295277



*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify writing that is likely AI generated as AI generated and AI paraphrased or likely AI generated and AI paraphrased writing as only AI generated) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.



ii. Turnitin Result FYP2 (Chapter 4-6)


Page 1 of 128 - Cover Page
Submission ID trnoid::1:3528586863

A B

CHAPTER 4, 5, 6 IMRAN

 dr. faheem
 Quick Submit
 Institute of Space Technology

Document Details

Submission ID	trnoid::1:3528586863	126 Pages
Submission Date	Apr 6, 2026, 2:41 PM GMT+5	22,115 Words
Download Date	Apr 6, 2026, 2:53 PM GMT+5	119,312 Characters
File Name	CHAPTER_4,_5,_6_IMRAN.pdf	
File Size	9.7 MB	


Page 1 of 128 - Cover Page
Submission ID trnoid::1:3528586863

CHAPTER 4, 5, 6 IMRAN

ORIGINALITY REPORT

6%	2%	1%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to LKCFES Student Paper	1%
2	Submitted to University of Huddersfield Student Paper	1%
3	Submitted to Asia Pacific University College of Technology and Innovation (UCTI) Student Paper	<1%
4	Submitted to University of Wales Institute, Cardiff Student Paper	<1%
5	Submitted to Universiti Poly-Tech Malaysia Student Paper	<1%
6	Submitted to TMC Academy Pte Ltd Student Paper	<1%
7	www.coursehero.com Internet Source	<1%
8	purehost.bath.ac.uk Internet Source	<1%
9	Submitted to HELP UNIVERSITY Student Paper	<1%
10	Submitted to universititeknologimara Student Paper	<1%
11	www.calbar.ca.gov Internet Source	<1%



*% detected as AI

AI detection includes the possibility of false positives. Although some text in this submission is likely AI generated, scores below the 20% threshold are not surfaced because they have a higher likelihood of false positives.

Caution: Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (i.e., our AI models may produce either false positive results or false negative results), so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

Frequently Asked Questions

How should I interpret Turnitin's AI writing percentage and false positives?

The percentage shown in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was either likely AI-generated text from a large-language model or likely AI-generated text that was likely revised using an AI paraphrase tool or word spinner.

False positives (incorrectly flagging human-written text as AI-generated) are a possibility in AI models.

AI detection scores under 20%, which we do not surface in new reports, have a higher likelihood of false positives. To reduce the likelihood of misinterpretation, no score or highlights are attributed and are indicated with an asterisk in the report (*%).

The AI writing percentage should not be the sole basis to determine whether misconduct has occurred. The reviewer/instructor should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in accordance with their school's policies.

What does 'qualifying text' mean?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be likely AI-generated will be highlighted in cyan in the submission, and likely AI-generated and then likely AI-paraphrased will be highlighted purple.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.



Appendix D – Log Book

i. Log Book FYP1 (FYP4112)

CT206/ BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY (CT206)



FACULTY OF COMPUTING & MULTIMEDIA (FCOM)

FINAL YEAR PROJECT O1
FYP4112

LOG BOOK

STUDENT'S NAME :	MUHAMMAD IMRAN BIN MOHD HANIFAH
ID NO. :	AM0408016649
SUPERVISOR :	NORALIZA BINTI AZIZAN
PROJECT TITLE :	Cyber Safe Learning Hub

Scanned with
CS CamScanner

CT206/ BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY (CT206)

Week	Agenda	Next Agenda	Signature (Supervisor / Coordinator)
7/8/2025	1 Brainstorming Idea	Present Idea	JHG
14/8/2025	2 Present Idea	Title Approval	JHG
21/8/2025	3 Title Approval	Proposal Submission	JHG
28/8/2025	4 Proposal Submission	Chapter 1 Consultation	JHG
4/9/2025	5 Chapter 1 consultation	Discussion about client	JHG
MID-TERM BREAK			
11/9/2025	6 Discussion About Client	Chapter 2 consultation	JHG
22/9/2025	7 Chapter 2 consultation	Discussion about questionnaire questions	JHG
2/10/2025	8 Discussion about questionnaire questions	Chapter 3 consultation	JHG
7/10/2025	9 Chapter 3 consultation	Use Case & Flowchart Consult	JHG
15/10/2025	10 Use case & Flowchart Consult	Chapter 3 Analysis Consult	JHG
22/10/25	11 Chapter 3 Analysis Consult	Chapter 3 Consultation	JHG
29/10/25	12 Chapter 3 Consultation	Presentation Slide Consultation	JHG
5/11/25	13 Presentation Slide Consultation	Presentation and Report Submission	JHG

CT206/ BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY (CT206)

11/11/ 2025	14	Presentation and Report Submission		
----------------	----	---------------------------------------	--	--

Scanned with
CamScanner

ii. Log Book FYP2 (FYP4124)

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY



FACULTY OF COMPUTING & MULTIMEDIA (FCOM)

FINAL YEAR PROJECT 2

FYP4124

LOG BOOK

STUDENT'S NAME : Muhammad Imran Bin Mohd Haniffah
 ID NO. : AM2408616649
 SUPERVISOR : Noraliza Binti Azizan
 PROJECT TITLE : CyberSafe Learning Hub

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

Week		Agenda	Next Agenda	Signature (Supervisor / Coordinator)
24/1/26	1	FYP I Review	Chapter 4 Design Consultation	H.S.
31/1/26	2	Chapter 4 Design Consultation	Chapter 4 Design Consultation	H.S.
7/1/26	3	Chapter 4 Design Consultation	Chapter 4 Design Consultation	H.S.
14/1/26	4	Chapter 4 Design Consultation	Implementation Progress Consultation	H.S.
21/1/26	5	Implementation Progress Consultation	Implementation Progress Consultation	H.S.
~~MID-TERM BREAK~~				
27/1/26	6	Implementation Progress Consultation	Implementation Progress Consultation	H.S.
4/2/26	7	Implementation Progress Consultation	Implementation Progress Consultation	H.S.
11/2/26	8	Implementation progress consultation	Implementation Progress Consultation	H.S.
18/2/26	9	Implementation progress consultation	Report Progress Consultation	H.S.
25/2/26	10	Report progress consultation	Report Progress Consultation	H.S.
4/3/26	11	Report progress consultation	UAT Consultation	H.S.
11/3/26	12	UAT consultation	Slide & Poster Consultation	H.S.
16/3/26	13	Repa Slide & Poster Consultation	Final presentation	H.S.

CT206 / BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN CYBER SECURITY

1/4/26	14	Final Presentation	Final Report Submission	H/a
--------	----	-----------------------	----------------------------	-----

References

- Abdul Razack, A. K., & Mat Saad, M. F. (2024). Enhancing Cybersecurity Awareness through Gamification: Design an Interactive Cybersecurity Learning Platform for Multimedia University Students. *Journal of Informatics and Web Engineering*, 3(3), 21–40. <https://doi.org/10.33093/jiwe.2024.3.3.2>
- Ambikapathy, M., Abdul Hamid, M. K., & Mohd Sukor, M. A. A. (2024). Impact of Gamification on Student Motivation and Engagement. *Environment-Behaviour Proceedings Journal*, 9(SI21), 11–20. <https://doi.org/10.21834/e-bpj.v9isi21.6076>
- Anderson Kevin Gwenthure, & Flourensia Spty Rahayu. (2024). Gamification of Cybersecurity Awareness for Non-IT Professionals: A Systematic Literature Review. *International Journal of Serious Games*, 11(1), 83–99. <https://doi.org/10.17083/ijsg.v11i1.719>
- Awati, R. (2023, June). *What is Requirements Analysis? - Definition from WhatIs.com*. SearchSoftwareQuality. <https://www.techtarget.com/searchsoftwarequality/definition/requirements-analysis>
- Bhandari, P. (2021, July 15). *Questionnaire Design | Methods, Question Types & Examples*. Scribbr. <https://www.scribbr.com/methodology/questionnaire/>
- Dhanya Pramod. (2024). Gamification in cybersecurity education; a state of the art review and research agenda. *Journal of Applied Research in Higher Education*. <https://doi.org/10.1108/jarhe-02-2024-0072>
- Gabra, A. A., Sirat, M. B., Hajar, S., & Dauda, I. B. (2020). *Cyber security awareness among university students: A case study*. *Journal of Critical Reviews*, 7(12), 1086–1093. Retrieved from https://www.researchgate.net/publication/378308636_JOURNAL_OF_CRITICAL_REVIEWS_CYBER_SECURITY_AWARENESS_AMONG_UNIVERSITY_STUDENTS_A_CASE_STUDY
- Huitema, D., & Wong, A. (2025). *A Case Study in Gamification for a Cybersecurity Education Program: A Game for Cryptography*. ArXiv.org. <https://arxiv.org/abs/2502.06706>
- Jian, N. J., & Kamsin, I. F. B. (2021). Cybersecurity Awareness Among the Youngs in Malaysia by Gamification. *Atlantis Highlights in Computer Sciences*. <https://doi.org/10.2991/ahis.k.210913.061>
- Jr Maluda, A. A., Kasmin, I. F., Zainal Abidin, Z. M., & Vasudavan, H. (2023). Evaluating the Effectiveness of Gamification to Increase Cybersecurity Awareness among Students. *International Journal of Data Science and Advanced Analytics*, 4, 154–158. <https://doi.org/10.69511/ijdsaa.v4i0.157>

- Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, 27. <https://doi.org/10.1007/s10639-021-10807-6>
- Popa, O., Fagarasan, C., Pislă, A., & Cristea, C. (2021). Agile, waterfall and iterative approach in information technology projects. *IOP Conference Series: Materials Science and Engineering*, 1169(1). IOP. <https://doi.org/10.1088/1757-899x/1169/1/012025>
- Saunders, M., Lewis, P., & Thornhill, A. (2023, March 20). *Saunders, Research Methods for Business Students, 9ed.* Www.pearson.com. https://www.pearson.com/nl/en_NL/higher-education/subject-catalogue/business-and-management/saunders-research-methods-for-business-students-9ed.html
- Wu, T., Tien, K.-Y., Hsu, W.-C., & Wen, F.-H. (2021). Assessing the Effects of Gamification on Enhancing Information Security Awareness Knowledge. *Applied Sciences*, 11(19), 9266. <https://doi.org/10.3390/app11199266>