CyberSecureHub: An Educational Platform for Cybersecurity Learning

Germán Rodríguez Franceschini
Advisor: Alfredo Cruz, Ph.D.
Master in Computer Science
Graduate Project EXPO, May 2026

Abstract

This project developed CyberSecureHub, a web-based educational platform designed to centralize key areas of cybersecurity into a single interactive learning environment. Cybersecurity education is fragmented across separate websites, technical blogs, certification pages, and practice platforms. Entry-level professionals must move between resources to learn penetration testing, security operations, and career pathways, which slows learning and disconnects theory from practice.
The platform was implemented using Python and the Flet framework in web mode, allowing it to run in a standard browser without dedicated installation. It integrates Red Team content, Blue Team content, certification guidance, three tiers of Capture the Flag (CTF) challenges, and an AI chatbot for real-time support. The system was implemented and tested end-to-end. Results confirm that modular architecture can present offensive and defensive concepts together and that a contextual AI chatbot can support learning without replacing it.

Introduction

Cybersecurity has become one of the most critical areas of modern technology. Organizations rely on digital systems, online services, cloud platforms, and interconnected networks for daily operations. Companies must defend critical information, sustain service continuity, and respond to incidents. This demand has produced a need for educational tools that present offensive and defensive security in an organized way.
Learners are often introduced to offensive concepts such as reconnaissance, scanning, exploitation, and privilege escalation independently of defensive concepts such as monitoring, incident response, digital forensics, and vulnerability management. Certification information is also separated from technical material, and practical exercises are introduced on different platforms with little connection to learning content. Even simple concepts can require students to navigate several resources before they take shape.
Another challenge is the lack of immediate support when users encounter unfamiliar concepts or technical terms. Learners may understand the general idea of a topic but still struggle to connect it to real-world practice or to other areas of cybersecurity. Many learners spend more time searching for information than learning.
To address these problems, CyberSecureHub was developed as a centralized web-based educational platform combining Red Team content, Blue Team content, certification guidance, CTF exercises, and an AI chatbot for real-time support within a single interactive environment.

Background

Roshanaei & Jachura (2025) AI chatbots are becoming more popular as learning tools to offer real-time support. Chatbots can explain complex concepts and provide answers to technical questions. Generative AI can also help learners develop critical thinking when used as a guided support tool. Students still need structure and oversight because they may become over-reliant on AI-generated answers or accept responses without sufficient evaluation.
Wang, Tian, Gu, & Lu (2019) Hands-on experiments are important in cybersecurity education because they help learners develop operational skills and practice realistic attack and defense scenarios. CTF challenges support active learning by connecting cybersecurity concepts to practical tasks. A CTF becomes more useful as an educational tool when it includes guidance, background explanation, and structured learning activities rather than functioning purely as a competition.
Abhari, Safaei Pour, & Shirazi (2024) Training can become less effective when it is too generic, repetitive, or disconnected from actual roles and workflows. Cybersecurity readiness programs must be structured around real professional competencies and aligned with real world tools and environments that practitioners encounter in the field.
Švábenský, Čeleda, Vykopal, & Brišáková (2021) CTF challenges are popular in cybersecurity education to support learning by doing. These challenges enable learners to apply theoretical knowledge in real life situations to strengthen problem solving skills and span a wide range of knowledge areas including cryptography, web security, forensics, and reverse engineering.
Elkhodr & Gide (2025) Integrating generative AI in cybersecurity education requires careful pedagogical design. AI tools can support critical thinking and concept explanation when used responsibly, but instructors must ensure students evaluate AI responses critically rather than accepting them without question.

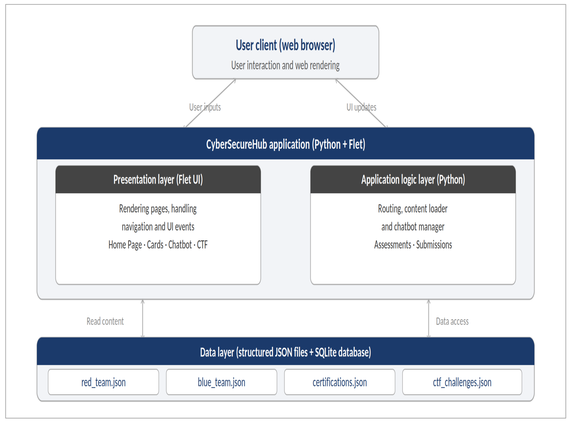
Problem

Cybersecurity is an extensive and complex industry and there is a lack of centralized, accessible content for students and early-career professionals. Penetration testing and security operations content is typically found on separate websites, technical blogs, and textbooks. An offensive security student may be exposed to tools or techniques without understanding how defensive teams monitor or respond to the same activities.
This project addresses the need for a centralized learning platform that includes structured content, hands-on exercises, and contextual real-time instructional support all within a single browser accessible environment that requires no installation.

Methodology

System Architecture:
CyberSecureHub was implemented using Python and the Flet framework in web mode, allowing the application to run in a standard browser without dedicated installation. The system architecture is organized into three layers to support organization, and maintainability.
(1) Presentation Layer renders all user facing views including the Home Page, navigation controls, topic cards, dialog windows, chatbot interface, assessment views, and CTF challenge screens. (2) Application Logic Layer coordinates routing, content delivery, challenge submissions, assessments, and chatbot interactions. (3) Data Layer static educational content is stored in structured JSON files; user accounts, assessment attempts, and CTF progress are persisted in a SQLite database.

Figure 1: High Level Architecture



Platform Modules:
Red Team Module (7 topics): Reconnaissance, Scanning & Enumeration, Web Application Vulnerabilities, Authentication & Access Control, Exploitation, Privilege Escalation, and Reporting. Each topic card presents a structured description, learning objectives, and an external video resource. The module presents penetration testing as a professional workflow emphasizing the purpose and expected deliverables of each phase rather than step by step tool usage.
Blue Team Module (6 topics): SOC Operations, Threat Intelligence, Incident Response, Digital Forensics, Vulnerability Management, and Identity & Access Management. Content is framed in terms of analyst decision making and workflow, aligned with the tiered SOC model and Canadian Centre for Cyber Security guidance.
Certifications Module (10 certifications): Organized into three career paths Penetration Tester (eJPT, CEH, OSCP), SOC Analyst (Security+, CySA+, BTL1, GCIA), and Governance, Risk & Compliance (CISA, CISM, CISSP). Role-based grouping allows learners to move from technical content to aligned credentials without external searching.

Figure 2: Navigation Flowchart

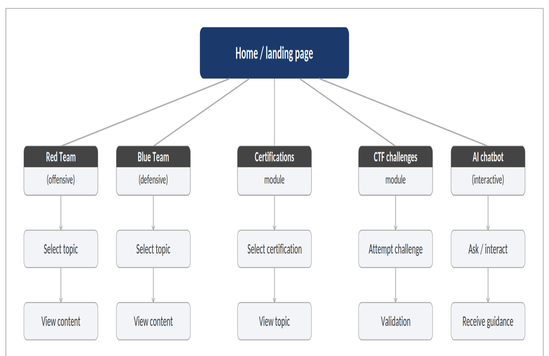
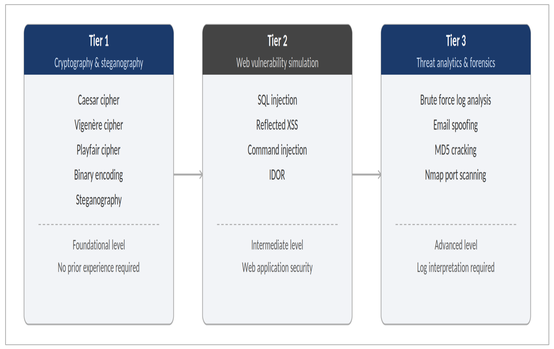


Figure 3: CTF Challenges

CTF Module with 31 Challenges Across 3 Tiers:
The CTF module is a guided learning environment. Each challenge targets a specific concept with a description, task, flag validation step, and hints on request.



Tier 1: Cryptography & Steganography: Caesar Cipher (monoalphabetic shift, C=(P+K) mod 26, brute force and frequency analysis attacks), Vigenère Cipher (polyalphabetic substitution, Tabula Recta, Kasiski examination, Index of Coincidence), Playfair Cipher (digraphic substitution, 5×5 key square, three positional rules), Binary Encoding, and Steganography/Metadata Analysis.
Tier 2: Web Vulnerability Simulation: SQL Injection (unparameterized queries, OWASP Top 10, authentication bypass), Reflected XSS (unvalidated input in HTML response, session cookie theft), Command Injection, and Insecure Direct Object Reference (IDOR).
Tier 3: Threat Analytics & Forensics: Brute Force Log Analysis (authentication log interpretation, failed-login pattern recognition), Email Spoofing (SMTP header analysis, phishing indicators, SPF/DKIM/DMARC), MD5 Cracking, and Nmap Port Scanning analysis.
AI Chatbot Integration:
A chatbot was developed using an external large language model API (Groq platform) and embedded across all primary modules. Workflow: (1) user submits a query via the Flet interface; (2) application logic formats the request with current module context; (3) secure HTTP POST sent to external LLM; (4) LLM generates contextual response; (5) response parsed and displayed inline without redirecting the user.
The chatbot was designed as a teaching assistant — clarifying concepts, terminology, and workflows without providing exploitation steps or direct CTF answers. In the CTF section specifically, it explains underlying concepts (encoding, hashing, log structure) without revealing flags or bypassing the learning process.

Results and Discussion

All modules were implemented and operated as intended. The results address all four research questions posed in the study.
Home Page & Navigation:
All five sections are reachable from the Home Page in a single click. During testing, new users were able to identify and navigate to any section without guidance, confirming that the layout achieves its goal of reducing onboarding friction. The card-based layout and dialog-based detail view worked as intended users opened and closed topic cards without leaving their current module.
Red Team Module:
Seven topics loaded correctly from the JSON data file and rendered without errors. The module presents penetration testing as a professional workflow each topic emphasizes the purpose, scope, and expected deliverables of a phase. External video links included in each topic card functioned as intended, opening in the browser without disrupting the current module view.
Blue Team Module:
Six topics loaded correctly. The module bridges the gap between the abstract concept of a SOC and the practical daily work analysts perform. Rather than presenting defensive security as a list of tools, each function is framed in terms of analyst decision making and workflow, which aligns with how the topic is treated in professional environments.
Certifications Module:
Ten certifications loaded and organized by career path. Role based grouping proved effective: a learner who has been reading the Red Team module can move to this section and immediately see which credentials align with an offensive security career path without needing to search externally. This confirms the module reduces student research time for career path exploration.
CTF Module:
All 31 challenges loaded correctly from ctf_challenges.json, flag validation worked as expected for each challenge, and hints displayed on request without revealing the answer. The tier structure performed as intended: Tier 1 was approachable for users with no prior CTF experience, while Tier 3 required analytical thinking and familiarity with log interpretation and protocol behavior.

Cont. of Results and Discussion

AI Chatbot:
The chatbot remained accessible throughout all sections and maintained appropriate boundaries. It produced contextually relevant responses across Red Team, Blue Team, Certifications, and CTF topics. In the CTF section, it explained concepts without revealing flags, confirming that the integration achieved its goal of functioning as a learning support layer rather than a shortcut. This differentiated behavior confirmed that the chatbot integration functioned as a guided support layer across all contexts.
Research Questions:
RQ1: Can a single platform present offensive and defensive concepts without confusion? Yes. The modular structure keeps Red Team and Blue Team content distinct while shared navigation makes clear that both belong to the same field.
RQ2: Can a web application reduce student research time for career paths? Yes. The Certifications module places credential guidance in the same environment as the technical content it relates to, eliminating the need for external searching.
RQ3: What framework balances maintenance with performance? Python and Flet produced a browser-accessible system requiring no installation, remaining easy to maintain throughout development by a single developer.
RQ4: Can an AI chatbot maintain appropriate scope boundaries? Yes. The chatbot maintained appropriate boundaries across all module contexts.

Conclusions

CyberSecureHub achieved its main goal of bringing cybersecurity education together in one accessible website. The platform combines organized learning content, practical exercises, certification guidance, and AI support in a connected way. All five modules were completed and worked as expected. The AI chatbot provided helpful answers in each area. The CTF module gave users a step-by-step path from basic cryptography to more advanced topics such as threat analysis and digital forensics.
The project shows that offensive security, defensive security, and career guidance can be taught in the same platform. Students and beginners can learn important concepts, complete hands-on activities, and explore certifications without using different systems.

Future Work

Formal User Studies: Conduct structured pre/post assessments to validate educational effectiveness and measure actual learning outcomes against a baseline.
Expanded CTF Content: Add challenges in reverse engineering, cloud security misconfigurations, binary exploitation, and advanced network forensics.
Collaborative Features: Add team-based CTF competition modes and an instructor dashboard for monitoring and tracking student progress.

References

Abhari, K., Safaei Pour, M., & Shirazi, H. (2024). How to design a better cybersecurity readiness program. MIS Quarterly Executive, 23(4). https://doi.org/10.17705/2msqe.00107

Wang, L., Tian, Z., Gu, Z., & Lu, H. (2019). Crowdsourcing approach for developing hands-on experiments in cybersecurity education. IEEE Access, 7, 169066–169071. https://doi.org/10.1109/ACCESS.2019.2952585

Roshanaei, M., & Jachura, M. G. (2025). Integrating AI in cybersecurity higher education: A path to workforce readiness. Journal of Intelligent Learning Systems and Applications, 17(2), 45–67. https://doi.org/10.4236/jilsa.2025.172005

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. Computers & Security, 102, 102154. https://doi.org/10.1016/j.cose.2020.102154

Elkhodr, M., & Gide, E. (2025). Integrating generative AI in cybersecurity education. arXiv. https://arxiv.org/abs/2502.15357

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST SP 800-61 Rev. 2). NIST. https://doi.org/10.6028/NIST.SP.800-61r2

Canadian Centre for Cyber Security. (2023). Best practices for setting up a security operations centre (ITSAP.00.500). Government of Canada.

OWASP. (2020). Web Security Testing Guide (WSTG) v4.2. https://owasp.org/www-project-web-security-testing-guide/v42/

Mansurov, A. (2016). A CTF-based approach in information security education. Modern Applied Science, 10(11), 159–166. https://doi.org/10.5539/mas.v10n11p159

Flet. (2025). Introduction. https://flet.dev/docs/.