# CyberMaze: A Virtual Cyber Security Learning and Assessment Platform

Ukasha Awan, Sami Ullah, Haroon Atieeque, Muhammad Ali Qureshi, Iram Haider
Dept. of Information & Communication Engineering, The Islamia University of Bahawalpur, Pakistan
Email: {tamshoonawan@gmail.com, samikharzi786@gmail.com, haroonatieeq6@gmail.com,
ali.qureshi@iub.edu.pk, iramhaider456@gmail.com}

***Abstract*—Modern cybersecurity is a rapidly developing field that requires a strong correlation between theoretical concepts and practical application. However, a significant disparity still exists between the two, which can be further widened by human factors - one of the primary causes of cyber threats. This paper proposes that CyberMaze bridge this gap and allow users to gain hands-on experience in key cybersecurity areas. CyberMaze offers an immersive learning environment encompassing four core domains: Network Security, Cryptography, Capture the Flag (CTF), and Cloud Security. Each domain consists of multiple levels designed to improve user skills and challenge them step by step progressively. In the Network Security module, a virtual Kali Linux system is deployed on AWS, allowing users to practice tools like Nmap. The cryptography domain assesses the proficiency of users in user techniques. The CTF module engages users through interactive exercises, helping them to use tools effectively to capture flags. Similarly, the cloud security domain evaluates the knowledge of users about the services of users, including CloudFormation, CloudWatch, Lambda Functions, EC2 instances, and S3 buckets. AWS virtual machines provide pre-configured environments, such as Kali Linux machines. The frontend is developed using HTML, CSS, and JavaScript, while Django is used as the backend framework. Django's integrated Django handles user data, including scores and progress tracking. Users who tested CyberMaze have gained key cybersecurity skills through interactive challenges, establishing a solid foundation for tackling real-world scenarios. Future work will focus on increasing challenge difficulty and expanding domains to improve the CyberMaze learning experience.**

***Index Terms*—AWS, Network Security, Cryptography, Capture the Flag, Cloud Security, Virtual Machine, Kali Linux, and Cyber Security Assessment.**

## I. Introduction

According to a study by IBM, 95% of cybersecurity breaches occur due to human error. This alarming statistic highlights the vulnerability of organizations. Employees often lack the necessary training to identify and mitigate cyber threats effectively. With proper training and awareness, these breaches can be largely prevented. This is where **CyberMaze** comes in, offering an innovative and user-friendly platform to develop practical cybersecurity skills in a simulated and gamified environment. By engaging participants in hands-on challenges, CyberMaze ensures effective and enjoyable learning [1] [2] [3].

For every individual working with technology or handling sensitive data, it's important to have knowledge of cyber-security—not just theoretical knowledge, but also practical experience. With the rise in cyber crimes, we need to assess our cybersecurity skills through real-world scenarios. CyberMaze aims to reduce the gap in theory and practice, by offering a virtual platform that constantly checks and improves a user's cybersecurity knowledge. It provides practical challenges across four key areas: network security, packet analysis, cryptography (like hash cracking), and cloud security. With tasks designed as Capture the Flag (CTF) games, users get to practice in realistic scenarios. This way, they learn by doing, not just reading, and become better at spotting and handling threats in real environments.

As a key component of CyberMaze, participants actively work with encryption and decryption activities, packet analysis, cloud security tools and techniques which are a central aspect of the security. Data breaches resulting from weak encryption are identified as 30The CyberMaze platform includes Capture the Flag (CTF) challenges that let participants solve actual cybersecurity problems by analyzing logs, exploiting vulnerabilities, and conducting reverse engineering tasks. CTF has a step-by-step learning method that advances participants from standard information discovery to complex offensive simulations. The importance of hands-on security assessment training becomes evident since research demonstrates that 70% of software applications do not pass their first security evaluation testing stage. Companies can lower their security vulnerabilities by 40% when implementing safe development practices in their CyberMaze CTF challenges (SANS Institute). Cloud security has become an essential capability for cybersecurity experts because 90% of companies are transitioning to cloud-based infrastructure. Through CyberMaze, users gain training on managing cloud security misconfigurations, identity and access management (IAM) control systems, and threat protection methods in the cloud. Users must collaborate with cloud providers through a shared responsibility model according to the platform's requirements. The training has participants determine insecure APIs and analyze vulnerabilities regarding account hijacking risks and data leakage exposure points. According to Gartner analysis, cloud security vulnerabilities stem mainly from customer configuration errors, which create 99% of cases (Gartner). Thus, structured cloud security training becomes crucial. Businesses with strong cloud security solutions reduce their breach recovery time by 35%, so it is vital to perform operational cloud security exercises.

By addressing these four domains, CyberMaze meets all the security awareness training needs [4]. As a result, the training


DOI: https://doi.org/10.67535/tsp.000001.026
Published under the ICACNC 2025 Proceedings

uses a challenge-based, hands-on methodology, ensuring that participants understand the concepts and have practical exposure to threats. As industries incorporate digital infrastructures in their tasks, preparing people with these skills is not a luxury; it is a necessity for the future of cybersecurity.

We begin by reviewing existing work on cybersecurity training approaches and gamification in cybersecurity education. We describe the methodology we used, the architecture of the platform, the evaluation scheme, scenario design and implementation, and a few other features of the platform. We elaborate on the four domains of CyberMaze and the challenges and tasks that the platform offers. Finally, the key findings of the paper and future goals of the platform are concluded.

## II. Related Work

### A. Traditional Training Approaches

Typical cybersecurity training techniques are based on conventional anchor training models, such as classroom teaching, textbook learning, and certification programs. Lectures, workshops, and seminars are typical classroom-based training methods with mainly theoretical content without practicality. Although knowledge is essential, textbook learning fails to contextualize this knowledge for real-world problem solving. Programs such as CompTIA, CISSP, and CEH certify experience but through incomplete curriculums with an undue focus on rote memorization over experiential learning. [5]. Although these traditional methods are helpful, they face many severe limitations. Most of the time, they fail to engage the learners because of their monotonous delivery methods. Cybersecurity is changing rapidly, and static content is becoming outdated very quickly. Furthermore, such minimal practical exposure makes learners unprepared for live challenges [6].

### B. Findings from Existing Studies

A desktop game, Hacked Time, is introduced by an interdisciplinary team at Carnegie Mellon University. Their study was conducted using Bandura's self-efficacy framework to enhance users' confidence and attitude towards cybersecurity tools [7]. To make it more interesting, the game provides an interactive design to the players by adding a bit of characters in the game. The main player acts as a time-travelling detective helping a student deal with a security breach. The game becomes more personally relevant to make the scenarios more engaging and carefully crafted. After receiving responses from 178 valid participants and measuring the demographics, the researchers are confident that the transformational goals of the game were achieved.

In another research [8], they converted three games into digital versions using Vassal and ran the game sessions via Google Cloud to monitor communication and self-efficacy of the team using a questionnaire. The game sessions and interviews were recorded and analyzed using thematic analysis. Nine participants, aged 23 to 30, were selected for the sessions and were divided into two groups. Although the researchers thoughtfully prepared the sessions, some technical issues were still observed. According to the participants, the topics were too broad, and they wished for more narrowly scoped topics. The study highlights the strong need for more engaging and intuitive approaches to game-based learning.

### C. Emerging Training Platform

Modern training platforms have evolved to overcome the limitations of the traditional approach. Cyber ranges are interactive environments that allow learners to learn cyber defense strategies in real time, such as IBM Security Range and Cyberbit. Capture the Flag competitions (CTF) are famous for hands-on problem-solving and critical thinking and are known and recognized in the cybersecurity community. In addition, gamified, practical training modules are available on online platforms such as TryHackMe, Hack The Box, and Cybrary. [9]. There are various benefits to these innovative platforms. Interactive learning environments are effective in engaging users and sure are fun! Scalability enables these platforms to service users from the greenhorn to advanced practitioners [10]. More such real-time feedback mechanisms make learning outcomes even more effective as they will allow the learner to identify and rectify his mistakes immediately.

However, these platforms are not perfect. Language barriers can limit access for non-English-speaking learners. Furthermore, domain-specific training is still a concern for many platforms because not all offer the focused challenges required within all possible cybersecurity domains, such as cryptography, social engineering, and cloud security.

TABLE I
Popular Game-Based Cybersecurity Learning Platforms

| Platform | Description |
|---|---|
| Hack The Box | Pen-testing labs with real-world challenges [11]. |
| TryHackMe | Guided labs and gamified learning paths [12]. |
| RangeForce | Blue team skill training and SOC simulations [13]. |
| CyberStart | Puzzle-based challenges for students [14]. |
| PicoCTF | Free CTF-style learning from CMU [15]. |
| Immersive Labs | Role-based simulations for cyber teams [16]. |

### D. Gamification in Cybersecurity Education

Gamification involves bringing game-like elements to education, such as scoring, leagues, challenges, etc., to increase engagement and motivation. It has been an effective means of promoting active learning in cybersecurity education. Gamification motivates learners to improve performance by encouraging competition through leaderboards and scoring systems. Interactive and engaging activities improve information retention much better than passive learning techniques. In addition, gamified challenges offer learners immediate problem-solving activities, connecting theoretical knowledge with its practical application. Table 1 highlights some of the most famous gamified learning platforms for cybersecurity students

and professionals. Gamification of cybersecurity education is exemplified by Capture the Flag (CTF) competitions. Participants solve challenges from cryptography, reverse engineering domains, and network security. This method has been proven to work in renowned CTF competitions such as DEF CON CTF, PicoCTF, and Google CTF [17]. From TryHackMe and Hack The Box, we have seen that gamification is also utilized on gamified learning platforms. TryHackMe offers gamification and structured learning paths to keep learners engaged. Hack The Box is a penetration test and provides a game-like environment to test your skills. In this case, gamified approaches consistently produce greater engagement of the learner and better skill acquisition than traditional approaches.

### *E. Trends and Statistics Supporting the Need for Hands-On Learning*

Cybersecurity threats are growing more frequently than ever before. Cybersecurity Ventures predicts in a 2023 report that cybercrime will cost the world $10.5 trillion annually by 2025. The attack surface has also increased: factors like increasing use of cloud services, IoT devices, and remote work have made cybersecurity training a proactive matter.

There is a vast shortage of skilled cybersecurity workers in the employable workforce. The (ISC)² Cybersecurity Workforce Study reports a shortage of nearly 3.4 million cybersecurity professionals globally. All too often, employers complain about lack of experience. But this makes it even more essential to train people with theoretical notions, hands-on skills, and the ability to solve real-world problems [18].

Hands-on learning is a well-documented earning method. Studies conducted by leading institutions have shown that hands-on learning retention rates are about 75%, while lecture-based learning rates are about 10%. Cyber ranges and CTF competitions have successfully built learner confidence and technical knowledge [19].

Organizational workforce development programs have become increasingly practical and training-based. For example, more than 70 percent of Fortune 500 companies now use cyber ranges as part of their training initiatives. The growing adoption of gamified platforms shows that they're cost-effective and practical in simulating real-world scenarios, which confirms the importance of hands-on training.

## III. Proposed Methodology

CyberMaze is an advanced cybersecurity training system that includes learning through interactive tasks and games. The website architecture guarantees firm security, and SCSA meets users' needs while presenting viable cybersecurity scenarios. This chapter describes the structural framework of the CyberMaze website, including its significant components, user-website interaction flow, evaluation criteria, and database operations.

## IV. Proposed Methodology

CyberMaze is an advanced cybersecurity training system that includes learning through interactive tasks and games. The website architecture guarantees firm security, and SCSA meets users' needs while presenting viable cybersecurity scenarios. This chapter describes the structural framework of the CyberMaze website, including its significant components, user-website interaction flow, evaluation criteria, and database operations.

### *A. Web Framework and Interaction Flow*

For the backend framework, Django is used to manage user interaction, security features, and content delivery. Django framework views handle authentication, HTTP requests, user credentials, database, and scenario content. Structured navigation of the web platform is ensured by the URL routing of the framework (e.g., /login/, /challenge/level1/).

Static front-end assets (HTML templates, CSS, JS) facilitate a responsive and interactive user experience. Training module access is streamlined by the system's dynamic rendering of challenge content and evaluation results.

### *B. Scenario Engine and Adaptive Learning*

CyberMaze provides users with customized game-based scenarios with prerequisites, tools, virtual labs, and hints used to complete the level using the scenario engine. These engines are used to map levels based on user preferences and contextual relevance. The engine tracks users' overall progress and adapts scenario complexity accordingly. User actions are monitored in real time and give meaningful feedback according to the actions.

### *C. Engagement Through Gamification*

CyberMaze integrates game-based mechanics to engage users. Challenges are structured in a way that progresses from easy to hard levels so that users start with enhancing foundational knowledge all the way up to hardcore cyber knowledge. The scoring system is designed to award points based on accuracy and completion speed.

### *D. Data Management and Logging*

A robust data layer is employed to manage CyberMaze operations securely and seamlessly. User databases are designed to store credentials, profiles, and registration data. Users' records are logged with all the performance metrics, timestamps, and scenario metadata that are then used for the evaluation scheme. For auditing and system improvement, activity logs are captured.

### *E. Level Design and Implementation*

CyberMaze incorporates its features and uses realistic cases that enable practical training in cybersecurity. Such scenarios are used to model the existing and potential cyber threats and issues. The key features include dynamic scenarios, threat modeling, and scenario levels. Dynamic scenarios are created by the scenario engine, which then adjusts the difficulty according to the user's skill set. Moreover, threat modeling is used in learning environments to mimic attacks on the infrastructure so that user devices will not be impacted. Conclusively, scenario levels are sorted by the difficulty level to complicate the device's use.

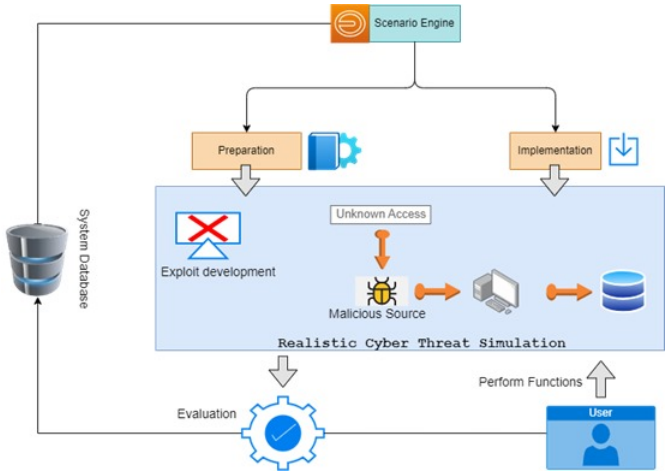


Fig. 1. Architecture

### F. Evaluation Scheme

Assessment is one of the profound features of CyberMaze, designed to evaluate users' performance effectively. The evaluation scheme includes a scoring system where users are awarded points based on the difficulty level of the challenges they complete. Bonus points may also be given for innovative approaches or for completing tasks faster than expected. Performance metrics are tracked, such as the number of attempts taken to overcome obstacles and the time required to complete each task. The results are displayed on the user panel and activity feed, while leaderboards are used to encourage healthy competition among participants. All user credentials and scores are securely stored in the database, ensuring system integrity and user data protection. Evaluation reports are generated instantly and are tailored to each user's activity and progress.

### G. Security Features

To ensure a secure and seamless experience, CyberMaze incorporates robust security measures:

### H. Authentication and authorization

The proposed model allows access to the user account while entering encrypted user account details. Also, it facilitates some measures of management to prevent unauthorized access. Users' personal information, along with their records and credentials, is stored encrypted in the database. Backup is done so as not to lose data, based on an average of three times per week. Some examples are performed on systems with secure virtual machines to prevent tasks from running concurrently with user equipment. This also makes it possible to avoid putting users' systems at risk during training.

### I. Database Design

Database functionality is one of the pillars of the CyberMaze platform, as all the essential data necessary for its operation is securely stored in a structured database. Key entities include the Users Table, which saves user credentials like usernames, email addresses, and passwords. The passwords are stored in a hashed format to ensure security. The Scores Table is responsible for recording user evaluations, results, and time taken to complete challenges. The Scenarios Table stores information related to each challenge, such as its level, type, and a brief description. Lastly, the Logs Table monitors and records user actions, which is essential for auditing purposes and performance evaluations.

### J. User Flow

The interaction flow within the CyberMaze platform is designed to be intuitive and user-friendly. The first step is user registration and login, where users create an account using a username and password. These passwords are encrypted and securely stored in the database, and the platform employs multiple authentication factors to enhance security. Once logged in, users can proceed to scenario selection, where they choose from a variety of available challenges based on their expertise level and area of interest. The scenario engine processes this request and returns the selected scenario. Afterward, users execute the challenge within a secure virtual machine (VM) environment. Progress is tracked in real time, and performance is assessed throughout the challenge. Once a task is completed, users receive a comprehensive evaluation and feedback. The performance data is stored in the database and visualized on the user dashboard, helping users track their growth and identify areas for improvement.

## V. Domains

### A. Network Communication in the Context of CTF

Understanding how devices interact with a network is at the heart of cybersecurity. When two devices communicate, they send data packets to one another. Thus, each packet contains information about the source and destination IP addresses, protocol used, etc., and information relative to the data transmission itself.

IP-to-IP Communication Process starts with request initiation. A source device (e.g., client) requests a destination device

(e.g., server). It wraps this request into a packet containing everything a router and processor must know to route and process. It travels through the network and is guided by intermediate devices such as routers and switches. The packet is routed to its destination by routers, and the switch handles the local network traffic. The source gets the request, then the destination processes and generates the response, and then sends it back to the source. At the same time, it creates a conversation like this. When the data exchange is completed, TCP-based communication is terminated.

### *B. The Four Stages of the CTF Module*

Capture the Flag module is broken down into four parts, each bringing increasingly tricky tasks. The stages are:

*1) Stage 1: Packet Analysis:* At this introductory level, learners study traffic in a network using Stage 1.pc, which is included in the learning material. They will consist of packet type, contents, source, and destination IP addresses of the packet, which makes it easier to find essential details about the packets. [20]

To analyze the packet capture, follow these steps: Launch Wireshark, Install Wireshark, and use Safe Modeanden. Download the Stage 1.pcap file. Open the newly downloaded file using Wireshark. Analyze packet data, accessing the information about the type of packet and packet inside, along with the source IP and the destination IP.

*2) Stage 2: Packet Analysis Part 2:* As you can see, this stage progresses from the previous level of analysis by including new, more complex analysis tasks. Using Stage 2. pcapng file, learners open packets and extract objects, such as HTTP packets, and then answer questions about these objects and whether they are scripts, images, etc. Open the Stage 2.pcapng file using the Wireshark network analyzer tool that was provided in the class. Extract objects from packets and analyze details such as components of objects (e.g., typeface, color, or location) and check the origin and terminal of the data packets transmitting through the system.

*3) Stage 3: Packet Analysis Part 3:* At this interesting level, people are increasingly analyzing network traffic. Analyze the tools section of the analyzer. Firewalls, credentials, and MAC addresses are all information put in place in the 'tools' section. Tasks in this stage include identifying the username, locating the packet number of the user, and finding what the argument is in a packet. Locating where the data packet came from and where it's going. They download the Stage 3.pcapng file and conduct deep traffic digging to find secrets.

*4) Stage 4: Packet Analysis Part 4:* Learners in this last stage analyze packets using the Injector.pcap file, which contains some packets that are considered malicious. The targeted activity is based on the analysis of the f examination of the f Spam Detector Log suspicious activity from the IP 127.0.0.1, nature of the attack [21]. Initially, copy Injector.pcap on the Wireshark and analyze packet data to determine. Then, check which HTTP frame seems to be malicious. In more precise cases, there is a question of what type of attack or security problem is present in separate frames, such as frames 4 and 16. Analyze the queries being sent in these frames and provide outputs for the study, including the flag injector to the Injector analysis.

At these stages, learners acquire comprehensive knowledge of network communication's vicissitudes and skills in using procedures to prevent network security threats. CyberMaze guarantees that participants will gain all the knowledge and tools required for the Cybersecurity profession.

The participants download the Injector. pcap file to investigate traffic and look for malicious behaviors and anomalies. This stage explores in detail how to sharpen packet analysis skills and techniques for detecting possible threats in a network.

Each stage is an additional step to improve participants' experience in understanding network security, building analytical skills, and a practical approach to solving cybersecurity challenges. The module puts these stages in a real-world CTF competition context, which makes it an educational and fun module to teach.

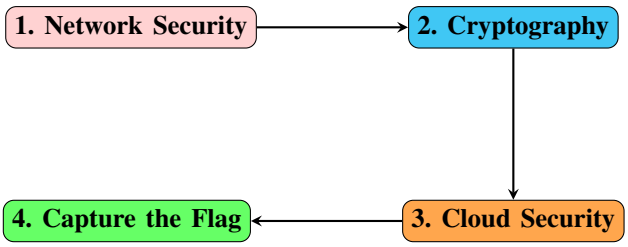


Fig. 2. Key steps in the security process

## VI. Conclusion

CyberMaze platform is a robust, gamified learning environment that fills critical cybersecurity education gaps. It combines real-world challenges, a gamified structure, and hands-on scenarios in multiple domains to equip users with the technical knowledge to protect against emerging security threats.

Types of challenges, based on each respective domain, such as Cryptography, Network Security, Cloud Security, and Capture the Flag (CTF), are targeted expressions of real-world complications. Deciphering encrypted data and analyzing network packets are activities that aid them in sharpening their problem-solving abilities and technical expertise. Including AWS security scenarios like the Cloud Recon Challenge exposes participants to cloud-specific risks and best practices.

CyberMaze aims to be accessible and friendly to users. In a safe, controlled environment, participants can interact with challenges through a web-based interface. Users who work through similarly tricky tasks feel a sense of accomplishment. Experiential learning is a key highlight of CyberMaze. Participants can directly transfer the skills they have gained through working with realistic scenarios to industry settings. CyberMaze remains relevant for anyone who wants to improve their organization's security. Its focus on training through scenarios, gamified approach, and ease of access make It a

TABLE II
CYBERMAZE PLATFORM CHALLENGES AND TASKS OVERVIEW

| Section | Description | Key Concepts | Tasks |
|---|---|---|---|
| Cryptography | Central to the CyberMaze platform, focusing on encoding, decoding, and analyzing secured systems. | Encryption, decryption, code-cracking, practical exercises. | Practice cryptographic methods, identify weaknesses, and crack codes. |
| XOR Cipher Challenge | Introduces XOR encryption and decryption through practical exercises. | Boolean XOR operation, encryption/decryption process, strengths, and weaknesses of XOR. | Perform XOR operations to encrypt/decrypt plaintext and understand XOR's strengths and weaknesses. |
| The Missing Treasure Map | A cipher-based challenge where learners decode an encrypted map using substitution ciphers. | Substitution ciphers, frequency analysis, problem-solving. | Analyze and break substitution ciphers using frequency analysis and pattern recognition. |
| Substitution Cipher Mystery | An entry-level challenge requiring users to decrypt a message using a substitution cipher. | Substitution ciphers, logical reasoning, historical context. | Decipher a substitution cipher using logical thinking and learn about its historical applications. |
| Hash Cracking | Focuses on the role of hash functions in securing data and identifying weaknesses. | Hashing concepts, collision vulnerabilities, ethical hacking. | Explore hash functions, identify weaknesses, and use online tools to crack hashed passwords. (Tools: Xorbin, Hashcat, Crackstation) |
| Cloud Security | Addresses security issues in cloud environments through practical scenarios. | Cloud infrastructure security, AWS services, compliance. | Analyze security flaws in AWS, audit logs, and identify unauthorized activities. |
| Cloud Recon | Evaluates security flaws in AWS Lambda functions and S3 buckets. | AWS security, IAM policies, cloud vulnerability analysis. | Download and analyze cloud-recon.yaml, identify vulnerabilities, and submit discovered flags. (Tools: AWS Management Console, CloudTrail) |
| Trail of Troubles | Learners analyze AWS logs to detect and trace malicious activities. | Log analysis, API call tracking, detecting unauthorized access. | Download CloudTrail logs, identify malicious activities, and find and submit the hidden flag. (Tools: AWS Management Console, CloudTrail) |
| Network Security | Explores various tools and techniques to assess network vulnerabilities. | Network scanning, penetration testing, SQL injection. | Perform network scans, identify vulnerabilities, and exploit weaknesses in web applications. (Tooks: Nmap, Burp Suite (optional), SQLmap (optional)) |
| Stay Aware Using Nmap | Introduces network scanning using Nmap, focusing on vulnerability assessment. | Port scanning, service identification, advanced scanning techniques. | Perform port checks, service identification, and advanced scanning on specified IP addresses. (Tool: Nmap) |
| SQL Injection | Teaches how to find and exploit SQL injection vulnerabilities in web applications. | SQL injection methods, database exploitation, data retrieval. | Identify vulnerable packets, extract database information, retrieve usernames and passwords through SQL injection. (Tools: Nmap, Burp Suite (optional), SQLmap (optional)) |

prime exemplar of best practices in addressing the cyber skills gap. As such, the resource is flexible and can remain relevant to new layers of cybersecurity instruction in perpetuity.

## REFERENCES


[1] I. Haider, M. A. Qureshi, A. Amin, and A. Saeed, "An efficient cyber security framework for network intrusion detection using hybrid classifier," in *2023 25th International Multitopic Conference (INMIC)*. IEEE, 2023, pp. 1–6.

[2] I. Haider, M. A. Qureshi, A. Saeed, and M. A. Haider, "Enhanced model for data security in cyberspace using combined steganographic and encryption techniques," in *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences, and Technology (ICES&T)*. IEEE, 2023, pp. 1–6.

[3] M. C. Natalia, S. Cayhono, R. Purwoko, and I. G. Maha Putra, "Gamification design as learning media to motivate students to increase cyber security awareness towards phishing," in *2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS)*, 2023, pp. 252–256.

[4] S. Almass and S. K. Chowdhary, "Comprehensive study on cyber security and cyber attacks," in *2024 First International Conference on Electronics, Communication and Signal Processing (ICECSP)*, 2024, pp. 1–6.

[5] R. Jouaibi, A. K. Gaylard, and B. Lee, "Employee cyber-security awareness training (csat) programs in ireland's financial institutions," in *2022 Cyber Research Conference - Ireland (Cyber-RCI)*, 2022, pp. 1–4.

[6] Y. S. Park, C. S. Choi, C. Jang, D. G. Shin, G. C. Cho, and H. S. Kim, "Development of incident response tool for cyber security training based on virtualization and cloud," in *2019 International Workshop on Big Data and Information Security (IWBIS)*, 2019, pp. 115–118.

[7] T. Chen, M. Stewart, Z. Bai, E. Chen, L. Dabbish, and J. Hammer, "Hacked time: Design and evaluation of a self-efficacy based cybersecurity game," in *Proceedings of the 2020 ACM Designing Interactive Systems Conference*, ser. DIS '20. New York, NY, USA: Association for Computing Machinery, 2020, p. 1737–1749. [Online]. Available: https://doi.org/10.1145/3357236.3395522

[8] M. Gutfleisch, M. Schöps, S. Sayin, F. Wende, and M. A. Sasse, "Putting security on the table: The digitalisation of security tabletop games and its challenging aftertaste," in *2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)*, 2022, pp. 217–222.

[9] Angelogianni, I. Politis, P. L. Polvanesi, A. Pastor, and C. Xenakis, "Unveiling the user requirements of a cyber range for 5g security testing and training," in *2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2021, pp. 1–6.

[10] M. Karjalainen and T. Kokkonen, "Comprehensive cyber arena; the next generation cyber range," in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2020, pp. 11–16.

[11] Hack The Box, "Hack the box - penetration testing labs," https://www.hackthebox.com/, 2024, accessed: 2025-04-14.

[12] TryHackMe, "Tryhackme - learn cyber security online," https://tryhackme.com/, 2024, accessed: 2025-04-14.

[13] RangeForce, "Rangeforce - cyber security training platform," https://www.rangeforce.com/, 2024, accessed: 2025-04-14.

[14] CyberStart, "Cyberstart - learn cybersecurity through play," https://www.cyberstart.com/, 2024, accessed: 2025-04-14.

[15] picoCTF, "picoctf - free cybersecurity game," https://picoctf.org/, 2024, accessed: 2025-04-14.

[16] Immersive Labs, "Immersive labs - cyber workforce training," https://www.immersivelabs.com/, 2024, accessed: 2025-04-14.

[17] M. Beltrán, M. Calvo, and S. González, "Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2018, pp. 574–579.
[18] F. H. Sohime, R. Ramli, F. A. Rahim, and A. A. Bakar, "Exploration study of skillsets needed in cyber security field," in *2020 8th International Conference on Information Technology and Multimedia (ICIMU)*, 2020, pp. 68–72.
[19] H. Shahriar, M. Whitman, D. C.-T. Lo, F. Wu, C. Thomas, and A. Cuzzocrea, "Experiential learning: Case study-based portable hands-on regression labware for cyber fraud prediction," in *2019 IEEE International Conference on Big Data (Big Data)*, 2019, pp. 5814–5818.
[20] Y. Gautam, B. P. Gautam, and K. Sato, "Experimental security analysis of sdn network by using packet sniffing and spoofing technique on pox and ryu controller," in *2020 International Conference on Networking and Network Applications (NaNA)*, 2020, pp. 394–399.
[21] L. Bock, *Learn Wireshark: A Definitive Guide to Expertly Analyzing Protocols and Troubleshooting Networks Using Wireshark*. Packt Publishing, 2022.