Game-based teaching platform

Cyber Security

What is Cyber Security?

Cybersecurity is the practice of protecting computer systems, networks, data, and digital infrastructure from unauthorized access, attacks, damage, or theft

What problem we face learning cyber security

Too Broad

Many topics, hard to know where to start.

Lack of Practice

Too much theory, not enough hands-on experience.

Requires IT Basics

Need knowledge in networking, OS, and programming.

Takes Time

Slow progress can be discouraging.

What problem we face learning cyber security

High Costs

Some tools, courses, and certifications are expensive.

Constantly Changing

Hard to keep up with new threats and tools.

Legal Confusion

Unclear boundaries between ethical and illegal hacking

How our project going to solve that problem

Our **Game-Based Security Tool** solves the problem of low cybersecurity awareness by making learning **interactive, engaging, and accessible**. Instead of relying on boring lectures or static materials, the tool uses **gamified challenges** to teach users about threats like phishing, weak passwords, and malware in a fun and memorable way. This approach helps users **retain knowledge**, **apply it in real life**, and **develop better security habits**.

Overview of the Platform's Core Functionality

Our Cybersecurity game like teaching Platform is designed to simulate real-world hacking scenarios and educate users through progressive, interactive levels, which would be fun, easy to learn and affective at same time. The platform provides hands-on teaching at the most efficient way, using game like questions/exams between levels and well desined videos teaching in affective and fast way while maintaining a secure, fun and controlled learning environment

Technologies Used

1.Frontend: HTML, CSS, JavaScript, and React.js for a dynamic and responsive user interface.
2.Backend: Python and SQL for server-side logic, data management, and user authentication.
3.Authentication: Integration with a secure token-based system and optional multi-factor authentication (e.g., Google Authenticator).

Key Functional Features

1.User Authentication and Authorization:

- Secure sign-up and login forms.
- Token-based sessions (e.g., JWT) to protect user data.
- Optional integration with Google Authenticator for multi-factor authentication.

2. Level Progression System:

- Each level presents a new hacking concept (e.g., Reconnaissance, Scanning, Exploitation depends on which path user choose).
- Users must complete a mini-quiz or challenge to proceed (might add weekly challenges or any kind of events for more engagement in the learning process).
- Progress is tracked and stored securely in the database.

Key Functional Features

3.Interactive Learning Environment:

- Realistic simulations and quizzes.
- Visual feedback for correct/incorrect answers.
- Engaging UI using animations and themed design.

4. Admin Panel (Optional):

-Manage users, view progress reports, and upload new levels.
- Token Expiry: Tokens have limited lifetimes to prevent unauthorized access.
- Input Validation: All user inputs are sanitized to prevent SQL injection and XSS attacks.

THANK YOU

By

WALEED BASIM ELSHAYIB (2131363)

ADHAM SAMI AL-HAMAIDEH (2232537)

MOHAMMAD MUHSEN MAREI(2140721)

Supervised by

Ibrahim Moh'd Salem Obeidat

The Hashemite University, Zarqa, Jordan