International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 3, 2025

Cyberquest : The Security Challenge

A Vasavi Sujatha, A Rithisha, Samiha Sarwar, Shaik Mahin

[1]Assistant Professor, Department of Information Technology, Bhoj Reddy Engineering College for Women

[2.3.4]B,tech students, Department of Information Technology, Bhoj Reddy Engineering College for Women

ABSTRACT

Cyberquest is an interactive, web-based game designed to educate users on essential cybersecurity concepts through an engaging and gamified learning experience. The project aims to bridge the knowledge gap in cybersecurity by simulating real-world digital threats such as phishing, malware, social engineering, and weak passwords in a controlled, educational environment.Developed using Python, Flask, HTML/CSS, and JavaScript, the game provides a user-friendly interface with interactive challenges and quizzes. Players navigate through various security scenarios, where they must identify threats, make secure choices, and answer conceptual questions. The system tracks player scores and progress, offering instant feedback and motivation to improve.Cyberquest is ideal for students, professionals, and anyone interested in cybersecurity awareness. It combines fun gameplay with educational value, making it an effective tool for learning security best practices. The project also supports open-source collaboration, allowing contributors to enhance its features and expand the challenge library.By turning cybersecurity education into a game, Cyberquest makes learning accessible, enjoyable, and impactful.

Keywords: Cybersecurity, Gamification, Web-based learning, Interactive game, Flask, Python, Cyber awareness, Phishing, Malware, Security education, User engagement, Quiz-based learning, Threat simulation, Educational game, Open-source project.

1. INTRODUCTION

In today's digitally connected world, cybersecurity has become an essential part of everyday life. With rapid rise in cyber threats such as phishing attacks, ransomware, data breaches, and password theft, the need for cybersecurity awareness is more critical than ever. However, traditional learning methods often fail to engage users or convey real-world relevance effectively.

Cyberquest is an interactive web-based game developed to bridge this knowledge gap through an engaging and educational approach. The game immerses players in a virtual environment where they face simulated cybersecurity challenges, make decisions, and learn the consequences of their actions. By transforming complex cybersecurity concepts into fun and interactive gameplay, Cyberquest makes learning accessible and effective for users of all backgrounds.

Built using Python, Flask, HTML/CSS, and JavaScript, the game features educational content, real- time quizzes, and progress tracking to reinforce learning[1]. It is designed to be both informative and enjoyable, offering players a hands-on experience that promotes safe digital behavior [5].

Whether you're a student, a working professional, or simply a curious user, Cyberquest provides a unique platform to build awareness, test knowledge, and develop best practices in cybersecurity all while having fun.

Existing System:

Uses traditional learning methods like articles, videos, and courses, which focus on theoretical knowledge but lack engagement. Learning is mostly passive, leading to low retention and minimal practical application of cybersecurity concepts. Lacks interactive elements such as hands-on exercises and real-world simulations to help users develop cybersecurity skills. Does not provide real-time feedback, making it difficult for users to recognize mistakes and improve their understanding. Does not test problem-solving skills, making it harder for users to apply cybersecurity concepts in real-world situations.

Proposed System:

The proposed system, Cyberquest, is a web-based interactive game designed to educate users about cybersecurity through engaging gameplay. It simulates real-life cyber threats and challenges, allowing users to experience and respond to situations such as phishing attacks, malware infections, and password breaches in a controlled environment [4]. The system uses Python and Flask for backend logic, with HTML, CSS, and JavaScript for an intuitive user interface. Players progress through different levels, each introducing new cybersecurity concepts, and their actions are tracked to provide scores and feedback. By incorporating quizzes, instant feedback, and realistic scenarios, the proposed system offers an innovative, accessible, and effective way to enhance cybersecurity awareness and learning for users of all ages.

2-RELATED WORK

In recent years, there has been a significant shift towards using interactive and gamified approaches to cybersecurity education. Traditional methods such as lectures, textbooks, and static online tutorials often lack the engagement needed to motivate learners, especially those without a technical background. Research indicates that gamification—using game elements like scoring, levels, challenges, and instant feedback—can greatly enhance learner motivation and improve knowledge retention [6].

Several cybersecurity education platforms have been developed with this in mind. For example, Cybersecurity Lab by NOVA provides users with simulations that demonstrate common cyber attacks and defense mechanisms. Similarly, platforms such as Hack The Box and TryHackMe offer practical challenges to improve cybersecurity skills. However, these platforms tend to target users with some prior knowledge or technical expertise, which can be intimidating for beginners [14].

User surveys and feedback collected from these platforms highlight the need for more accessible, beginner-friendly cybersecurity education tools. Key user demands include simplified explanations, gradual progression of difficulty, real-time feedback, and engaging content that can hold learners' attention [10]. Additionally, many users express a preference for web-based platforms that require minimal setup and can be accessed from any device [9].

Given these insights, there is a clear opportunity to develop an interactive, web-based game like Cyberquest that caters to a wider audience. By combining educational content with an engaging gaming experience, Cyberquest aims to make cybersecurity concepts approachable and enjoyable for users of all ages and skill levels. This approach not only addresses gaps in existing resources but also supports continuous learning and awareness in a fun and motivating way [6].

3-REQUIREMENT ANALYSIS

1.1 Functional Requirements:

The functional requirements define the core operations and features that the system must perform. Below is the list of essential functionalities for the proposed Cyberquest system:

1. **User Registration and Login**

- The system must allow new users to register with a username, password, and email.
- Existing users must be able to securely log in and access their progress.

2. **Role-Based Access**

- Provide separate views for Admin (manage quizzes/content) and Players (play game, take quizzes).

3. **Interactive Game Environment**

- The system must allow users to navigate through different cybersecurity-themed levels.
- Each level must present a challenge or scenario involving a cybersecurity threat.

4. **Score Management System**

- The system must assign points based on correct answers and level completion.
- Scores should be stored in the user profile and displayed on a leaderboard.

3.2 Non-Functional Requirements:

The Non-functional requirements define the quality attributes and performance standards of the system. They ensure the platform is efficient, secure, and user-friendly for an optimal learning experience

1. **Usability**
- The game should have an intuitive and user-friendly interface suitable for users with basic cybersecurity knowledge.
2. **Performance**
- The system should respond to user inputs (e.g., quiz answers, navigation) within 1 second to ensure smooth gameplay.
3. **Reliability**
- The game should maintain consistent functionality across sessions, ensuring no loss of progress or scores due to crashes.

- **Software Requirements:**

Front-end development : HTML, CSS, JavaScript, React.js
Back-end development : Python, Flask, MySQL
Containerization : Docker
IDE : Visual Studio Code or PyCharm

- **Hardware Requirements:**

Processor : Intel i5 or above
RAM : 8GB or Higher
Hard Disk : 512 GB SSD or Higher
Operating System : Windows 10/11, macOS, or Linux

4. DESIGN

System Architecture:

It describes the structure and behavior of technology infrastructure of an enterprise, solution or system. In other words, System architecture can be described as the flow of application which is represented below in the pictorial form. The purpose of system architecture activities is to define a comprehensive solution based on principles, concepts, and properties logically related to and consistent with each other. The solution architecture has features, properties, and characteristics which satisfy, as far as possible, the problem or opportunity expressed by a set of system requirements (traceable to mission/business and stake holders requirements).

System architecture is abstract, conceptualization-oriented, global, and focused to achieve the mission and life cycle concepts of the system. It also focuses on high-level structure in systems and system elements [12]. It addresses the architectural principles, concepts, properties, and characteristics of the system-of-interest. It may also applied to more than one system, in some cases forming the common structure, pattern, and set of requirements for classes or families of similar or related systems [9].

The SEBoK considers systems engineering to cover all aspects of the creation of a system, including system architecture.

The majority of interpretations of system architecture are based on the fairly intangible notion of structure (i.e relationships between elements). Some authors limit the types of structure considered to be architectural: for example, restricting themselves to functional and physical structure. Recent practice has extended consideration to include behavioral, temporal and other dimensions of structure.

ISO/IEC/IEEE 42010 Systems and Software Engineering – Architecture Description (ISO 2011) provides a useful description of the architecture considering the stakeholder concerns, architecture viewpoints, architecture views, architecture models, architecture descriptions, and architecting throughout the life cycle.

A discussion of the features of systems architectures can be found in(Maier and Rechtin 2009). An attempt to develop and apply a systematic approach to characterizing architecture belief systems in systems engineering has been described by the INCOSE UK Architecture Working Group (Wilkinson et al.2010, Wilkinson 2010).

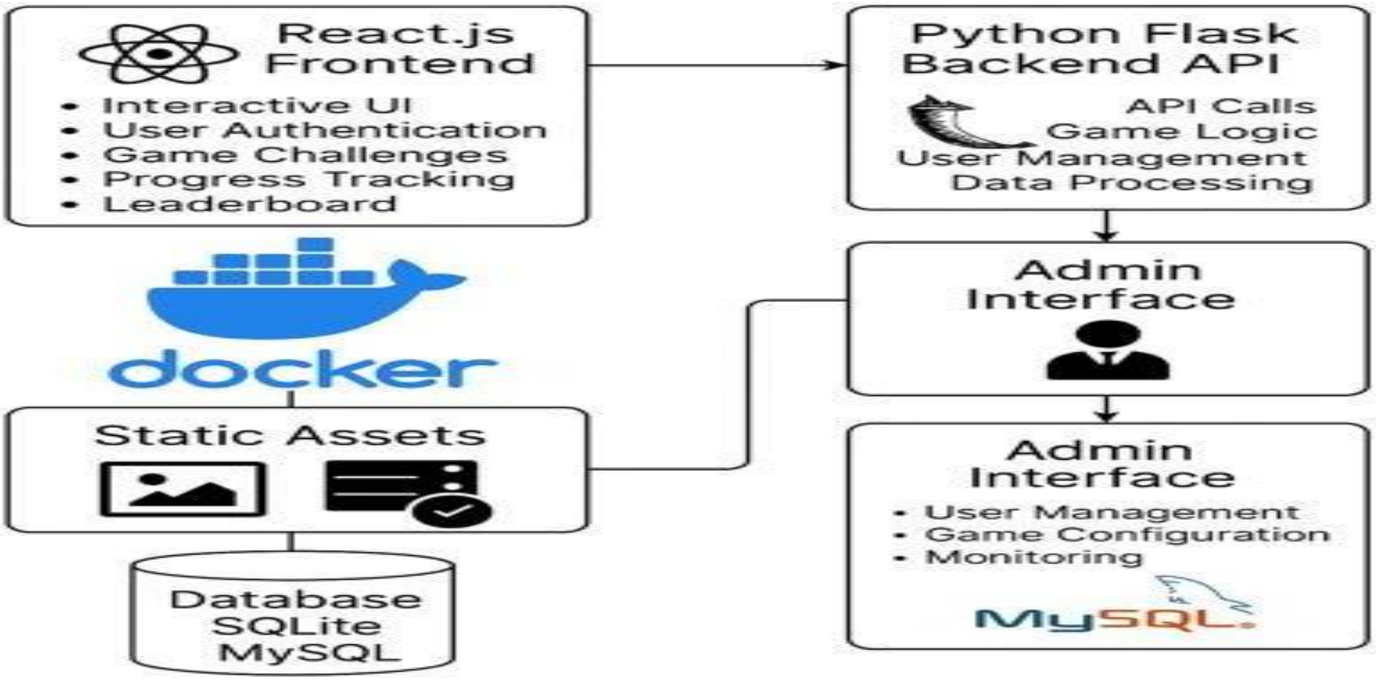


Fig. 4.1.1.1 System Architecture

4.1.1 Technical Architecture:

Technical Architecture refers to the structural process of designing and building system's architecture with focus on the users and sponsors view of the environment. Technology architecture associates application components from application architecture with technology components representing software and hardware components. Its components are generally acquired in the market place and can be assembled and configured to constitute the enterprise's technological infrastructure. A technical architecture diagram provide a bird's eye view of the infrastructure of our project. The diagram illustrates how components in a system interact with one another in the large scale of things. Technical Architecture (TA) is a form of IT architecture that ids used to design computer system. It involves the development of a technical blueprint with regard to the arrangement, interaction, and interdependence of all elements so that system-relevant requirements are met.

Throughout the past decade, architecture has become a broadly used term in the context of information technology. This doesn't come as a surprise considering how most companies had to redesign their IT landscape to adopt digital trends like cloud computing software as service (SaaS). This digital transition required not only skilled developing teams but first and foremost IT architects. In their roles as IT strategists and planners, they map out a target architecture and make sure that all IT decisions align with business goals and requirements.

But IT architecture encompasses a variety of different roles and disciplines that are sometimes difficult to tell apart. This is largely due to highly dynamic nature of IT, its widespread adoption throughout all industries and business that have developed their own practices. In general, there's differentiation between enterprise architecture, solution architecture and technology architecture. In order to understand what technology architecture means, it's helpful to examine the term architecture on its own.

At its core, the term architecture describes the formation of a structure by strategically assembling single components. In this process of assembling, the architect has to adhere to certain rules or requirements like legal constraints, financial constraints or scientific laws. In the world technology architecture design, the focus lies on technology limitations, meaning that a technology architect makes sure that a new application is compatible with the existing technology at a company by specifying things like the communications network or hardware that it uses.

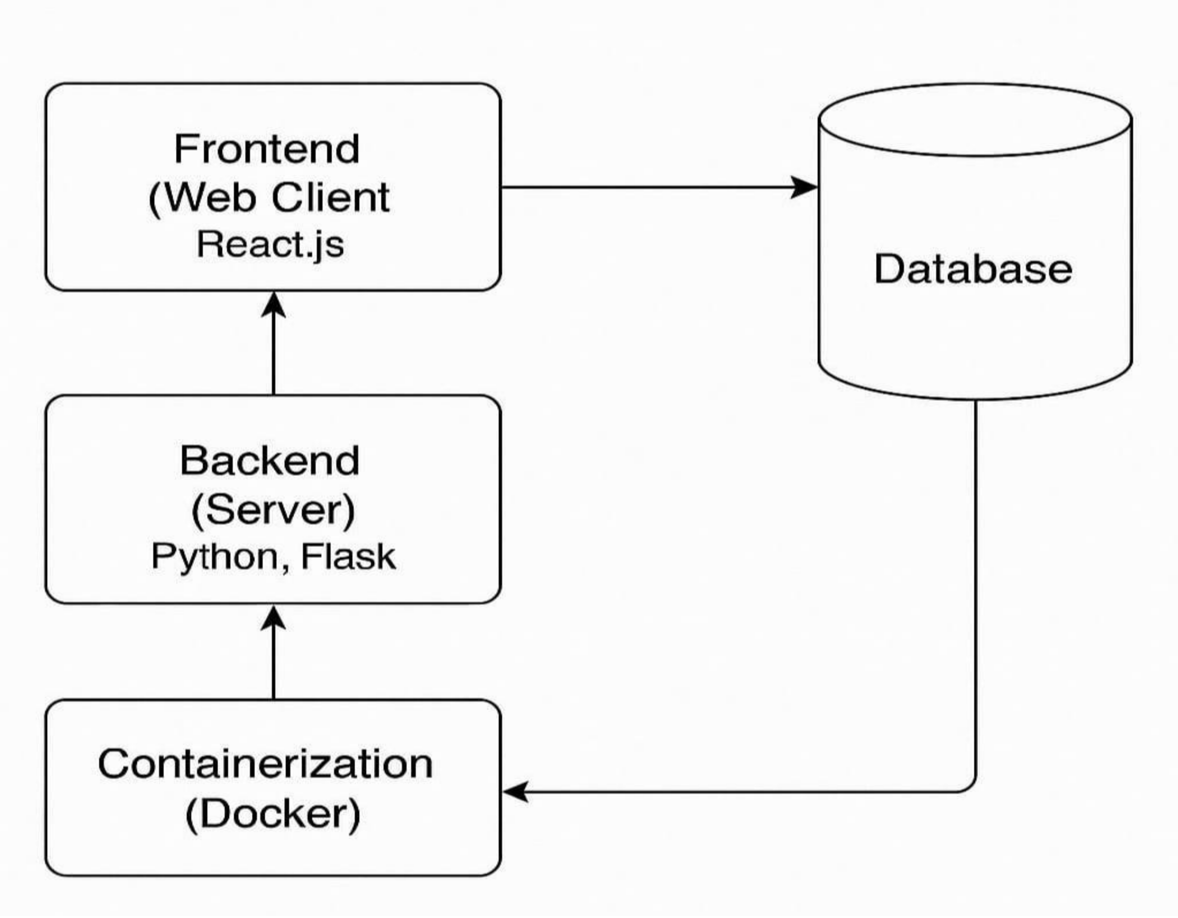


Fig. 4.1.2.1 Technical Architecture

5. IMPLEMENTATION

5.1 Libraries

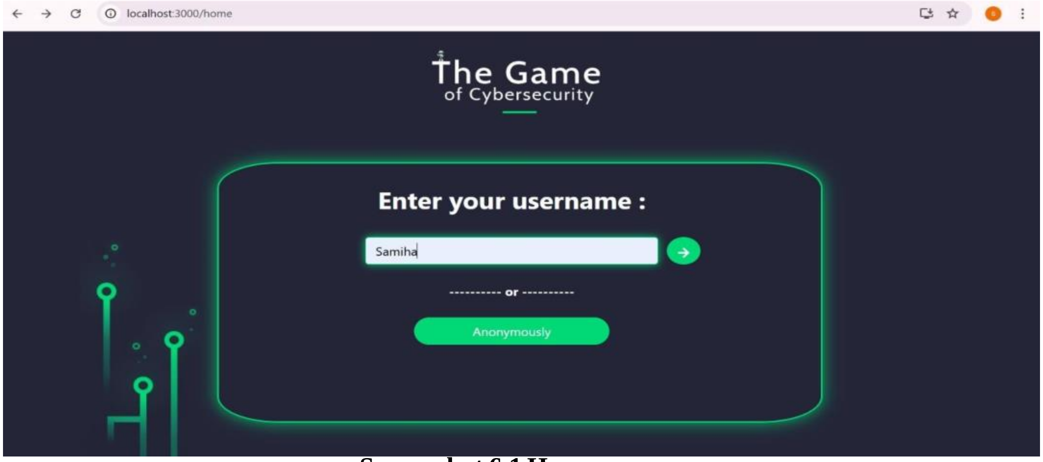
Backend (Python / Flask)

1. **Flask**
- Web framework used to build the backend.
- Handles routing, templates, and request/response management.
2. **Flask-Cors** (if present)
- Allows Cross-Origin Resource Sharing (CORS) support for frontend-backend communication.
3. **Werkzeug**
- A Flask dependency that handles routing, debugging, and server operations.
4. **Jinja2**
- Template engine used with Flask for rendering HTML with dynamic data.
5. **os / sys**
- Standard Python libraries for file system operations and system interactions.
6. **json**
- To manage user data, quizzes, or game state in a structured format [11].

Frontend (HTML / CSS / JavaScript)

1. **HTML5 & CSS3**
- Markup and styling for UI elements and layout.
2. **Bootstrap** (if used)
- Frontend framework for responsive and clean UI design.
3. **JavaScript**
- Adds interactivity, like dynamic buttons, real-time feedback, and score updates.
4. **jQuery** (optional)
- Simplifies JavaScript operations (e.g., DOM manipulation, AJAX calls).

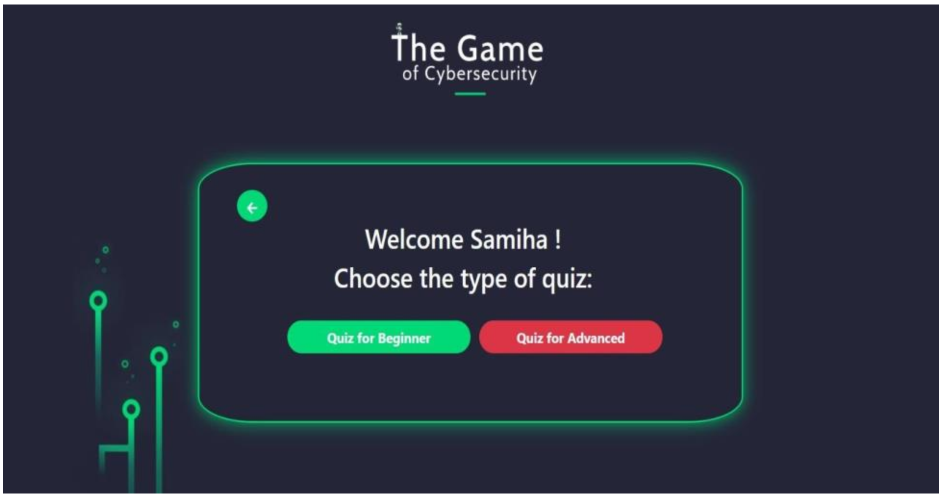
6-Screenshots



Enter your username :

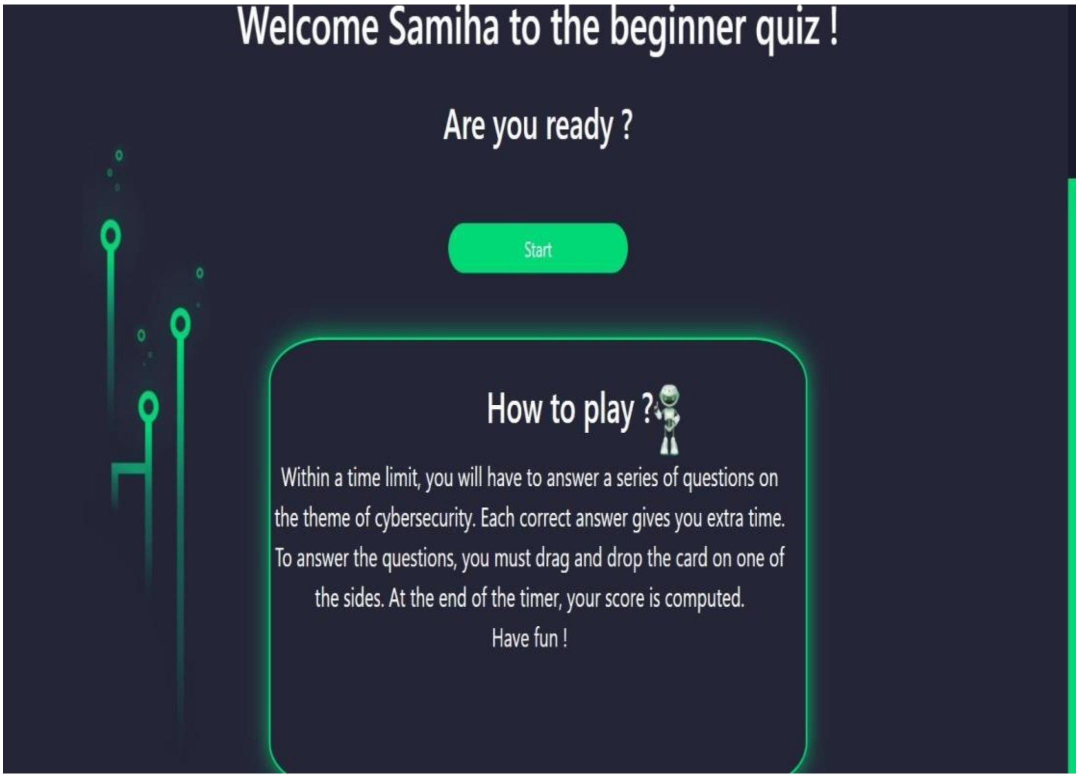
Samiha

Screenshot 6.1 Home page



Welcome Samiha !
Choose the type of quiz:

Screenshot 6.2 Type of Quiz



Welcome Samiha to the beginner quiz !

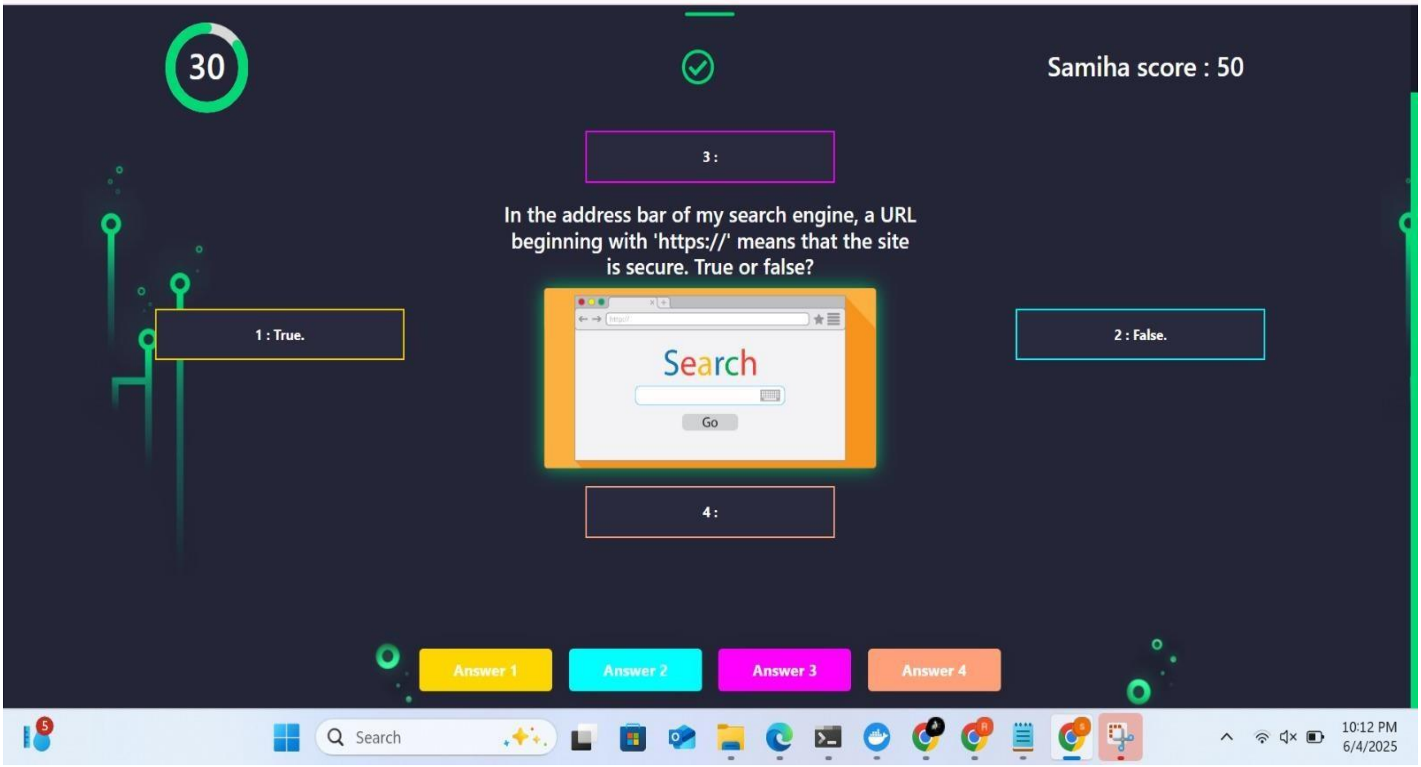
Are you ready ?

How to play ?

Within a time limit, you will have to answer a series of questions on the theme of cybersecurity. Each correct answer gives you extra time. To answer the questions, you must drag and drop the card on one of the sides. At the end of the timer, your score is computed.

Have fun !

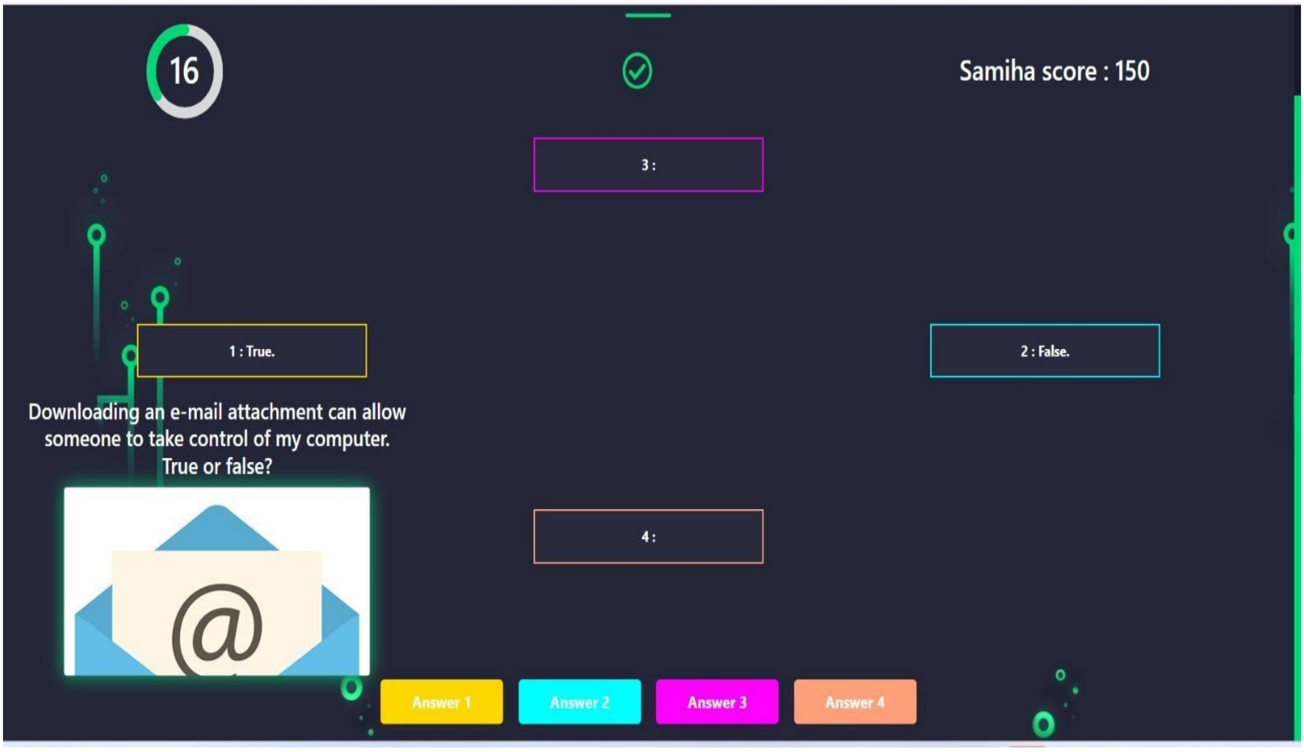
Screenshot 6.3 Beginner level Quiz



Samiha score : 50

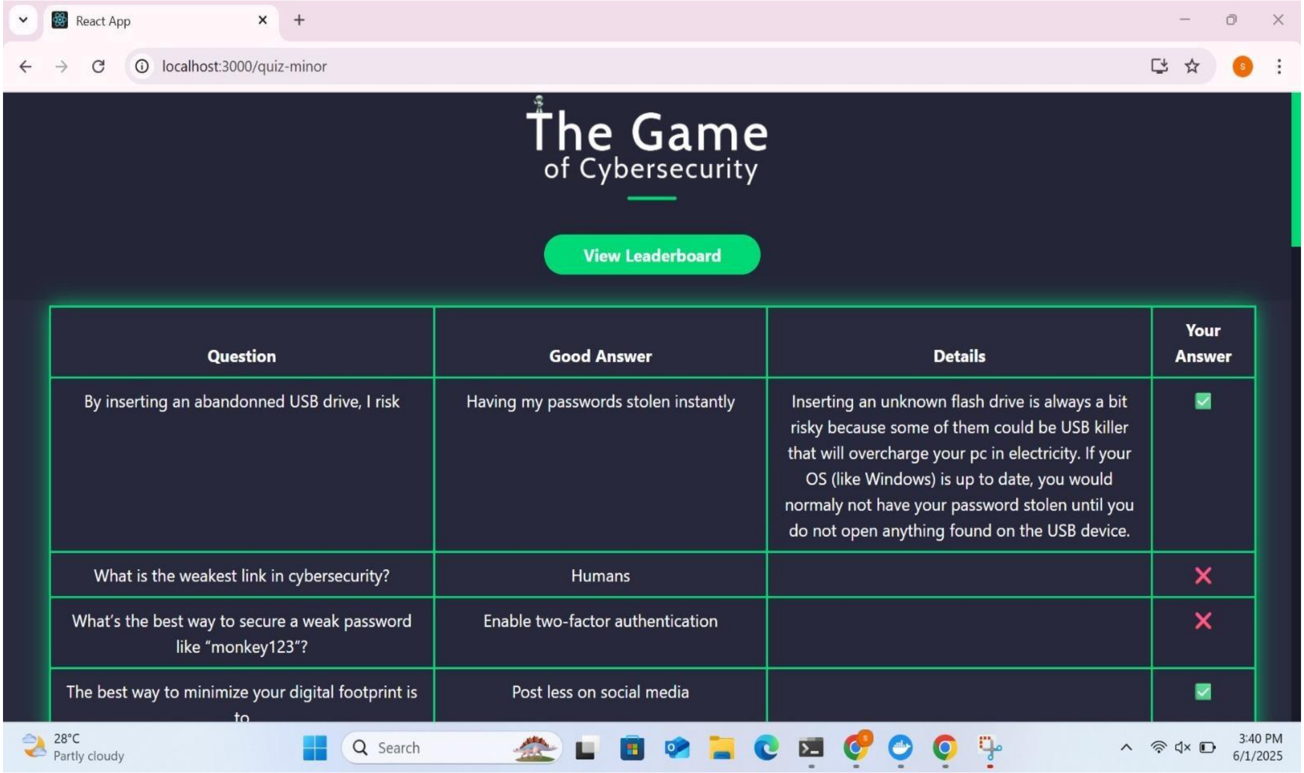
In the address bar of my search engine, a URL beginning with 'https://' means that the site is secure. True or false?

Screenshot 6.4 Quiz using buttons



Downloading an e-mail attachment can allow someone to take control of my computer. True or false?

Screenshot 6.5 Quiz using Swipe feature

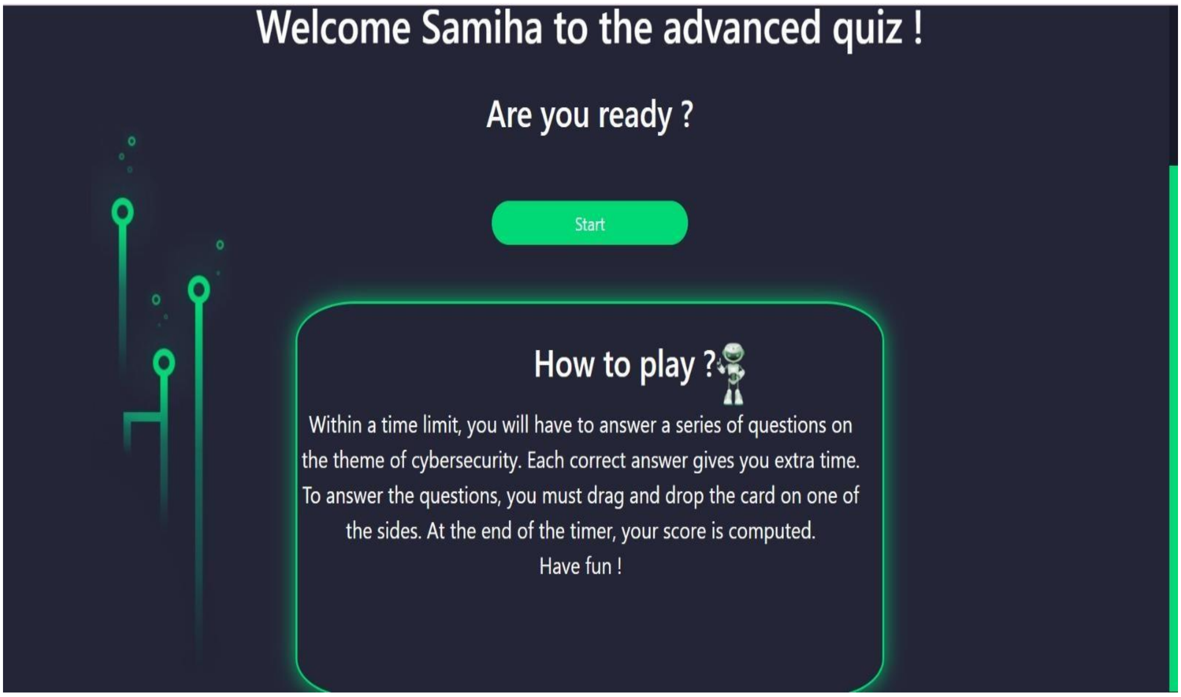


The Game of Cybersecurity

View Leaderboard

Question	Good Answer	Details	Your Answer
By inserting an abandonned USB drive, I risk	Having my passwords stolen instantly	Inserting an unknown flash drive is always a bit risky because some of them could be USB killer that will overcharge your pc in electricity. If your OS (like Windows) is up to date, you would normaly not have your password stolen until you do not open anything found on the USB device.	✓
What is the weakest link in cybersecurity?	Humans		✗
What's the best way to secure a weak password like "monkey123"?	Enable two-factor authentication		✗
The best way to minimize your digital footprint is to	Post less on social media		✓

Screenshot 6.6 Beginner level



Welcome Samiha to the advanced quiz !

Are you ready ?

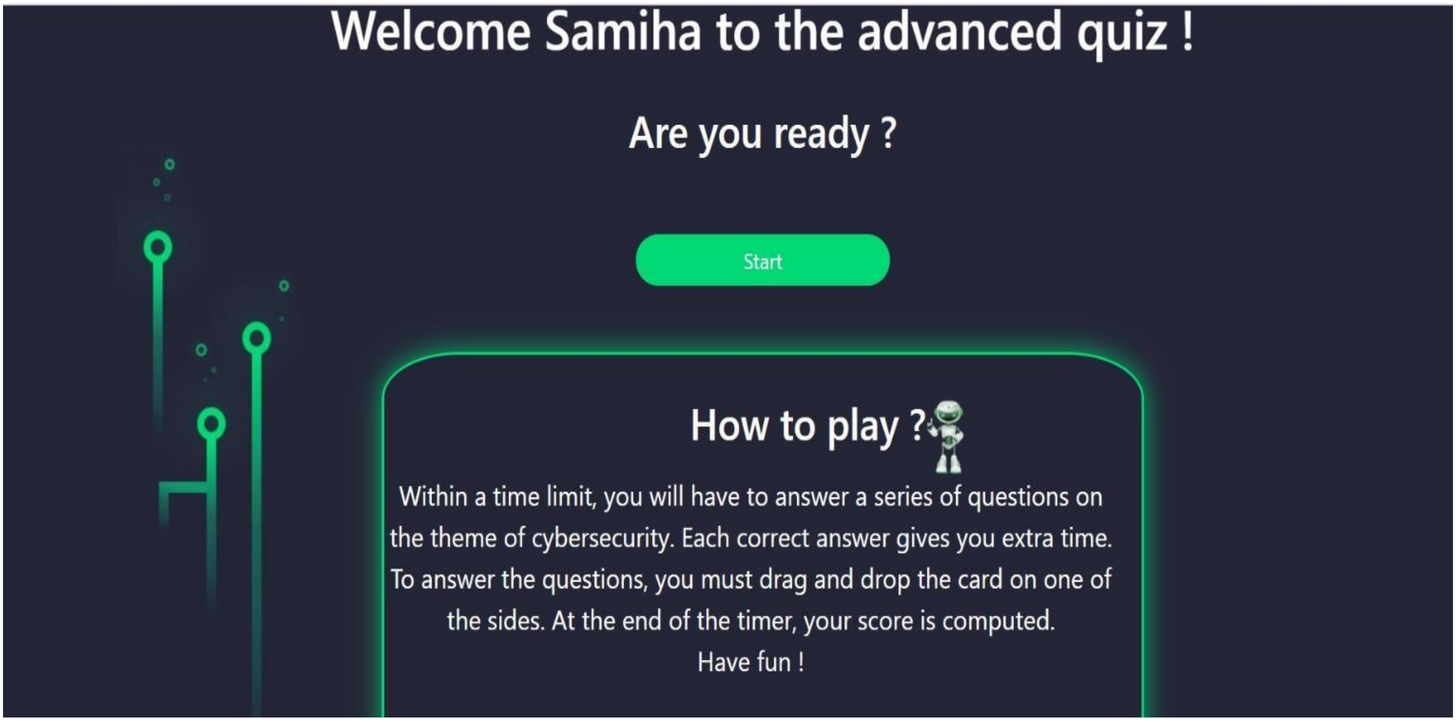
Start

How to play ?

Within a time limit, you will have to answer a series of questions on the theme of cybersecurity. Each correct answer gives you extra time. To answer the questions, you must drag and drop the card on one of the sides. At the end of the timer, your score is computed.

Have fun !

Screenshot 6.7: Beginner level Leaderboard



Welcome Samiha to the advanced quiz !

Are you ready ?

Start

How to play ?

Within a time limit, you will have to answer a series of questions on the theme of cybersecurity. Each correct answer gives you extra time. To answer the questions, you must drag and drop the card on one of the sides. At the end of the timer, your score is computed.

Have fun !

Screenshot 6.8 : Advanced level Quiz

7-CONCLUSION

The Cyberquest : The Security Challenge project successfully demonstrates an engaging and educational approach to learning cybersecurity concepts through a gamified quiz platform. Built using a modern full-stack architecture—ReactJS for the frontend and Flask for the backend it allows users to interact with real-time questions, timers, and score tracking in a seamless and responsive environment.With Docker-based deployment, the project ensures easy scalability and cross-platform compatibility, making it suitable for educational use, workshops, and training scenarios. Its RESTful API design allows future extensibility, such as user authentication, advanced question sets, and persistent databases.Overall, this project achieves its objective of making cybersecurity learning interactive and accessible, and it provides a solid foundation for further development and integration into real-world e-learning platforms.

REFERENCES

[1] S. Garfinkel and G. Spafford, Practical Unix and Internet Security, O'Reilly Media, 2003.

[2] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST Special Publication, 2007.

[3] C. Pfleeger and S. Pfleeger, Security in Computing, 4th ed., Prentice Hall, 2006.

[4] OWASP Foundation, "OWASP Top Ten Web Application Security Risks," [Online]. Available: https://owasp.org/www-project-top-ten/

[5] A. S. Tanenbaum, Computer Networks, 5th ed., Pearson, 2011.

[6] T. Chen et al., "Cybersecurity Game Design: Learning through Fun," IEEE Security & Privacy, vol. 17, no. 5, pp. 54–62, 2019.

[7] R. M. Yampolskiy, "Artificial Intelligence Safety Engineering: Why Machine Ethics is a Wrong Approach," in Philosophy and Theory of Artificial Intelligence, Springer, 2012.

[8] A. Shostack, Threat Modeling: Designing for Security, Wiley, 2014.

[9] A. Kumar, "Web Development using Flask and React," International Journal of Web Engineering, vol. 3, no. 1, pp. 45–50, 2020.

[10] S. Krutz and R. Vines, Cloud Security: A Comprehensive Guide, Wiley, 2010

[11] M. Hafiz, "Security Patterns: Best Practices for Secure Software Development," Software Engineering Institute, Carnegie Mellon, 2013.

[12] Docker Inc., "Docker Documentation," [Online] Available : https://docs.docker.com/

[13] E. Bertino and R. Sandhu, "Database Security—Concepts, Approaches, and Challenges," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 1, pp. 2–19, 2005.

[14] S. Northcutt and J. Shenk, Security Awareness Training for All Users, SANS Institute, 2008.