Cool Cyber Games – Interactive Platform for Teaching Cybersecurity

Requirements Document

Matthew Goembel, Anthony Clayton, Ludendorf Brice, Ben Allerton
Team Members

Sneha Sudhakaran
Faculty Advisor

College of Science and Engineering
Florida Institute of Technology
Melbourne, United States

February 2025

Index

1. Introduction

1.1 Purpose

Cool Cyber Games is an interactive platform designed to teach cybersecurity concepts through gamification. The platform provides hands-on experience, real-world cybersecurity challenges, progress tracking, making cybersecurity education engaging and accessible.

1.2 Document Conventions

This document follows the IEEE 830-1998 Standard for Software Requirements Specifications.

1.3 Intended Audience and Reading Suggestions

This document is intended for:

- Development Team
- Faculty Advisor
- Stakeholders interested in cybersecurity education

1.4 Project Scope

The system will offer:

- Interactive tutorials and quizzes
- Fun games and simplified cybersecurity concepts
- Hands-on activities and real-world cybersecurity challenges and simulations
- Comprehensive tutorials and practical applications
- Progress tracking, certification system, and overall leaderboard
- Accessibility from all OS systems and mobile devices
- Backend integration with a database to store points, track progress, and manage user data
- Secure and fast login system
- Authorization system to maintain a secure server

2. Overall Description

2.1 Product Perspective

Cool Cyber Games is a standalone web-based application that integrates front-end, back-end, database, authentication, and gamification technologies. It is designed for cross-platform compatibility and accessibility.

2.2 Product Functions

- Interactive Tutorials & Quizzes
- Gamified Learning Modules
- Real-world Cybersecurity Challenges
- Progress Tracking & Certification
- Web-based Interface
- User Accounts using Google OAuth 2.0

2.3 User Characteristics

- Beginners of all ages
- Content is catered to adults (18-35)
- No prior cybersecurity knowledge required
- Users seeking hands-on cybersecurity training

2.4 Constraints

- Realistic and engaging cybersecurity scenarios
- Secure authentication system
- Compliance with accessibility standards
- Must be playable on both desktop and mobile web browsers

3. Specific Requirements

3.1 Functional Requirements

3.1.1 User Authentication

- The system shall support OAuth integration for Google authentication.

3.1.2 Interactive Tutorials and Quizzes

- The system shall provide step-by-step guidance on cybersecurity concepts in the tutorials.
- The system shall include multiple-choice, drag-and-drop, and scenario-based questions in quizzes.

3.1.3 Gamified Learning Modules

- The system shall present cybersecurity challenges in a game-like format.
- The system shall mirror real-world cybersecurity threats in the simulations.
- The system shall include levels and increasing difficulty progression.
- The system shall provide hints and guidance for difficult levels.

3.1.4 Progress Tracking and Certifications

- The system shall track user progress and provide certificates upon course completion.
- The system shall maintain a leaderboard to encourage user engagement.

3.1.5 User Dashboard

- The system shall have a dashboard page for the user to view

3.2 Non-functional Requirements

3.2.1 Performance Requirements

- The system shall support at least 100 concurrent users.
- The system shall ensure load times do not exceed 2 seconds per page.
- The system shall minimize memory and processing overhead for smooth gameplay.
- The system shall not exceed 100GB of bandwidth monthly due to free-tier restrictions on Render.

3.2.2 Security Requirements

- The system shall implement HTTPS for secure communication.
- The system shall follow OWASP security guidelines.

3.2.3 Usability Requirements

- The system shall be user-friendly and accessible to non-technical users.
- The system shall comply with ADA accessibility standards.
- The system shall provide an intuitive UI/UX for a smooth gameplay and learning experience.

3.2.4 Scalability Requirements

- The system shall support additional features in the future.
- The system shall allow for modular expansion of game content.
- The system shall have options to increase server bandwidth.
- The system shall have options to increase database storage capacity.

4. Interface Requirements

4.1 User Interfaces

- The system shall ensure the interface is intuitive and visually appealing.
- The system shall provide dark and light mode options for user comfort.
- The system shall provide ADA features such as color-blind assist.

4.2 Software Interfaces

- The system shall implement the front-end using HTML, CSS, JavaScript.
- The system shall integrate a back-end using Node.js, Render, and Express.js.
- The system shall use two MongoDB databases for User/Game storage.
- The system shall use Godot for game development.

4.3 Hardware Interfaces

- The system shall be compatible with standard desktop and mobile browsers.

5. Other Requirements

5.1 Database Requirements

- The system shall use a MongoDB game database to store user progress, scores, and achievements.
- The system shall use a MongoDB user database to store public facing non-sensitive user information such as email, name, and avatar for their account.

5.2 Compliance Requirements

- The system shall comply with the ADA.
- The system shall follow industry standards for cybersecurity education platforms.

5.3 Assumptions and Dependencies

- The system shall assume users have an internet connection.
- The system shall assume users have or can create a Google account.
- The system shall assume third-party libraries remain actively maintained.

6. Appendix

This document is subject to change as development progresses. Future iterations will include additional details on implementation, testing, and deployment strategies.