FAZAIA BILQUIS COLLEGE NUR KHAN BASE RAWALPINDI

Submitted By:

Tasmia Fatima

BSCS-13-F24-49

Maria Atta

BSCS-13-F24-01

Submitted To:

Dr. Inam Ullah Khan

Table of Contents:

Abstract

In the digital age, websites are under constant threat from hackers who attempt to access sensitive information using a variety of techniques. Traditional security measures, such as firewalls, can block attackers but do not provide insight into their methods. The **Sentinel Cyber Defense System** is designed as an advanced security solution that combines a professional website with a **Honeytrap** mechanism. The Honeytrap acts as a decoy, luring suspicious users into a fake environment where all their actions are recorded for analysis. This system provides both protection and intelligence, allowing administrators to study attacker behavior and strengthen security measures proactively.

1. Introduction

- Cybersecurity has become a critical concern for websites and online applications. Conventional methods, such as firewalls and antivirus tools, are reactive—they block attacks but do not capture the details of intrusions.
- The **Sentinel Cyber Defense System** goes beyond these tools by introducing a **Honeytrap mechanism**. A Honeytrap is essentially a fake environment or a decoy designed to attract attackers. When a hacker attempts to breach the system, they are redirected to the Honeytrap, which records their activities without their knowledge.
- This project serves both as a **security solution** and an **educational demonstration**, showing how modern cybersecurity techniques can combine prevention and intelligence-gathering.

2. Problem Statement

Despite advances in cybersecurity, websites remain vulnerable to the following issues:

1. **Clever Attackers:** Hackers often use sophisticated tools to guess passwords, exploit vulnerabilities, or inject malicious code (e.g., SQL Injection).

2. **Invisible Attacks:** Many intrusions go undetected until significant damage occurs.
3. **Lack of Insight:** Traditional systems block attackers but do not analyze their behavior, limiting the ability to anticipate future attacks.

The Sentinel Cyber Defense System addresses these problems by **actively studying suspicious behavior** and protecting real user data through a decoy environment.

3. Objectives

The primary objectives of this project are:

- To create a **secure web system** that can detect and trap suspicious users.
- To **log and analyze hacker activity** in a controlled environment.
- To implement a **risk scoring system** that evaluates login attempts based on behavior.
- To provide a **professional web interface** that simulates a real business environment.
- To demonstrate practical cybersecurity techniques for academic and educational purposes.

4. System Design

4.1 System Architecture

The system is divided into three layers:

1. **Frontend (User Interface):**
    - Designed using HTML, CSS, and Bootstrap.
    - Provides pages for login, admin dashboard, careers, and news.
2. **Backend (Business Logic):**
    - Implemented in PHP.
    - Handles login authentication, risk scoring, and Honeytrap redirection.
3. **Database (Data Storage):**
    - MySQL database stores user credentials, job applications, and action logs.

Flow Diagram:

4.2 Honeytrap Mechanism

The Honeytrap is a **decoy system** designed to trap malicious users. Features include:

- **Fake Admin Dashboard:** Appears identical to the real panel but contains no real data.
- **Action Logger:** Tracks clicks, keystrokes, and navigation patterns.
- **Confusion Module:** Buttons show fake errors or delays to mislead attackers.

- **Live Monitoring:** Real admins can view all activity in real-time and categorize users by risk.

5. Implementation Details

5.1 Login & Risk Scoring

- Users are assigned a **risk score (0–100)** based on login behavior.
- Suspicious patterns (e.g., SQL injection strings, multiple failed attempts) increase the score.
- High-risk users are redirected to the Honeytrap automatically.

5.2 Public Pages

- **Careers Page:** Secure form for job applications.
- **News Page:** Articles on cybersecurity topics (IoT Botnets, phishing) with images.

5.3 Monitoring & Alerts

- Admin dashboard displays:
  - **Green:** Safe users
  - **Red:** Blocked users
  - **Orange:** Users inside Honeytrap

6. Scope and Limitations

- **Smart Login:** Monitors login behavior beyond password checks.
- **Honeytrap:** Captures attacker behavior in a controlled environment.
- **Live Threat Feed:** Real-time visualization of user activity.
- **Public Pages:** Careers and news feed to simulate a professional website.
- **Action Logging:** Every click and keystroke is recorded.

7. Technologies Used

Component	Technology	Purpose
Frontend	HTML, CSS, Bootstrap	Responsive and professional UI

Backend	PHP	Handles logic, login, and Honeytrap operations
Database	MySQL	Stores users, logs, applications
JavaScript	JS	Interactive elements, popups, action tracking

8. Advantages

- Proactively detects and traps malicious users.
- Captures detailed attacker behavior for analysis.
- Provides a professional-looking website to hide security mechanisms.
- Educates about practical cybersecurity implementations.

9. Limitations

- No multi-factor authentication yet.
- Limited analytics and reporting for admins.
- Currently designed for demonstration/educational purposes rather than enterprise deployment.

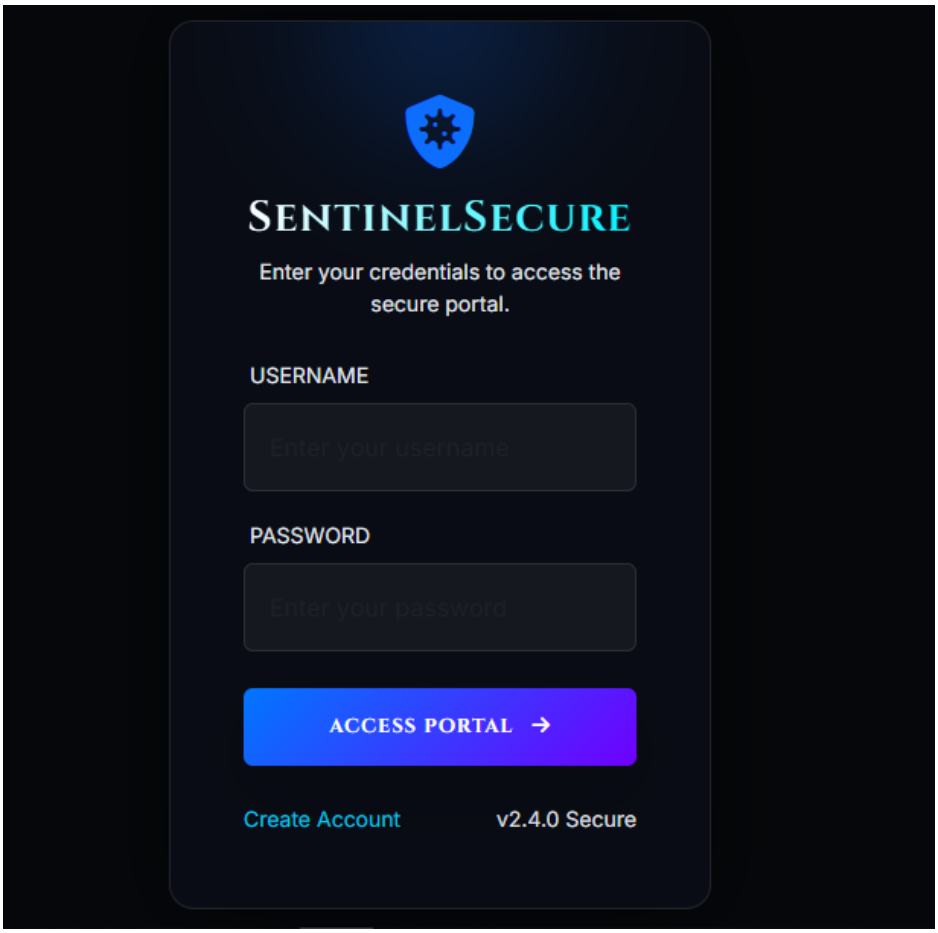
10. Algorithms Used

Mention:

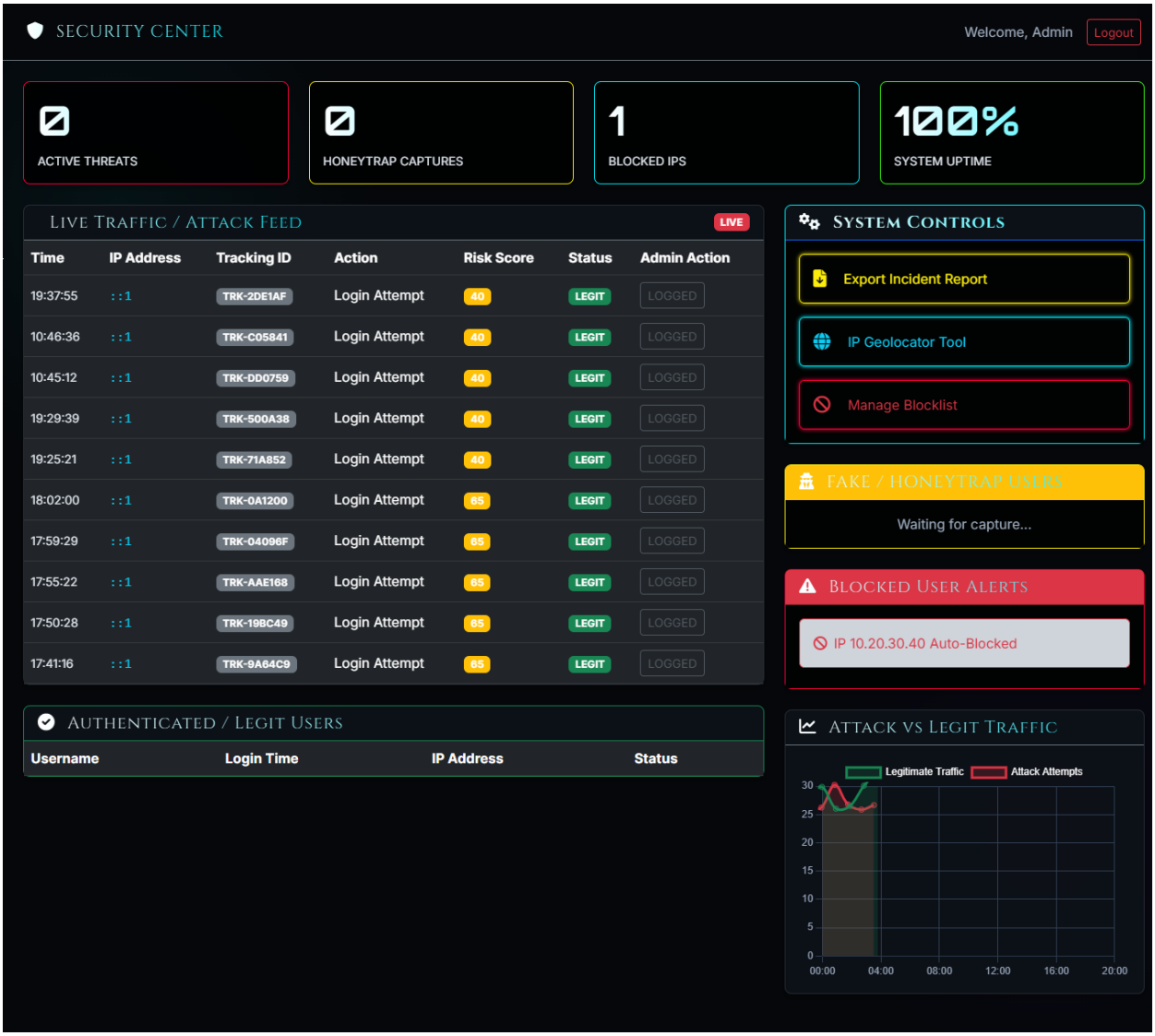
- Risk scoring algorithm (based on login behavior)
- Redirection logic (if-else based on score)
- Logging and monitoring logic

11. Results / Output

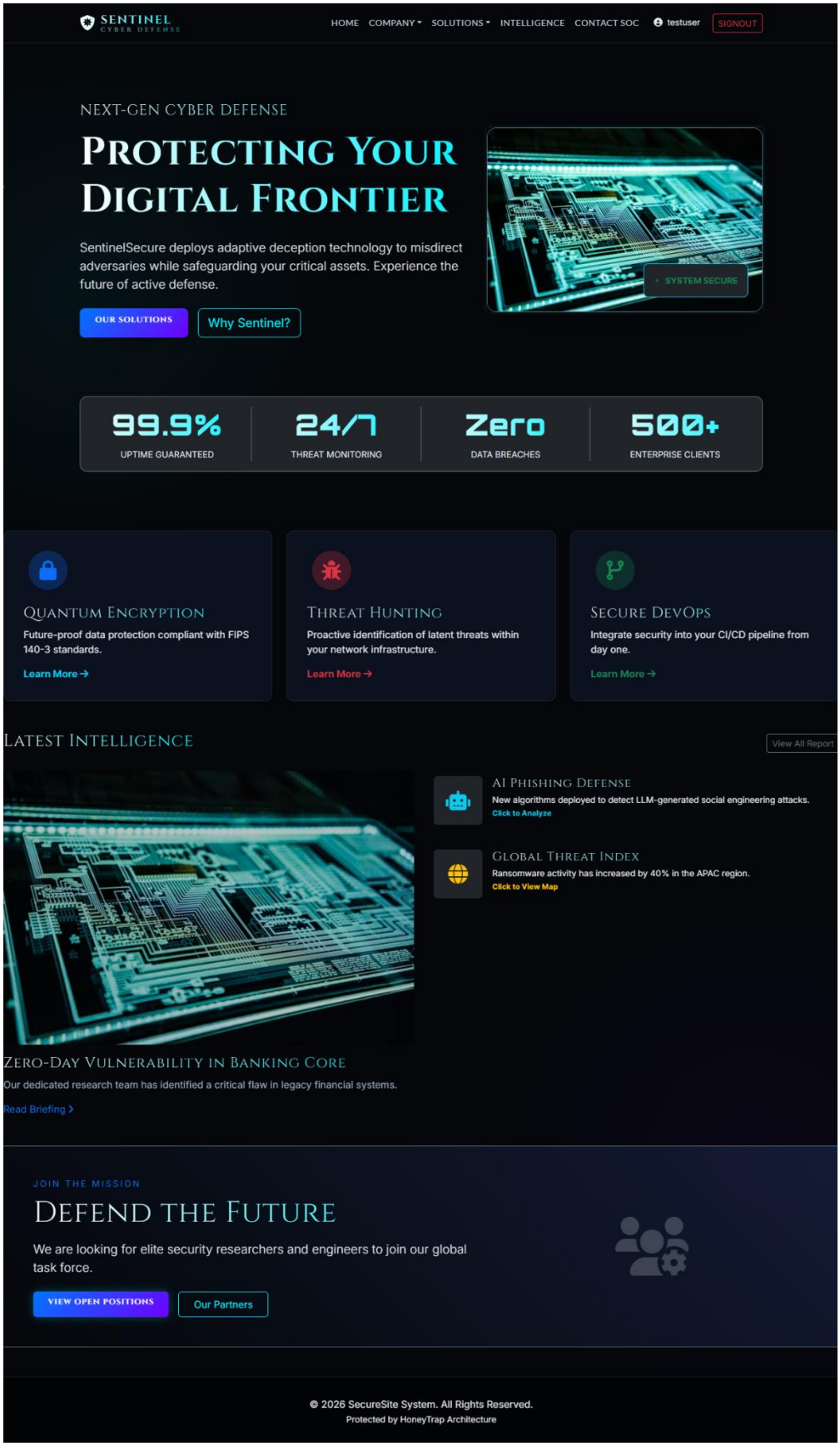
- **Login page**



- **Admin dashboard**



- **Honeytrap interface**


SENTINEL
CYBER DEFENSE
HOME
COMPANY
SOLUTIONS
INTELLIGENCE
CONTACT SOC
testuser
SIGNOUT
NEXT-GEN CYBER DEFENSE
PROTECTING YOUR DIGITAL FRONTIER
SentinelSecure deploys adaptive deception technology to misdirect adversaries while safeguarding your critical assets. Experience the future of active defense.
OUR SOLUTIONS
Why Sentinel?
SYSTEM SECURE
99.9%
UPTIME GUARANTEED
24/7
THREAT MONITORING
Zero
DATA BREACHES
500+
ENTERPRISE CLIENTS
QUANTUM ENCRYPTION
Future-proof data protection compliant with FIPS 140-3 standards.
Learn More →
THREAT HUNTING
Proactive identification of latent threats within your network infrastructure.
Learn More →
SECURE DEVOPS
Integrate security into your CI/CD pipeline from day one.
Learn More →
LATEST INTELLIGENCE
View All Report
AI PHISHING DEFENSE
New algorithms deployed to detect LLM-generated social engineering attacks.
Click to Analyze
GLOBAL THREAT INDEX
Ransomware activity has increased by 40% in the APAC region.
Click to View Map
ZERO-DAY VULNERABILITY IN BANKING CORE
Our dedicated research team has identified a critical flaw in legacy financial systems.
Read Briefing ›
JOIN THE MISSION
DEFEND THE FUTURE
We are looking for elite security researchers and engineers to join our global task force.
VIEW OPEN POSITIONS
Our Partners
© 2026 SecureSite System. All Rights Reserved.
Protected by HoneyTrap Architecture

13. Testing

TEST CASE	INPUT	EXPECTED OUTPUT	ACTUAL OUTPUT	STATUS
NORMAL LOGIN	Valid credentials	Access granted	✅	Pass
SQL INJECTION	' OR '1'='1	Redirect to Honeytrap	✅	Pass
MULTIPLE FAILED ATTEMPTS	Wrong password x5	Account locked / redirected	✅	Pass
ADMIN LOGIN	Admin credentials	Access to real dashboard	✅	Pass

14. Future Enhancements

- Implement multi-factor authentication for admins.
- Enhance analytics dashboard with charts and alerts.
- Make system mobile-friendly.
- Integrate with external security monitoring tools.
- Automate risk assessment using AI algorithms.

11. Conclusion

The **Sentinel Cyber Defense System** is an advanced cybersecurity solution combining a professional website with a hidden Honeytrap. It allows administrators to **proactively protect data**, monitor suspicious activity, and study attacker behavior in a safe environment. This project demonstrates practical cybersecurity techniques, providing both protection and educational value.

12. References

1. PHP Documentation – https://www.php.net/
2. MySQL Documentation – https://dev.mysql.com/doc/
3. HTML & CSS Reference – https://developer.mozilla.org/
4. Cybersecurity Articles: IoT Botnets, SQL Injection Techniques