CYBER-WISE

PROJECT SYNOPSIS

OF MINOR PROJECT

BACHELOR OF TECHNOLOGY

Computer Science & Engineering

SUBMITTED BY

Aditya Sankhyan	Shashank Sharma	Armaandeep Singh
CRN:2115004	CRN:2115165	CRN:2115021
URN:2104058	URN:2104187	URN:2104074

January 2025

GURU NANAK DEV ENGINEERING COLLEGE,

LUDHIANA

INDEX

INTRODUCTION

In today's digital age, small businesses are increasingly vulnerable to cyber threats that can compromise sensitive data, damage their reputation, and result in financial losses. Many small business owners lack the technical expertise and resources to implement robust cybersecurity measures, leaving their websites exposed to risks such as data breaches, hacking, and fraud. As cyberattacks become more sophisticated, the need for accessible, affordable, and effective security solutions has never been more critical.

Cyberwise aims to address this gap by offering a comprehensive platform that combines essential cybersecurity features with user-friendly educational resources. This platform is designed to help small business owners secure their websites, protect sensitive data, and reduce the risk of cyberattacks, all while providing valuable cybersecurity education. By offering simple, scalable security tools and educational materials, Cyberwise empowers businesses to take control of their online security and build trust with their customers.

The project focuses on three core objectives: developing and implementing fundamental security features for websites, creating a modular and scalable cybersecurity framework, and offering an accessible web-based scanner to identify vulnerabilities. Ultimately, Cyberwise strives to make cybersecurity both approachable and actionable for small business owners, ensuring they can operate confidently in an increasingly interconnected digital world.

RATIONALE

As cyber threats continue to rise, small businesses are particularly vulnerable due to limited resources and expertise in cybersecurity. Protecting online presence and sensitive data has become essential, not optional. Cyberwise addresses this gap by providing affordable, user-friendly security tools to safeguard businesses against common threats and secure sensitive information.

- Prevention of Data Breaches:

Data breaches can cause significant financial, reputational, and legal damage. Cyberwise helps businesses prevent unauthorized access, data loss, and cyberattacks, minimizing these risks.

- Protection of Sensitive Information:

Small businesses store valuable data such as customer details and intellectual property. Cyberwise ensures this information remains confidential and secure.

- Cost-Effective and Accessible Security:

Many small businesses cannot afford complex cybersecurity solutions. Cyberwise offers a cost-effective, easy-to-integrate platform, making security accessible to all businesses.

- Empowering Small Businesses:

Cyberwise also serves as an educational tool, empowering business owners to understand and implement cybersecurity best practices, building confidence in their digital operations.

Objectives

1. To Develop and Implement Core Security Modules for Foundational Functionality .
2. To Integrate and Thoroughly Test a Modular and Scalable Cybersecurity Framework.
3. To develop an accessible, user-friendly Web Cyber Scanner to help small owners safeguard sensitive data and build customer trust.

Literature Review

The literature review focuses on analyzing existing research, frameworks, and tools in the field of cybersecurity to inform the development of the Cyberwise AB Website. Key findings include:

Cybersecurity Challenges for Small Businesses:

Studies highlight that small businesses often lack the resources and expertise to implement effective cybersecurity measures, making them prime targets for cyber threats.

Common threats include phishing, ransomware, and data breaches, which emphasize the need for accessible and affordable solutions.

Existing Tools and Frameworks:

Tools such as web vulnerability scanners (e.g., OWASP ZAP, Nessus) provide robust vulnerability assessments but may be too complex or costly for small business owners.

Scalable frameworks like NIST Cybersecurity Framework and ISO/IEC 27001 are effective for larger organizations but require simplification for smaller entities.

User-Centric Design in Cybersecurity Solutions:

Research underscores the importance of user-friendly interfaces and educational resources to empower non-technical users in implementing cybersecurity practices.

Gamification and interactive tutorials have proven effective in enhancing engagement and knowledge retention.

Feasibility Study

1. Knowledge and Expertise

To successfully develop and launch Cyberwise, a combination of expertise in the following areas is required:

- Cybersecurity: Ensuring robust protection against a wide range of cyber threats.
- Web Development: Building a scalable, reliable platform for users to access and implement security measures.
- UX Design: Focusing on delivering a seamless, user-friendly experience for businesses and site owners.

External Consultation: Depending on the complexity of specific security tasks, external cybersecurity consultation may be necessary to enhance protection measures.

2. Clear Objectives

The primary objectives for the Cyberwise platform are:

- Core Security Features: Develop and implement essential security tools to protect websites from common threats, such as malware, unauthorized access, and data breaches.
- Scalable Security Framework: Build a modular security framework that is adaptable and can evolve with new and emerging cyber threats.
- Web Vulnerability Scanner: Create an easy-to-use, accessible web scanner that businesses can use to identify vulnerabilities in their websites.

3. Integration with Existing Infrastructure

- Compatibility: Cyberwise must integrate seamlessly with popular CMS platforms like WordPress, Shopify, and other custom websites. It is essential to ensure that integration does not disrupt the functionality or user experience of existing systems.

4. Resource Allocation

- Hardware and Software Resources:
    - Development will require reliable cloud infrastructure to support scalability.
    - Cybersecurity tools and server management resources will be necessary for maintenance and operational efficiency.

METHODOLOGY

1. Project Planning and Research

- Objectives: Define project objectives targeting small business owners.
- Research: Conduct research on cybersecurity needs and analyze existing solutions to identify gaps.

2. Requirement Analysis and System Design

- User Requirements: Gather user requirements and ensure alignment with small business needs.
- Compliance: Ensure compliance with security standards and regulations.
- System Design: Design scalable system architecture, including core security modules and web scanner integration.

3. Technology and Content Development

- Tech Stack: Select tech stack (React.js, Python, Node.js, MongoDB/MySQL).
- Educational Content: Create interactive educational content for cybersecurity awareness.

4. Implementation and Integration

- Security Modules: Develop and integrate core security modules.
- Web Scanner: Integrate the web scanner for vulnerability detection.
- Platform Components: Develop other platform components for a cohesive user experience.

5. Testing and Deployment

- Testing: Conduct unit, integration, usability, and security testing.
- Deployment: Deploy on a secure cloud environment with user support and documentation

Facilities Required

1. Software Requirements

- Frontend Development:
    - Framework: Next.js
    - UI Libraries:
        - NextUI
        - Tailwind CSS
- Backend and Database:
    - Firebase:
        - Firestore
        - Firebase Authentication
        - Firebase Hosting
- Security Features:
    - SSL/TLS
    - JWT
    - Data validation and sanitization
- Testing and Debugging:
    - OWASP ZAP
    - Browser developer tools
- Version Control:
    - Git and GitHub

2. Hardware Requirements

- Development Machines:
    - 8GB RAM, i5/i7 processor
- Devices for Testing:
    - Smartphones and tablets

Expected Outcomes

1. Enhanced Cybersecurity for Small Businesses

   Access to robust security tools to safeguard sensitive data and reduce vulnerability to cyber threats.

2. Increased Cybersecurity Awareness

   Educational resources to improve understanding of cybersecurity best practices.

3. User-Friendly Vulnerability Assessment Tool

   Simple, intuitive web cyber scanner to identify and address website vulnerabilities.

4. Scalable and Modular Framework

   Flexible architecture that adapts to evolving security challenges and future enhancements.

5. Customer Trust and Confidence

   Implementing security measures helps build trust and loyalty among customers.

References

- WebSecInsights, "The Role of Encryption in Web Security: Best Practices and Techniques,"WebSecInsights Guides, [Online]. Available: https://www.websecinsights.com/guides/role-encryption-web-security-best/. [Accessed: Jan. 28, 2025].
- Crawlbase, "Web Crawling: Techniques and Frameworks for Collecting Web Data," Crawlbase Blog, [Online]. Available: https://crawlbase.com/blog/web-crawling-techniques-and-frameworks/. [Accessed: Jan. 28, 2025].
- W. Zaatour, "Next.js 14 with Firebase: A Practical Walkthrough," DEV Community, [Online]. Available: https://dev.to/wadizaatour/integrating-nextjs-with-firebase-a-practical-walkthrough-4j30 . [Accessed: Jan. 28, 2025].
- KnowledgeHut, "Data Encryption: Types, Algorithms, Methods, and Techniques," KnowledgeHut Blog, [Online]. Available: https://www.knowledgehut.com/blog/security/data-encryption. [Accessed: Jan. 28, 2025].