Security Web Application For Nexus Shield Solutions Pvt Ltd Pandharpur

Amey Bhatlavande[1], Suraj Bhandare[2], Suraj Adsul[3], Abhijit Gidde[4], Sumit Das[5]
[1, 2, 3, 4, 5] Dept of Information Technology
[1, 2, 3, 4, 5] SVERI's College of Engineering(Poly.),Pandharpur, Maharashtra, India

Abstract- *"WebSecureity," the Security Web Application, is a thorough cybersecurity solution designed to provide friendly, secure products including vulnerability assessments, penetration testing, safe web development, and ethical hacking instruction. The front end of the platform was constructed using HTML, CSS, JavaScript; PHP handled backend logic; and MySQL was used for data management. It has admin control panels, dynamic service request tools, WhatsApp based communication, and protection against well known threats including SQL injection and XSS. The incentive, studies, execution, and assessment of the system are given in this article.*

Keywords- Cybersecurity, Vulnerability Assessment, Penetration Testing, Ethical Hacking, Web Application Security, Network Security, Mobile Application Security, SQL Injection, XSS Protection, Secure Software Development, Web Secureity, Cybersecurity Training.

I. INTRODUCTION

In today's digital age where online services and web applications exist in everyone's space, the subject of cybersecurity is paramount. Everyone, whether an individual, organization, or institution, is increasingly facing larger threats via malware, phishing, data breaching, and unauthorized access. To address these issues, the Security Web Application "WebSecureity" was designed and built to serve as a digital platform that includes security service addressability, in conjunction with educational modules.

The system provides addressability to pertinent cybersecurity services such as VAPT for Web Application and Networking of the system, and serves as a learning platform with approaches in ethical hacking. The architecture framework integrates the Design Principles of Secure by Design, implemented with PHP, MySQL, JavaScript and library references, has a dynamic admin panel for the authentication process, an active form validation, and encrypted and stored essences with client-server encrypted communications.

The application is also expandable and evolves with current trends, maintains regard within its parameters for other forms of intrusion detection such as the incorporation of an advanced security tool kit, real time alerts and computable elements for payment as issues arise or emerge. With the growing regard for cyber security awareness for small organizations, businesses and educational institutes, Web Secureity represents an easy access point designed for those with limited capacity.

II. IDENTIFY, RESEARCH AND COLLECT IDEA

We began this journey by identifying the divide between the theoretical cybersecurity education and the practice.

After our research of learning platforms (EC-Council, Udemy, Offensive Security, among others), we noticed most provided a structured educational path toward certification, but did not provide any practical service/delivery model for learning.

During this process, we conducted interviews with students and small-business owners to pinpoint pain points associated with getting affordable and realistic cybersecurity services. Our hope was to conceptualize WebSecureity as two-sided: a service to deliver security and a fair payment model to allow users to also build a set of ethical hacking skills. We also researched different types of open-source tools, and took the time to research and familiarize ourselves with secure development practices.

As part of our user research, we investigated different vulnerabilities including Cross-Site Request Forgery (CSRF), local file inclusion (LFI), and command injection. We used DVWA and other security tools (OWASP ZAP and Burp Suite) to simulate specific attack patterns, and understand different mitigation strategies.

III. WRITE DOWN YOUR STUDIES AND FINDINGS

During the development of our Security Web Application, WebSecureity, we took a thoughtful, research-based approach to turn our initial concept into a fully functional and secure platform. We blended theoretical insights from academic sources with practical knowledge gained through hands-on experimentation, tool testing, and valuable user feedback.

A. Research-Driven Development Process

We delved into various secure coding principles to tackle common web threats, including:

- SQL Injection (SQLi)
- Cross-site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Remote Code Execution (RCE)

Our architectural and coding choices were heavily influenced by OWASP's Top 10 vulnerabilities. To simulate attacks and test our system's defenses, we utilized open-source platforms like DVWA (Damn Vulnerable Web Application) and tools such as Burp Suite and OWASP ZAP.

B. System Design and Architecture

We structured the system into several interconnected modules:

- Frontend (UI/UX): Built with HTML, CSS, and JavaScript, incorporating AJAX for a smooth user experience.
- Backend: PHP was used to manage form submissions, login processes, database operations, and validations.
- Database: MySQL served as the backbone for storing service requests, admin credentials, and client interactions.
- Security Layer: We implemented input sanitization, prepared statements, and session handling to ensure secure data transactions.

The database schema included:

- users (for admin credentials)
- requests (to store service request data)
- messages (optional chat/query storage for future real-time communication)

C. Key Functional Modules Implemented

Service Request Form: This feature allowed users to submit their cybersecurity needs, with validation occurring both client-side (JavaScript) and server-side (PHP), and data was securely stored in MySQL using prepared statements.

Admin Panel: A secure interface with login functionality, designed for reviewing submitted requests and managing client communications.

WhatsApp Integration: We added "Click-to-chat" buttons on the Courses and Services pages, enabling instant user support.

IV. GET PEER REVIEWED

After developing the WebSecureity platform and drafting this research paper, we entered a crucial phase of peer review to assess the work's effectiveness, accuracy, and overall presentation. We reached out for feedback from various sources to ensure a comprehensive evaluation.

Key reviewers included:

Prof. Amey S. Bhatlavande, our project guide, who offered valuable insights on the technical aspects, security measures, and architectural design.

Faculty members from the Information Technology department at SVERI's COE (Polytechnic), who examined the project from both an academic and documentation standpoint.
Peers and classmates, who provided feedback on usability, navigation, and the overall user interface experience.

We organized the feedback into several categories:

Technical Review: This focused on secure coding practices, database design, and the implementation of security controls recommended by OWASP.

Usability Review: This looked at UI responsiveness, layout clarity, form functionality, and the flow of the admin panel.
Security Review: This evaluated backend validation, protection against SQL injection, session management, and potential XSS vulnerabilities.

Documentation Review: This ensured that the paper followed IJSART formatting guidelines, included enough detail, and clearly outlined the project's lifecycle.

V. IMPROVEMENT AS PER REVIEWER COMMENTS

The reviewers highlighted secure coding practices and backend optimization as key.

To this effect:

SQL queries were rewritten to utilize parameterized statements, reducing the risk of SQL injection.

Input validation and sanitization were implemented at all data entry points to avoid common weaknesses like Cross-Site Scripting (XSS).

Session management was enhanced by incorporating session expiration controls and secure cookies, enhancing access control in the admin panel.

UI/UX Improvements

Classmates' and instructors' usability feedback assisted in improving the user experience of the platform:The web application's navigation flow was restructured to become more intuitive for users.The layout of the form on the service request and login pages was reconfigured for improved responsiveness and visual readability.Mobile responsiveness was improved to provide accessibility on devices.

Security Enhancements

According to simulated penetration testing and reviewer feedback:
The system was secured from XSS and injection-based attacks through updated backend filters and encoding systems.

Access to admin panel was protected by enhanced authentication checks and login attempt tracking.

D. Documentation and Format Improvement

In accordance with academic publishing standards:

The entire paper followed IJSART guidelines, proper section titles, figure captioning, and referencing.Explanations for technical diagrams like DFDs, UML diagrams, and flowcharts were elaborated for the sake of clarity.

VI. CONCLUSION

The WebSecureity platform was created to meet the increasing demand for secure, accessible, and user-friendly cybersecurity services. By integrating cutting-edge technologies like PHP, MySQL, and front-end technologies like HTML, CSS, and JavaScript, the system effectively offers services like Vulnerability Assessment and Penetration Testing (VAPT), secure web and mobile application development, and ethical hacking training.

The project fills crucial gaps realized in current systems—e.g., the absence of real-time user engagement, dynamic request management, and personalized communication—by including features such as WhatsApp integration, an admin dashboard, and secure request storage. These implementations lead to a more efficient and client-focused experience.

Security testing confirmed the system's immunity to prevalent attacks such as SQL injection and XSS attacks, assuring the strength of its backend framework. In addition, modifications implemented upon peer and faculty feedback improved the platform's technical merit, usability, and documentation, aligning the work with academic publication standards.

In summary, WebSecureity is a secure and scalable cybersecurity solution that not only protects digital assets but also enables individuals and organizations to defend against changing cyber threats with the knowledge and tools to do so. The project demonstrates a high level of dedication to digital safety, innovation, and education in the field of cybersecurity.

VII. ACKNOWLEDGMENT

We would like to extend our sincere thanks to Prof. Amey S. Bhatlavande, our venerable guide, for his unwavering support, technical expertise, and encouragement during the process of developing the WebSecureity project. His insightful suggestions on cybersecurity and software architecture played a crucial role in molding this research and making our concepts a reality.

We are equally thankful to the Department of Information Technology at SVERI’s College of Engineering (Polytechnic), Pandharpur, for providing us with the resources and academic environment necessary to complete this project successfully.

Our sincere thanks to Mrs. R. K. Malgonde (HOD) and Dr. Nitin D. Misal (Principal) for their constant motivation and for creating a platform that nurtures innovation and practical learning.

We also wish to extend our gratitude to Prof. Prashant S. Bhandare for showing us LaTeX and assisting us in organizing this paper to academic standards.

A special note of thanks to our peers and classmates for their constructive criticism during the testing and review process, and to our friends and families for their constant emotional and technical support throughout the entire course of this project.

Without the combined efforts and contributions of all those who helped, this job would not have been accomplished. We are appreciative beyond measure.

REFERENCES

[1] Singh, R., Verma, P., and Kumar, A. (2020). Web Application Security: Challenges and Solutions. International Journal of Computer Applications, 176(22), 15–20.

[2] Kumar, V., and Sharma, A. (2019). A Survey on Network Security Techniques and Challenges in Modern Cybersecurity. Journal of Network Security, 5(3), 10–17.

[3] Patel, M., Joshi, R., and Desai, A. (2021). Security Threats in Mobile Healthcare Applications: A Review. International Journal of Cybersecurity, 7(1), 25–31.

[4] Jones, D., and Clark, T. (2022). Red Teaming in Healthcare Organizations: A Cybersecurity Strategy. Cyber Defense Review, 6(4), 50–58.

[5] Cybersecurity Ventures. (2021). The 2021 Official Cybersecurity Jobs Report. [Online]. Available: https://cybersecurityventures.com/jobs-report/

[6] Zhao, Y., Chen, L., and Wei, H. (2020). Secure Software Development in Healthcare Systems: Integrating Security into the SDLC. Journal of Information Security and Applications, 54, 102536