Sasmita.M, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Design And Development Of An Owasp Immersive Web Security Lab

Sasmita.M [1] , Sangeetha.V [2] , Dr. Kamalakkannan S [3]

[1,2] UG Students, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Pallavaram, Chennai-600177, Tamil Nadu, India

[3] Professor and programme co-ordinator, Vels Institute of Science, Technology And Advanced Studies (VISTAS), Pallavaram, Chennai-600177, Tamil Nadu, India.

Abstract- With the rapid growth of web applications, security vulnerabilities have become a major concern in modern systems. Many applications remain vulnerable due to improper input validation and insecure coding practices. This project presents an OWASP Immersive Web Security Lab designed to provide hands-on learning of common web vulnerabilities such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Command Injection, File Upload Vulnerabilities, and Path Traversal. The system uses a controlled environment where users can perform attacks and observe system behavior in real time. The platform is developed using web technologies and Docker-based containerization to ensure safe and isolated lab environments. It also includes quizzes and automated verification to evaluate user performance. The results show that the system improves understanding of web security concepts and helps users learn secure coding practices effectively. This project serves as a practical educational tool and a foundation for advanced cybersecurity training systems.

Keywords— Web Security, OWASP Top 10, SQL Injection, Cross-Site Scripting, File Upload Vulnerability, Penetration Testing.

I. INTRODUCTION

Web applications are widely used in various domains such as finance, healthcare, and education. However, they are highly vulnerable to cyberattacks due to insecure development practices. Common vulnerabilities include SQL Injection, Cross-Site Scripting (XSS), and file upload flaws, which can lead to data breaches and system compromise.

Traditional learning methods focus mainly on theory and lack practical exposure. Therefore, there is a need for a system that provides hands-on experience in identifying and exploiting vulnerabilities.

This project introduces an OWASP-based Web Security Lab that enables users to learn and practice security concepts in a controlled environment.

II. LITERATURE SURVEY

Research in web security highlights the importance of identifying and preventing common vulnerabilities. OWASP Top 10 provides a standard list of critical risks in web applications.

Studies on SQL Injection and XSS demonstrate how improper input validation leads to security breaches. Platforms like PortSwigger Web Security Academy provide practical examples for learning vulnerability exploitation.

However, many existing systems require complex setup and lack integrated assessment features. This project addresses these limitations by providing a simple and interactive learning platform.

III. PROBLEM DEFINITION

Web applications face several security challenges, including:

© 2026 Sasmita.M This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

- Lack of proper input validation
- Insecure file handling mechanisms
- Difficulty in understanding vulnerabilities
- Limited practical learning environments
- Complex setup of existing tools

These issues make it difficult for beginners to learn and apply web security concepts effectively.

IV. PROPOSED SYSTEM

The proposed system is a Web Security Training Platform designed to provide hands-on experience in vulnerability exploitation.

The system performs the following functions:

- Provides modules for SQL Injection, XSS, Command Injection, File Upload, and Path Traversal
- Deploys isolated lab environments using Docker
- Allows users to perform attacks safely
- Includes quizzes and automated verification
- Tracks user progress and performance

The platform ensures a structured and user-friendly learning experience.

V. RESULTS AND DISCUSSION

The system was tested with different vulnerability scenarios.

- Users successfully performed SQL Injection and retrieved database data
- XSS attacks executed scripts in browser environments
- File upload vulnerabilities allowed execution of malicious files
- Path traversal attacks enabled access to restricted files

The results show that the platform effectively demonstrates real-world attack scenarios and improves user understanding of web security concepts.

VI. CONCLUSION

This project presents an OWASP Immersive Web Security Lab that provides a practical approach to learning web vulnerabilities. The system combines theoretical knowledge with hands-on labs, improving the learning experience.

It is simple, efficient, and suitable for students and developers. The platform highlights the importance of secure coding practices and vulnerability testing in modern web applications.

REFERENCES

1. OWASP Foundation, OWASP Top 10 Web Application Security Risks
2. D. Stuttard and M. Pinto, The Web Application Hacker's Handbook
3. G. Weidman, Penetration Testing: A Hands-On Introduction to Hacking
4. PortSwigger, Web Security Academy