Website Security Assessment Report

Demo Web Application (Lab Environment)

Prepared by: RedLayer Security

Executive Summary

A security assessment was conducted on an intentionally vulnerable demo web application to identify common security weaknesses. The purpose of this assessment is to demonstrate the testing methodology, reporting style, and risk analysis approach used during real-world engagements.

Scope of Testing

• Black-box testing approach
• Web application assessment
• OWASP Top 10 based testing
• Denial-of-Service and social engineering excluded

Tools Used

• OWASP ZAP
• Burp Suite Community Edition
• Nmap
• Manual testing techniques

Findings Summary

ID	Vulnerability	Risk Level	Status
01	SQL Injection	High	Open
02	Cross-Site Scripting (XSS)	Medium	Open
03	Missing Security Headers	Low	Open

Detailed Findings

1. SQL Injection

Risk: High
Description: Improper input validation allows manipulation of backend SQL queries.
Impact: Unauthorized access to sensitive data.
Recommendation: Use parameterized queries and strict input validation.

2. Cross-Site Scripting (XSS)

Risk: Medium
Description: User-supplied input is reflected without proper encoding.
Impact: Session hijacking and client-side attacks.
Recommendation: Implement output encoding and content security policies.

3. Missing Security Headers

Risk: Low
Description: Important HTTP security headers are not configured.
Impact: Increased exposure to browser-based attacks.
Recommendation: Enable headers such as X-Frame-Options and Content-Security-Policy.

Conclusion

The assessment identified multiple vulnerabilities that should be addressed to improve the overall security posture of the application. A follow-up assessment is recommended after remediation to validate fixes.