Web Application Penetration Test Report

Target: Deliberately Vulnerable Web Application

Client: Internal Portfolio Project

Tester: Edmond Degand

Date: February 1-3, 2025

Scope: Web Application at http://192.168.1.100

1. Executive Summary

The objective of this penetration test was to assess the security posture of a deliberately vulnerable web application, simulating an unauthorized attacker attempting to gain access, extract sensitive data, and exploit system weaknesses.

The assessment identified several critical and high-severity vulnerabilities, including:
- SQL Injection allowing complete authentication bypass and database dumping.
- Directory Listing exposing backup files.
- Remote Code Execution through an outdated file upload feature.

Immediate remediation is strongly recommended to mitigate these risks.

Severity Summary

Severity	Vulnerabilities Identified	Count
Critical	SQL Injection, Remote Code Execution	2
High	Directory Listing, Exposed Admin Panel	2
Medium	Missing Security Headers, Insecure Cookies	2
Low	Information Disclosure in Server Banners	1

2. Scope of Engagement

In-Scope Asset: Web application running at http://192.168.1.100
Out of Scope: Internal network devices, social engineering, physical security assessments
Testing Period: February 1, 2025 - February 3, 2025

3. Methodology

This assessment followed the OWASP Testing Guide, with phases:
- Reconnaissance: Identified open ports, exposed directories, and technologies.
- Scanning & Enumeration: Mapped web pages, forms, and endpoints.
- Vulnerability Testing: Tested for SQL Injection, XSS, and insecure file upload.
- Exploitation: Confirmed and exploited vulnerabilities.
- Reporting: Documented findings, evidence, and recommendations.

Web Application Penetration Test Report

4. Findings

Finding: SQL Injection in Login Form

Description: Bypassed authentication, full database dump.
Recommendation: Use parameterized queries, input validation, WAF.

Finding: Remote Code Execution via File Upload

Description: Uploaded PHP shell, remote command execution.
Recommendation: Restrict file types, disable script execution in upload directory.

Finding: Directory Listing Enabled

Description: Exposed sensitive backups in /backup/.
Recommendation: Disable directory listing, relocate sensitive backups.

Finding: Exposed Admin Panel

Description: Unauthenticated access to admin portal.
Recommendation: Restrict access, enable MFA.

Finding: Missing Security Headers

Description: Increased risk of XSS, clickjacking.
Recommendation: Configure secure headers (CSP, HSTS, X-Frame-Options).

Finding: Insecure Cookies

Description: No HttpOnly or Secure flags on cookies.
Recommendation: Apply secure cookie attributes (HttpOnly, Secure, SameSite).

5. Tools Used

- Nmap: Port and service discovery
- Dirbuster: Directory brute forcing
- SQLmap: Automated SQL Injection testing
- Burp Suite: Manual web app testing
- Metasploit: Exploitation framework
- Nikto: Basic web scanner

6. Recommendations Summary

- Apply input sanitization and parameterized queries to prevent SQL Injection.
- Disable directory listing and relocate backups outside the web root.
- Secure file uploads, restrict file types, and disable script execution.
- Apply HTTP security headers (CSP, HSTS).
- Restrict access to admin interfaces and enforce MFA.

- Regularly conduct security reviews.

7. Conclusion

This penetration test identified significant vulnerabilities that could lead to unauthorized access, data breaches, and full system compromise. Immediate remediation and ongoing secure development practices are recommended.

8. Author

Tester: Edmond Degand
LinkedIn: https://linkedin.com/in/edmonddegand
Email: edmonddeg@gmail.com