Web Application Penetration Testing Report

Automated Vulnerability Assessment

Target : http://127.0.0.1/DVWA/

Assessment Date : 17-07-2026

Assessment Type : Black Box Web Application Testing

This report contains the findings identified during
the automated penetration testing assessment.

Web Application Penetration Test Report

Target : http://127.0.0.1/DVWA/

Assessment Date : 17-07-2026 13:13

Executive Summary

Total Findings : 6

Critical : 2

High : 4

Medium : 0

Low : 0

Findings

SQL Injection

Severity : HIGH

CVSS : 9.8

CWE : CWE-89

OWASP : A03:2021 Injection

Parameter : Form Input

Payload : "

Refleted XSS

Severity : HIGH

CVSS : 6.1

CWE : CWE-79

OWASP : A03:2021 - Injection

Parameter : name

Payload : <script>alert(1)</script>

Evidence : Payload reflected in response.

Impact : No impact information available.

Recommendation : Follow secure coding and OWASP best practices.

Reference : N/A

Refleted XSS

Severity : HIGH

CVSS : 6.1

CWE : CWE-79

OWASP : A03:2021 - Injection

Parameter : txtName

Payload : <script>alert(1)</script>

Evidence : Payload reflected in response.

Impact : No impact information available.

Recommendation : Follow secure coding and OWASP best practices.

Reference : N/A

Command Injection

Severity : CRITICAL

CVSS : 9.8

CWE : CWE-78

OWASP : A03:2021 - Injection

Parameter : ip

Payload : ; id

Evidence : Command execution detected (uid=)

Impact : Attackers may execute arbitrary operating system commands, resulting in complete server compromise.

Recommendation : Avoid shell execution. Use safe APIs, validate input, allow-list commands and execute services with least privilege.

LFI

Severity : CRITICAL

CVSS : 9.1

CWE : CWE-98

OWASP : A01:2021 - Broken Access Control

Parameter : page

Payload : ../../../../etc/passwd

Evidence : Sensitive file exposed (Application response changed after LFI payload.).

Impact : No impact information available.

Recommendation : Follow secure coding and OWASP best practices.

Reference : N/A

Insecure File Upload

Severity : HIGH

CVSS : 8.8

CWE : CWE-434

OWASP : A05:2021 - Security Misconfiguration

Parameter : uploaded

Payload : test.php

Evidence : uploaded

Impact : Uploading malicious files can result in remote code execution and complete server compromise.

Recommendation : Validate file extensions, MIME types and file signatures, rename uploads, store files outside the web root and disable execution permissions.

Reference : OWASP A05:2021 Security Misconfiguration | CWE-434

Conclusion

Immediate remediation of Critical and High severity vulnerabilities is recommended. Perform a verification scan after remediation to confirm all issues have been resolved.