

INTRUDER

Security Assessment Report

Target: testphp.vulnweb.com

Scan ID: 5f1c3bb607ff4428af3e9edab132e3ed

Generated: 2026-01-26 11:42 UTC

Executive Summary

This report presents the findings of a comprehensive security assessment conducted on testphp.vulnweb.com.

Metric	Count
Total Subdomains	1
Live Assets	1
Technologies Detected	4
Open Ports	0
Total Vulnerabilities	23
Critical/High Severity	12

Reconnaissance Findings

Discovered Subdomains

Total: 1

- testphp.vulnweb.com

Technology Stack

Nginx, PHP, Ubuntu, DreamWeaver

Open Ports & Services

No open ports detected.

Vulnerability Assessment

Total Findings: 23

Critical: 10, High: 2, Medium: 5, Low: 0, Info: 0

1. [MEDIUM] Unknown

Tool: Dalfox

Location: N/A

2. [MEDIUM] Unknown

Tool: Dalfox

Location: N/A

3. [MEDIUM] Unknown

Tool: Dalfox

Location: N/A

4. [HIGH] Unknown

Tool: Dalfox

Location: N/A

5. [HIGH] Unknown

Tool: Dalfox

Location: N/A

6. [MEDIUM] Unknown

Tool: Dalfox

Location: N/A

7. [MEDIUM] Unknown

Tool: Dalfox

Location: N/A

8. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

9. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

10. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

11. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

12. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

13. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

14. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

15. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

16. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

17. [CRITICAL] SQL Injection Detected

Tool: SQLMap

Location: <http://testphp.vulnweb.com>

18. [UNKNOWN] /: Retrieved x-powered-by header:

PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.

Tool: Nikto

Location: N/A

19. [UNKNOWN] /: The anti-clickjacking X-Frame-Options header is not present.

Tool: Nikto

Location: N/A

20. [UNKNOWN] /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.

Tool: Nikto

Location: N/A

21. [UNKNOWN] /clientaccesspolicy.xml contains a full wildcard entry.

Tool: Nikto

Location: N/A

22. [UNKNOWN] /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards.

Tool: Nikto

Location: N/A

23. [UNKNOWN] /crossdomain.xml contains a full wildcard entry.

Tool: Nikto

Location: N/A

Recommendations

- URGENT: Address all Critical and High severity vulnerabilities immediately.
- Implement a Web Application Firewall (WAF) if not already in place.
- Enable security headers (CSP, HSTS, X-Frame-Options, etc.).
- Conduct regular security assessments and maintain an up-to-date asset inventory.
- Implement vulnerability disclosure program for responsible reporting.

This report was automatically generated by INTRUDER (Jarvis OS).