علوم الحاسب ونظم المعلومات
Info Sys & Comp Science

جامعة ٦ أكتوبر
October 6 University

PENETRATION TESTING REPORT

Client: testphp.vulnweb

Target: http://testphp.vulnweb.com/search.php

Generated: 1/6/2026, 12:39:38 AM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2026-01-05
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

This security assessment identified a total of 7 observed findings across various endpoints on the target application, http://testphp.vulnweb.com/search.php. The highest severity level identified was Critical (V-002), and overall confidence in the available evidence is Medium.

Please note that High or Critical severity findings exist with Low evidence confidence; these require manual validation before conclusions can be drawn.

1.2 Key Observations

Key security-related behaviors observed during testing include potential SQL injection vulnerabilities, reflected cross-site scripting (XSS) attacks, and missing security headers. These observations are based on automated testing results and structured technical observations but do not confirm exploitation.

---

2. ASSESSMENT CONTEXT

- Target Application: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Assessment Nature: Automated testing with evidence-based review
- Methodology Reference: OWASP Testing Guide, PTES

---

3. OBSERVED SECURITY FINDINGS

V-001 - SQL Injection Vulnerability

- **Finding ID:** V-001
- **Severity Level:** High
- **Evidence Confidence:** Medium

Observation Summary

Automated testing revealed potential SQL injection vulnerabilities at multiple endpoints, including http://testphp.vulnweb.com/search.php and http://testphp.vulnweb.com/userinfo.php. The observed behavior may indicate a risk of unauthorized data access or manipulation.

Why This Matters

If exploited, this vulnerability could allow attackers to inject malicious SQL code, potentially leading to sensitive data exposure or database compromise. However, the available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
    - HTTP Method: POST
    - Parameter: N/A
    - Payload Tested: N/A
    - Observed Response or Behavior: Potential SQL injection vulnerability observed.
- Endpoint: http://testphp.vulnweb.com/userinfo.php
    - HTTP Method: POST
    - Parameter: N/A
    - Payload Tested: N/A
    - Observed Response or Behavior: Potential SQL injection vulnerability observed.

V-002 - Reflected Cross-Site Scripting (XSS) Attack

- **Finding ID:** V-002
- **Severity Level:** Critical
- **Evidence Confidence:** Low

Observation Summary

Automated testing identified a potential reflected XSS attack vector at http://testphp.vulnweb.com/search.php. The observed behavior may indicate an attacker could inject malicious scripts, potentially leading to sensitive data exposure or unauthorized actions.

Why This Matters

If exploited, this vulnerability could allow attackers to execute arbitrary JavaScript code on the victim's browser, potentially leading to sensitive data exposure or unauthorized actions. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
  - HTTP Method: POST
  - Parameter: searchFor,goButton
  - Payload Tested: N/A
  - Observed Response or Behavior: Potential reflected XSS attack observed.

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL Injection Vulnerability	High	Medium
V-002	Reflected Cross-Site Scripting (XSS) Attack	Critical	Low
V-003	INFO DISCLOSURE HEADERS	Medium	Medium
V-004	MISSING SECURITY HEADERS	Medium	Medium
V-005	PERMISSIONS POLICY	Medium	Medium
V-006	TLS SECURITY CHECK	Medium	Medium

---

5. REMEDIATION & VALIDATION GUIDANCE

For V-001: SQL Injection Vulnerability

Remediation Strategy:

1. Validate and sanitize all user input to prevent malicious SQL code injection.
2. Implement a Web Application Firewall (WAF) to detect and block suspicious traffic.

Manual Validation Recommendation: Validate the effectiveness of these measures by testing with known vulnerable payloads.

For V-002: Reflected Cross-Site Scripting (XSS) Attack

Remediation Strategy:

1. Validate all user input, especially in search parameters.
2. Implement a Content Security Policy (CSP) to restrict script execution from untrusted sources.

Manual Validation Recommendation: Validate the effectiveness of these measures by testing with known XSS payloads.

---

6. OVERALL ASSESSMENT VERDICT

Based on observed findings and their evidence confidence, immediate remediation is recommended for V-001 due to its High severity level despite Medium evidence confidence. For V-002, manual validation is required before conclusions can be drawn about the potential impact of a Critical severity finding with Low evidence confidence.

Routine security hardening is sufficient for other identified vulnerabilities (V-003 through V-006).

---

7. TECHNICAL APPENDIX

For V-001: SQL Injection Vulnerability

Finding ID: V-001 Endpoint(s): http://testphp.vulnweb.com/search.php, http://testphp.vulnweb.com/userinfo.php Parameter(s): N/A Payload(s) tested: N/A Observed response patterns: Potential SQL injection vulnerability observed.

For V-002: Reflected Cross-Site Scripting (XSS) Attack

Finding ID: V-002 Endpoint: http://testphp.vulnweb.com/search.php Parameter: searchFor,goButton Payload(s) tested: N/A Observed response patterns: Potential reflected XSS attack observed.

END OF REPORT