🔒 PENETRATION TESTING REPORT

Client: testphp.vulnweb

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

Generated On: 12/31/2025, 8:59:33 AM

Classification: CONFIDENTIAL

DOCUMENT INFORMATION

Item	Value
Report Type	Evidence-Based Security Assessment
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2025-12-31
Generated By	VulnCraft AI

---

1. EXECUTIVE SUMMARY

1.1 Assessment Overview

Total number of observed findings: 2. Highest severity level identified: Critical. Overall confidence level of the available evidence is Low.

Note that High and Critical severity findings exist with Low evidence confidence, requiring manual validation before conclusions can be drawn.

1.2 Key Observations

Observed behaviors include potential SQL vulnerabilities and reflected XSS attacks. These require further investigation to confirm exploitability.

---

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

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

Observation Summary

Observed behavior is inconclusive and requires manual validation: The application's search functionality may be vulnerable to SQL injection attacks.

Why This Matters

If true, this could allow unauthorized access to sensitive data. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Simple string inputs
- Observed Response or Behavior: No clear indication of SQL injection

Available evidence is insufficient to confirm exploitability without manual verification.

V-002 - Reflected XSS

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

Observation Summary

Observed behavior may indicate a reflected cross-site scripting vulnerability: The application's search functionality may be vulnerable to reflected XSS attacks.

Why This Matters

If true, this could allow attackers to inject malicious scripts. However, available evidence is insufficient to confirm exploitability without manual verification.

Technical Evidence

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Simple string inputs
- Observed Response or Behavior: No clear indication of XSS

Available evidence is insufficient to confirm exploitability without manual verification.

4. FINDINGS SUMMARY

ID	Title	Severity	Evidence Confidence
V-001	SQL	High	Low
V-002	Reflected XSS	Critical	Low

---

5. REMEDIATION & VALIDATION GUIDANCE

V-001 - SQL

Recommend focused manual validation of the search functionality to confirm or deny SQL injection vulnerabilities.

V-002 - Reflected XSS

Suggest targeted action on the search functionality to prevent reflected XSS attacks, with a focus on validating user input and sanitizing output.

---

6. OVERALL ASSESSMENT VERDICT

Based solely on the observed findings and their evidence confidence: Immediate remediation is not recommended due to Low evidence confidence. Manual validation of both SQL injection and reflected XSS vulnerabilities is advised before conclusions can be drawn or actions taken.

---

7. TECHNICAL APPENDIX

V-001 - SQL

Finding ID: V-001 Endpoint(s): /search.php Parameter(s): query Payload(s) tested: Simple string inputs Observed response patterns: No clear indication of SQL injection.

V-002 - Reflected XSS

Finding ID: V-002 Endpoint(s): /search.php Parameter(s): query Payload(s) tested: Simple string inputs Observed response patterns: No clear indication of XSS.