🔒 PENETRATION TESTING REPORT

Client: testphp.vulnweb

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

Generated: 12/31/2025, 10:04:24 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

This security assessment report is based on automated testing results and structured technical observations. A total of **2** findings were observed during the assessment.

The highest severity level identified was **Critical**, but this finding has a low evidence confidence, indicating that manual validation is required before conclusions can be drawn.

1.2 Key Observations

During the assessment, two security-related behaviors were observed:

- A potential SQL vulnerability with strong indicators suggesting its presence.
- A reflected cross-site scripting (XSS) issue with high severity but inconclusive evidence.

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 may indicate a potential SQL vulnerability at the affected endpoint. Strong indicators suggest its presence, but available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If confirmed, this finding could lead to unauthorized data access or manipulation. However, due to low evidence confidence, the actual impact remains unconfirmed and requires manual validation.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Various SQL injection payloads
- Observed Response or Behavior: Inconclusive; further investigation required for confirmation.

V-002 - Reflected XSS

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

Observation Summary

Observed behavior may indicate a potential reflected cross-site scripting (XSS) issue at the affected endpoint. However, available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If confirmed, this finding could lead to arbitrary code execution or sensitive data theft. Again, due to low evidence confidence, the actual impact remains unconfirmed and requires manual validation.

Technical Evidence

- Endpoint: http://testphp.vulnweb.com/search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Various XSS payloads
- Observed Response or Behavior: Inconclusive; further investigation required for confirmation. 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

For V-001 - SQL

To address this finding, we recommend focused manual validation of the affected endpoint. Specifically, test for and validate against various SQL injection payloads.

Reference: http://testphp.vulnweb.com/search.php (query parameter)

For V-002 - Reflected XSS

For this finding, targeted manual validation is also recommended to confirm or deny exploitability. Test various XSS payloads at the affected endpoint: http://testphp.vulnweb.com/search.php (query parameter)

---

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings and their evidence confidence, we recommend **manual validation** for both V-001 - SQL and V-002 - Reflected XSS. Immediate remediation is not advised without further investigation.

Routine security hardening of the application is also recommended to prevent similar vulnerabilities in the future.

---

7. TECHNICAL APPENDIX

For V-001 - SQL

- Finding ID: V-001
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): query
- Payload(s) tested: Various SQL injection payloads
- Observed response patterns: Inconclusive; further investigation required for confirmation.

For V-002 - Reflected XSS

- Finding ID: V-002
- Endpoint(s): http://testphp.vulnweb.com/search.php
- Parameter(s): query
- Payload(s) tested: Various XSS payloads
- Observed response patterns: Inconclusive; further investigation required for confirmation. Available evidence is insufficient to confirm exploitability without manual verification.