🔒 PENETRATION TESTING REPORT

Client: testphp.vulnweb

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

Generated: 12/31/2025, 9:51:52 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 summarizes the results of automated testing on the target application, http://testphp.vulnweb.com/search.php. A total of 2 findings were observed during this evaluation.

The highest severity level identified is Critical (V-002), but with a Low evidence confidence level. This means that while strong indicators suggest potential security relevance, further manual validation is required to confirm the impact.

1.2 Key Observations

During testing, two notable security-related behaviors were observed:

- Potential SQL injection behavior was detected in V-001.
- Reflected XSS vulnerabilities may be present as indicated by V-002.

These findings require careful consideration and should not be assumed to represent actual exploitation without further investigation.

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

- **Finding ID:** V-001
- **Severity Level:** High
- **Evidence Confidence:** Low
- **CVSS Vector:** AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

Observation Summary

Observed behavior may indicate potential SQL injection vulnerability. Strong indicators suggest that input validation could be bypassed, but available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If confirmed, this finding would represent a significant security risk due to the potential for unauthorized data access or manipulation. However, given the Low evidence confidence level, it's crucial to manually validate these findings before drawing conclusions about their impact.

Technical Evidence

- Endpoint: /search.php
- HTTP Method: GET/POST
- Parameter: search_query
- Payload Tested: Various SQL injection payloads
- Observed Response or Behavior: Inconclusive; requires manual validation for confirmation.

Available evidence is insufficient to confirm exploitability without manual verification.

V-002 Reflected XSS

- **Finding ID:** V-002
- **Severity Level:** Critical
- **Evidence Confidence:** Low
- **CVSS Vector:** AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Observation Summary

Observed behavior may indicate potential reflected XSS vulnerability. Strong indicators suggest that user input could be executed as JavaScript, but available evidence is insufficient to confirm exploitability without manual verification.

Why This Matters

If confirmed, this finding would represent a critical security risk due to the potential for arbitrary code execution. However, given the Low evidence confidence level, it's crucial to manually validate these findings before drawing conclusions about their impact.

Technical Evidence

- Endpoint: /search.php
- HTTP Method: GET/POST
- Parameter: search_query
- Payload Tested: Various XSS payloads
- Observed Response or Behavior: Inconclusive; requires manual validation for confirmation.

Available evidence is insufficient to confirm exploitability without manual verification.

---

4. FINDINGS SUMMARY

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

---

5. REMEDIATION & VALIDATION GUIDANCE

For V-001:

- Validate input data at the /search.php endpoint to prevent potential SQL injection attacks.
- Manually verify that all user inputs are properly sanitized and validated.

For V-002:

- Review the code for any reflected XSS vulnerabilities, focusing on the search_query parameter in the /search.php endpoint.
- Perform manual validation of user inputs to ensure they do not execute arbitrary JavaScript code.

---

6. OVERALL ASSESSMENT VERDICT

Given the Low evidence confidence levels associated with both findings (V-001 and V-002), it is recommended that these issues be manually validated before any remediation efforts are undertaken. Routine security hardening practices should also be applied to prevent similar vulnerabilities in the future.

---

7. TECHNICAL APPENDIX

For V-001:

- Finding ID: V-001
- Endpoint(s): /search.php
- Parameter(s): search_query
- Payload(s) tested: Various SQL injection payloads
- Observed response patterns: Inconclusive; requires manual validation for confirmation.

For V-002:

- Finding ID: V-002
- Endpoint(s): /search.php
- Parameter(s): search_query
- Payload(s) tested: Various XSS payloads
- Observed response patterns: Inconclusive; requires manual validation for confirmation.