PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 7:33:34 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 identified a total of 2 observed findings.
The highest severity level identified is Critical, but the evidence confidence for this finding is Low.
Overall, the available evidence suggests potential vulnerabilities exist that require manual validation.

1.2 Key Observations

Two security-relevant behaviors were observed during testing:

- Potential SQL injection behavior may be present due to observed patterns in error messages.
- A possible Reflected XSS vulnerability might exist based on detected behaviors at certain endpoints.

---

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

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

Strong indicators suggest potential SQL injection behavior may be present.
Observed error messages and patterns in the application's response could indicate an attempt to inject malicious SQL code.

WHY THIS MATTERS

If confirmed, this vulnerability would allow attackers to execute arbitrary database queries,
potentially leading to unauthorized data access or modification.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Various SQL injection payloads

- Observed Response or Behavior: Error messages indicating potential SQL syntax errors

Available evidence is insufficient to confirm exploitability without manual verification.

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 a possible Reflected XSS vulnerability.
Detected patterns in the application's response could suggest an attacker can inject malicious scripts via reflected input.

WHY THIS MATTERS

If confirmed, this vulnerability would allow attackers to execute arbitrary JavaScript code,
potentially leading to unauthorized access or control of user sessions.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload Tested: Various XSS payloads
- Observed Response or Behavior: Error messages indicating potential script injection attempts

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 GUIDANCE

SQL Injection (V-001)

- **Remediation Action:** Perform targeted manual validation of the application's database queries.
- **Scope:** Validate all user-inputted parameters and ensure they are properly sanitized before being used in SQL queries.

Reflected XSS (V-002)

- **Remediation Action:** Conduct a thorough review of the application's input handling mechanisms to prevent reflected XSS attacks.
- **Scope:** Ensure that any user-input data is thoroughly validated, encoded, or otherwise secured against injection and script execution.

---

6. OVERALL ASSESSMENT VERDICT

Based on the observed findings and their evidence confidence,
immediate remediation of these vulnerabilities cannot be confirmed without manual validation.
Therefore, we recommend targeted manual validation for both SQL Injection (V-001) and Reflected XSS (V-002).

Routine hardening is not sufficient due to the potential severity of these vulnerabilities.

---

7. TECHNICAL APPENDIX

V-001: SQL Injection

- Finding ID: V-001
- Endpoint(s): /search.php
- Parameter(s): query
- Payload(s) tested: Various SQL injection payloads
- Observed response patterns: Error messages indicating potential SQL syntax errors

V-002: Reflected XSS

- Finding ID: V-002
- Endpoint(s): /search.php
- Parameter(s): query
- Payload(s) tested: Various XSS payloads
- Observed response patterns: Error messages indicating potential script injection attempts