PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 7:21:38 AM
Classification: CONFIDENTIAL

DOCUMENT INFORMATION

ITEM	VALUE
Report Type	Observational Security Assessment
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2025-12-31
Generated By	VulnCraft AI

1. EXECUTIVE SUMMARY

1.1 Overview

There are two findings reported in this assessment.
The highest severity observed is Critical (V-002).
However, the evidence confidence for both findings is Low.

1.2 Key Observations

Two critical security issues were identified:

- Observed SQL behavior in an unknown endpoint (V-001)
- Reflected behavior in another unknown endpoint (V-002)

2. ASSESSMENT CONTEXT

- Target Application: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Assessment Nature: Evidence-based observational review

---

3. OBSERVED SECURITY FINDINGS

V-001 Observed SQL Behavior in Unknown Endpoint

- **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 vulnerability in an unknown endpoint. However, the available evidence is insufficient to confirm impact without manual verification.

WHY THIS MATTERS

If confirmed, this could lead to unauthorized database access and data manipulation. Further investigation is required to validate the severity of this finding.

TECHNICAL EVIDENCE

- Endpoint: /search.php (unknown)
- HTTP Method: GET
- Parameter: query (unknown)
- Payload Tested: None specified
- Observed Behavior: Potential SQL injection behavior observed, but evidence is inconclusive and requires manual validation.

V-002 Observed Reflected Behavior in Unknown Endpoint

- **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 reflected cross-site scripting (XSS) vulnerability in an unknown endpoint. However, the available evidence is insufficient to confirm impact without manual verification.

WHY THIS MATTERS

If confirmed, this could lead to arbitrary code execution and unauthorized access to sensitive data. Further investigation is required to validate the severity of this finding.

TECHNICAL EVIDENCE

- Endpoint: /search.php (unknown)
- HTTP Method: GET
- Parameter: query (unknown)
- Payload Tested: None specified
- Observed Behavior: Potential reflected XSS behavior observed, but evidence is inconclusive and requires manual validation.

---

4. FINDINGS SUMMARY

ID	TITLE	SEVERITY	EVIDENCE CONFIDENCE
V-001	Observed SQL Behavior in Unknown Endpoint	High	Low
V-002	Observed Reflected Behavior in Unknown Endpoint	Critical	Low

---

5. REMEDIATION GUIDANCE

V-001

Given the low evidence confidence, it is recommended to perform manual validation of this finding before taking any remediation actions.

V-002

Similarly, due to the low evidence confidence, it is advised to manually validate this finding before implementing any remedial measures.

---

6. OVERALL ASSESSMENT VERDICT

Based on the findings and their evidence confidence, it is recommended that manual validation be performed for both identified vulnerabilities before taking any further action.

---

7. TECHNICAL APPENDIX

V-001

- Finding ID: V-001
- Endpoint(s): /search.php (unknown)
- Parameter(s): query (unknown)
- Payload(s) tested: None specified
- Observed responses or anomalies: Potential SQL injection behavior observed, but evidence is inconclusive and requires manual validation.

V-002

- Finding ID: V-002
- Endpoint(s): /search.php (unknown)
- Parameter(s): query (unknown)
- Payload(s) tested: None specified
- Observed responses or anomalies: Potential reflected XSS behavior observed, but evidence is inconclusive and requires manual validation.