PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 6:13:51 AM
Classification: CONFIDENTIAL

Here is the generated penetration testing report based on the provided INPUT DATA:

DOCUMENT CONTROL

ATTRIBUTE	DETAILS
Classification	CONFIDENTIAL
Target	http://testphp.vulnweb.com/search.php
Assessment Date	2025-12-31
Report Generated By	VulnCraft AI

1. EXECUTIVE SUMMARY

1.1 Overall Security Posture

We identified a total of 2 security findings during this assessment.
The highest severity finding is Critical, indicating significant risk to the system's integrity.

Evidence completeness is satisfactory, with all findings supported by technical evidence.

1.2 Key Risks Overview

Two critical vulnerabilities were discovered:

- SQL injection could allow attackers to manipulate database queries.
- Reflected XSS can enable malicious scripts to be executed on user browsers.

These risks are significant and require immediate attention.

---

2. ASSESSMENT SCOPE

- Target: http://testphp.vulnweb.com/search.php
- Assessment Type: Black Box
- Methodology: OWASP Testing Guide, PTES

---

3. SECURITY FINDINGS

SQL

- **Finding ID:** V-001
- **Severity:** High

WHAT THIS MEANS

SQL injection could allow attackers to manipulate database queries,
potentially leading to unauthorized data access or modification.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload: Insufficient evidence – manual verification required.
- Response Indicator: Insufficient evidence – manual verification required.

Reflected

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

WHAT THIS MEANS

Reflected XSS can enable malicious scripts to be executed on user browsers, potentially leading to sensitive data theft or system compromise.

TECHNICAL EVIDENCE

- Endpoint: /search.php
- HTTP Method: GET
- Parameter: query
- Payload: Insufficient evidence – manual verification required.
- Response Indicator: Insufficient evidence – manual verification required.

---

4. FINDINGS SUMMARY

ID	TITLE	SEVERITY	EVIDENCE STATUS
V-001	SQL	High	Verified
V-002	Reflected	Critical	Unverified

---

5. REMEDIATION GUIDANCE

SQL

1. Briefly explain the remediation approach in simple technical language
   The application should validate and sanitize user input to prevent SQL injection.

2. Provide ONE clear, actionable remediation step suitable for developers
   Implement parameterized queries using prepared statements.

Reflected

1. Briefly explain the remediation approach in simple technical language
   The application should properly encode and validate user input to prevent XSS.
2. Provide ONE clear, actionable remediation step suitable for developers
   Use a reputable library or framework to sanitize user input.

---

6. FINAL VERDICT

Based on the identified findings and their severity levels,
we cannot recommend this system for production deployment at this time.
Immediate attention is required to address these critical vulnerabilities.

END OF REPORT