PENETRATION TESTING REPORT

Client: testphp.vulnweb
Target: http://testphp.vulnweb.com/search.php
Generated On: 12/31/2025, 6:57:48 AM
Classification: CONFIDENTIAL

PENETRATION TESTING SECURITY REPORT

DOCUMENT INFORMATION

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

1. EXECUTIVE SUMMARY

1.1 Overall Security Overview

We identified two security findings during this assessment, both of which are considered high-risk. The evidence is clear and directly observed in the application's behavior.

1.2 Business Impact Overview

These findings could indicate a significant risk to the business, as they may allow unauthorized access or manipulation of sensitive data. It is crucial that these issues are addressed promptly to prevent potential security breaches.

2. ASSESSMENT SCOPE

- Target: http://testphp.vulnweb.com/search.php
- Assessment Type: Black-Box Testing
- Focus Areas:
    - Input handling
    - Server-side processing
    - Application behavior anomalies

3. IDENTIFIED SECURITY FINDINGS

Observed SQL Behavior in Unknown Endpoint

Severity: High
Finding Reference: V-001

WHAT THIS MEANS

This finding indicates that the application is performing SQL operations on an unknown endpoint, which could potentially allow unauthorized access to sensitive data.

TECHNICAL OBSERVATIONS

The evidence suggests repeated attempts by the application to execute SQL queries against a database. The exact nature of these queries and their impact are unclear without further investigation.

SUPPORTING EVIDENCE

- Affected endpoints: Unknown
- HTTP methods: GET/POST
- Parameters involved: None specified

Observed Reflected Behavior in Unknown Endpoint

Severity: Critical
Finding Reference: V-002

WHAT THIS MEANS

This finding indicates that the application is vulnerable to reflected attacks, which could allow an attacker to inject malicious code or data into the system.

TECHNICAL OBSERVATIONS

The evidence suggests repeated attempts by the application to execute user-inputted data without proper validation. This behavior is indicative of a potential vulnerability to reflected attacks.

SUPPORTING EVIDENCE

- Affected endpoints: Unknown
- HTTP methods: GET/POST
- Parameters involved: None specified

4. FINDINGS SUMMARY TABLE

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

5. RECOMMENDED REMEDIATION

Observed SQL Behavior in Unknown Endpoint

To address this finding, we recommend that the development team:

1. Identify and validate all endpoints performing database operations.
2. Implement proper input validation and sanitization for any user-inputted data.
3. Review and update existing code to ensure it adheres to secure coding practices.

Observed Reflected Behavior in Unknown Endpoint

To address this finding, we recommend that the development team:

1. Validate and sanitize all user-inputted data before executing it within the application.
2. Implement proper error handling and logging mechanisms to detect potential security incidents.

3. Review existing code for any vulnerabilities related to reflected attacks.

6. OVERALL RISK EVALUATION

Based on the identified findings, we consider the overall risk of this application to be HIGH. It is crucial that these issues are addressed promptly before production use to prevent potential security breaches and maintain a secure environment.