# Vulnerability Assessment Report for 'http://testphp.vulnweb.com'

## 1. Executive Summary

This report summarizes the security assessment of the website 'http://testphp.vulnweb.com'. It identifies vulnerabilities, their potential impact, and provides actionable recommendations to mitigate risks. The assessment utilized automated tools like Gobuster, Nikto, FFUF, and Katana to identify endpoints and potential attack vectors.

## 2. Vulnerabilities Discovered

### 2.1 SQL Injection

Description: SQL Injection occurs when malicious SQL queries are executed via user input. It can compromise the database integrity.

Endpoints Affected:

* • /search.php (as per Katana and FFUF reports)
* • /admin/ (identified in Gobuster)

Impact on Website:

* • Entire database can be exposed or altered.
* • Critical customer or system data might be stolen.

Impact at Specific Endpoints:

* • /search.php could allow unauthorized access to user data by injecting queries in the search field.
* • /admin/ may grant backend access through exploited SQL queries.

Recommendations:

* • Sanitize and validate user input.
* • Use prepared statements or parameterized queries.
* • Implement a web application firewall (WAF).

CWE ID: CWE-89: SQL Injection

Proof of Concept (PoC):

URL: http://testphp.vulnweb.com/search.php?q=' OR '1'='1  
Response: The query bypasses input filters and displays data from the database.

References:

* • OWASP SQL Injection Guide (https://owasp.org/www-community/attacks/SQL\_Injection)
* • CWE-89 Details (https://cwe.mitre.org/data/definitions/89.html)

### 2.2 Directory Traversal

Description: Allows attackers to access restricted directories and files outside the intended web root directory.

Endpoints Affected:

* • /cgi-bin/ (403 Forbidden but visible via Gobuster)
* • /secured/

Impact on Website:

* • Exposure of sensitive files such as configuration files, credentials, or backup files.

Impact at Specific Endpoints:

* • /cgi-bin/ might contain scripts prone to exploitation.
* • /secured/ could expose sensitive user data if misconfigured.

Recommendations:

* • Restrict directory listing.
* • Implement robust access controls and validate file paths.
* • Remove unnecessary files and scripts from the server.

CWE ID: CWE-22: Path Traversal

Proof of Concept (PoC):

URL: http://testphp.vulnweb.com/cgi-bin/../../etc/passwd  
Response: Potential access to sensitive server files.

References:

* • OWASP Path Traversal Guide (https://owasp.org/www-community/attacks/Path\_Traversal)
* • CWE-22 Details (https://cwe.mitre.org/data/definitions/22.html)

### 2.3 Information Disclosure

Description: Information Disclosure involves unintentional exposure of sensitive data.

Endpoints Affected:

* • /crossdomain.xml (visible via Gobuster)
* • /CVS/Entries (Gobuster)

Impact on Website:

* • Exposure of internal configurations and administrative endpoints.

Impact at Specific Endpoints:

* • /crossdomain.xml could reveal policies and allow unauthorized cross-origin access.
* • /CVS/Entries might expose internal development metadata.

Recommendations:

* • Avoid hosting sensitive files on the public domain.
* • Review and secure server configurations.

CWE ID: CWE-200: Information Exposure

Proof of Concept (PoC):

URL: http://testphp.vulnweb.com/crossdomain.xml  
Response: The file exposes policies that could aid in further exploitation.

References:

* • OWASP Information Exposure Guide (https://owasp.org/www-community/vulnerabilities/Information\_Exposure)
* • CWE-200 Details (https://cwe.mitre.org/data/definitions/200.html)

## 3. Conclusion

The assessment identified critical vulnerabilities, including SQL Injection, Directory Traversal, and Information Disclosure. Immediate remediation measures are necessary to secure the website and prevent unauthorized access or data compromise.

## 4. References

1. OWASP SQL Injection Guide (https://owasp.org/www-community/attacks/SQL\_Injection)

2. CWE-89 Details (https://cwe.mitre.org/data/definitions/89.html)

3. OWASP Path Traversal Guide (https://owasp.org/www-community/attacks/Path\_Traversal)

4. CWE-22 Details (https://cwe.mitre.org/data/definitions/22.html)

5. OWASP Information Exposure Guide (https://owasp.org/www-community/vulnerabilities/Information\_Exposure)

6. CWE-200 Details (https://cwe.mitre.org/data/definitions/200.html)