AUTOMATED VULNERABILITY SCANNING ASSESSMENT REPORT

Target: testphp.vulnweb.com

Document Classification:	Educational Assessment
Date:	September 15, 2025
Assessment Type:	Automated Web Application Vulnerability Scanning
Organization:	ZeroDayVault Cyber Security Internship Program

1. EXECUTIVE SUMMARY

This report documents the findings from an automated vulnerability scanning assessment conducted against testphp.vulnweb.com, an intentionally vulnerable web application maintained by Acunetix for security testing purposes. The assessment utilized multiple professional-grade security tools to identify critical vulnerabilities including SQL injection vectors, Cross-Site Scripting (XSS), information disclosure issues, and security header misconfigurations.

Key Findings:

- Target system successfully enumerated with comprehensive service identification
- Multiple critical vulnerabilities confirmed through automated scanning tools
- Administrative directories and sensitive files exposed through directory enumeration
- Web application demonstrates significant security weaknesses including injection flaws
- Missing security headers and CSRF protection across all application endpoints

Risk Summary:

- Critical Risk: 3 findings (SQL Injection, XSS, Information Disclosure)
- High Risk: 2 findings (Admin Directory, FTP Log Exposure)
- Medium Risk: 6 findings (Security Headers, CSRF, Cross-Domain Policy)
- Low Risk: 2 findings (Version Disclosure, Header Information)

2. ENGAGEMENT DETAILS

Target Information:

- Primary Target: testphp.vulnweb.com
- IP Address: 44.228.249.3
- DNS Record: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
- Geographic Location: United States (AWS US-West-2)

Tools Utilized:

- Nmap 7.95 (Network discovery, port scanning, NSE vulnerability scripts)
- Dirb v2.22 (Directory enumeration and brute-forcing)
- Nikto v2.5.0 (Web vulnerability scanning)
- OWASP ZAP (Comprehensive web application security testing)
- Nuclei (Template-based vulnerability detection)
- WhatWeb (Technology fingerprinting)

3. TECHNICAL FINDINGS

3.1 Host Discovery Results

The target host was successfully identified and confirmed operational through network reconnaissance.

Host Status:	Active
Response Time:	0.00029s latency
Infrastructure:	Amazon Web Services (AWS)
Network Accessibility:	Confirmed via ICMP and TCP connectivity

3.2 Port and Service Enumeration

Comprehensive port scanning revealed a single accessible service with aggressive firewall filtering protecting other ports.

Port	Protocol	Service	Version	Status
80	TCP	HTTP	nginx 1.19.0	Open

4. VULNERABILITY ASSESSMENT

4.1 Critical Risk Vulnerabilities

SQL Injection (Multiple Endpoints)

- Severity: Critical
- CVSS Score: 9.1
- Detection Method: Nmap NSE Scripts, OWASP ZAP
- Impact: Complete database compromise, data exfiltration, authentication bypass
- Evidence: MySQL error messages confirmed, 44+ injection points identified

Cross-Site Scripting (Reflected)

- Severity: Critical
- CVSS Score: 8.1
- Detection Method: OWASP ZAP Active Scanner
- Location: /secured/newuser.php
- Parameter: uuname (username field)
- Impact: Session hijacking, account takeover, malicious content injection

6. RISK ANALYSIS AND RECOMMENDATIONS

6.1 Immediate Actions Required

1. Remove PHP Information Disclosure - Delete or restrict access to /secured/phpinfo.php (Timeline: Immediate, Priority: Critical)
2. Implement SQL Injection Prevention - Deploy parameterized queries across all database interactions (Timeline: Immediate, Priority: Critical)
3. Cross-Site Scripting Remediation - Implement output encoding and input validation (Timeline: Immediate, Priority: Critical)
4. Configure Restrictive Cross-Domain Policies - Replace wildcard permissions with specific domain allowlists (Timeline: Immediate, Priority: Critical)

8. CONCLUSION

The automated vulnerability scanning assessment successfully identified comprehensive security vulnerabilities across testphp.vulnweb.com. As an intentionally vulnerable educational platform, the target demonstrated expected security weaknesses including critical SQL injection vulnerabilities, Cross-Site Scripting flaws, information disclosure issues, and security configuration problems.

The assessment methodology proved highly effective in identifying both network-level and application-layer security issues through the combined use of multiple automated tools. The comprehensive scanning approach revealed significant attack vectors that would require immediate attention in a production environment.

9. APPENDICES

Appendix A: Command Reference

- `nmap -sn testphp.vulnweb.com`
- `nmap -sV -p- -sC -T4 testphp.vulnweb.com`
- `dirb http://testphp.vulnweb.com`
- `nikto -h http://testphp.vulnweb.com -o nikto_report.txt`
- `nuclei -u http://testphp.vulnweb.com -as -o nuclei.txt -c 10`
- `zap-baseline.py -t http://testphp.vulnweb.com -r zap_baseline.html`

Appendix B: Tool Output Files

- Host Discovery: namoSN.txt
- Service Detection: Service-Version.txt
- Vulnerability Assessment: VulnerabilityScanning.txt
- Directory Enumeration: Basic-Directory-Brute-force.txt
- Web Vulnerability Scan: nikto_report.txt
- Technology Detection: WebTechnologyDetection.txt
- Nuclei Output: nuclei.txt
- OWASP ZAP Report: 2025-09-15-ZAP-Report.html