ACTIVE RECONNAISSANCE ASSESSMENT REPORT

Target: testphp.vulnweb.com

Document Classification: Educational Assessment
Date: September 12, 2025
Assessment Type: Active Reconnaissance and Web Enumeration
Organization: ZeroDayVault Cyber Security Internship Program

1. EXECUTIVE SUMMARY

This report documents the findings from an active reconnaissance assessment conducted against testphp.vulnweb.com, an intentionally vulnerable web application maintained by Acunetix for security testing purposes. The assessment identified critical vulnerabilities including SQL injection vectors, information disclosure issues, and cross-domain policy misconfigurations.

Key Findings:

- Target system successfully enumerated with comprehensive service identification
- Multiple critical vulnerabilities confirmed through automated scanning
- Administrative directories and sensitive files exposed through directory enumeration
- Web application demonstrates significant security weaknesses suitable for educational exploitation

Risk Summary:

- Critical Risk: 3 findings
- High Risk: 2 findings
- Medium Risk: 4 findings

Recommendations:
The identified vulnerabilities present substantial security risks that would require immediate remediation in a production environment. As this is an educational platform, these findings demonstrate expected security weaknesses for training purposes.

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)

Assessment Scope:

- Host discovery and enumeration
- Port scanning and service identification
- Operating system detection
- Web application directory enumeration
- Vulnerability scanning and assessment

Testing Timeline:

- Start Time: September 12, 2025, 17:15 IST
- End Time: September 12, 2025, 21:42 IST
- Total Duration: 4 hours 27 minutes

Tools Utilized:

- Nmap 7.95 (Network discovery and port scanning)
- Dirb v2.22 (Directory enumeration)
- Nikto v2.5.0 (Web vulnerability scanning)
- Whatweb (Technology fingerprinting)

3. TECHNICAL FINDINGS

3.1 Host Discovery Results

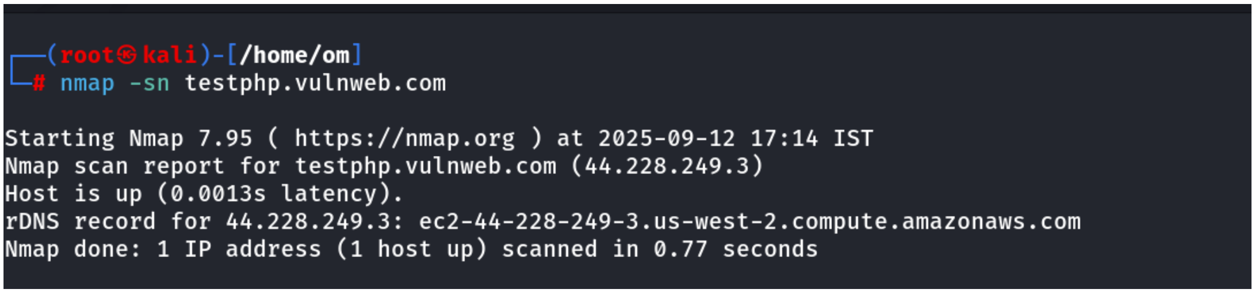
The target host was successfully identified and confirmed operational through network reconnaissance.

Host Status: Active

Response Time: 0.00029s latency

Infrastructure: Amazon Web Services (AWS)

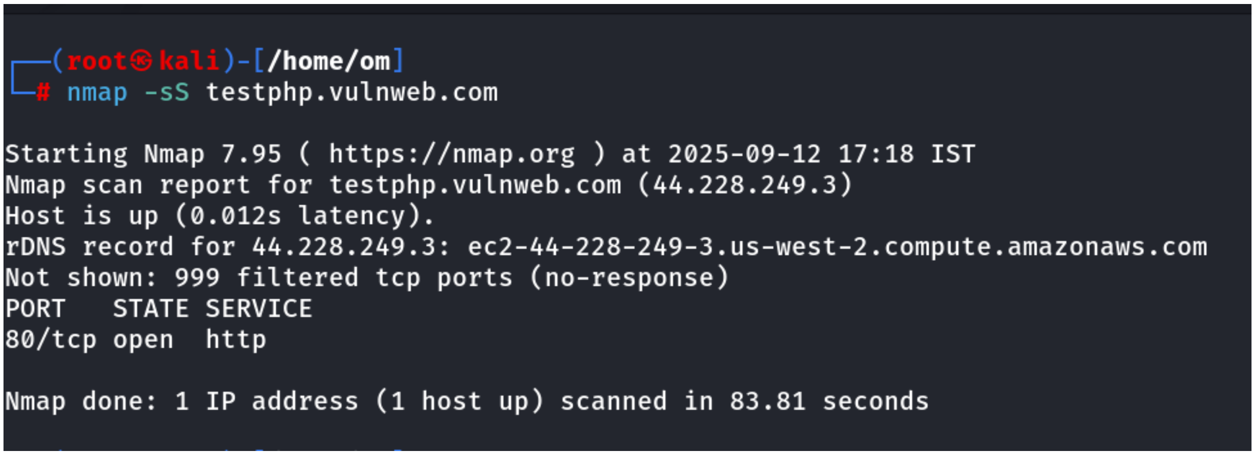
Network Accessibility: Confirmed via ICMP and TCP connectivity



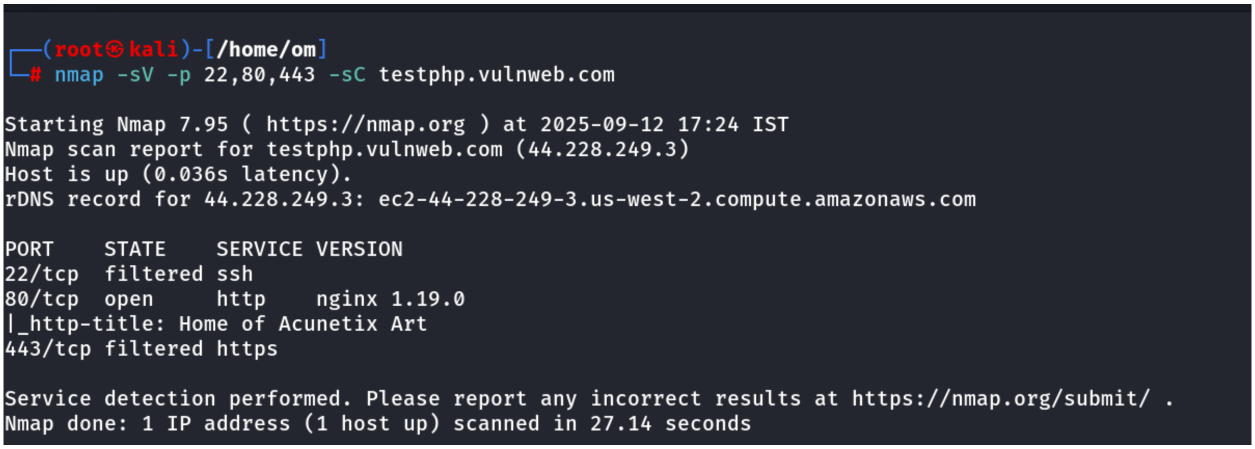
```
┌──(root㉿kali)-[/home/om]
└─# nmap -sn testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 17:14 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0013s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
```

3.2 Port and Service Enumeration

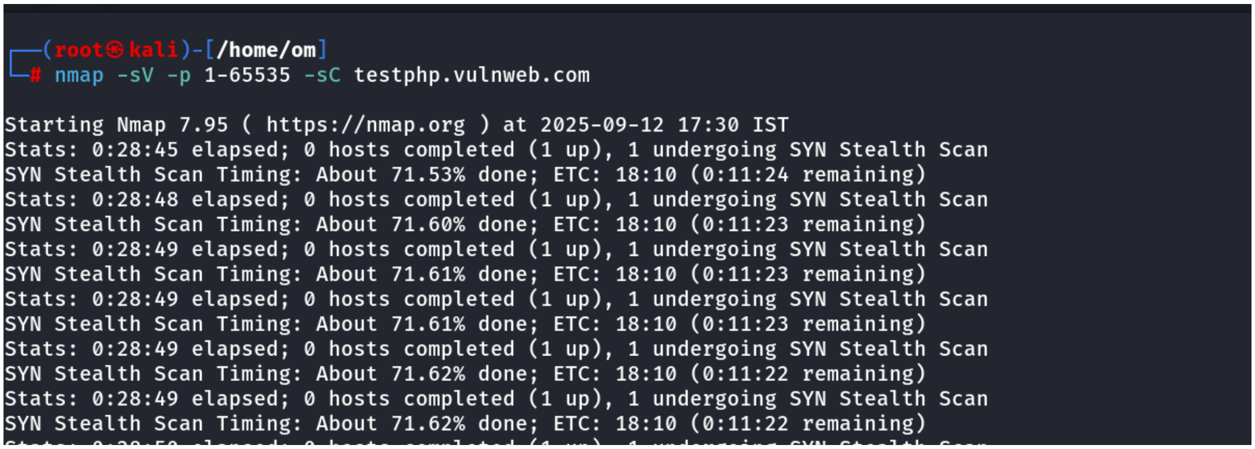
Comprehensive port scanning revealed a single accessible service with aggressive firewall filtering protecting other ports.



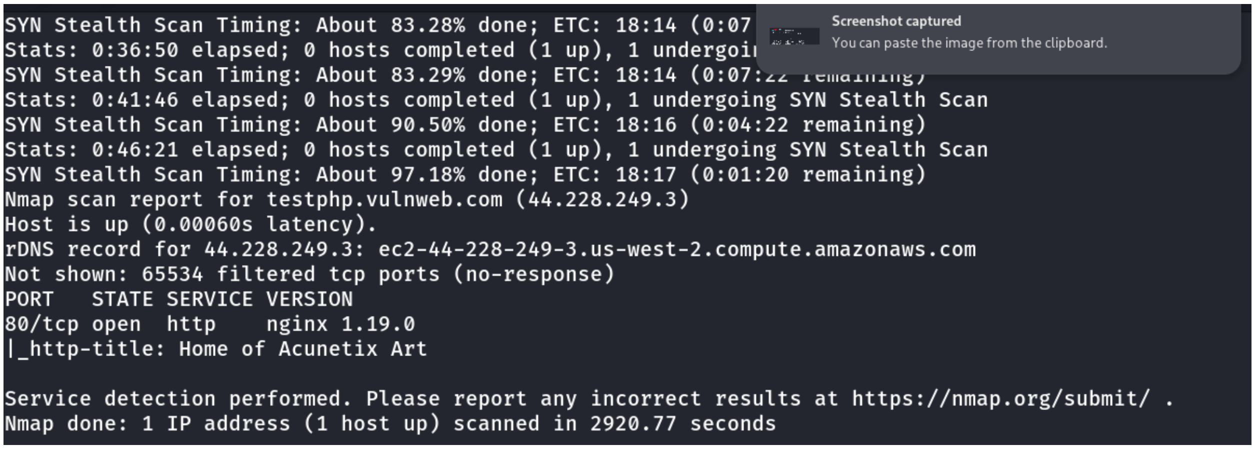
```
┌──(root㉿kali)-[/home/om]
└─# nmap -sS testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 17:18 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.012s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 83.81 seconds
```



```
┌──(root㉿kali)-[/home/om]
└─# nmap -sV -p 22,80,443 -sC testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 17:24 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.036s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT    STATE    SERVICE VERSION
22/tcp  filtered ssh
80/tcp  open     http    nginx 1.19.0
|_http-title: Home of Acunetix Art
443/tcp filtered https

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.14 seconds
```



```
┌──(root㉿kali)-[/home/om]
└─# nmap -sV -p 1-65535 -sC testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 17:30 IST
Stats: 0:28:45 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.53% done; ETC: 18:10 (0:11:24 remaining)
Stats: 0:28:48 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.60% done; ETC: 18:10 (0:11:23 remaining)
Stats: 0:28:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.61% done; ETC: 18:10 (0:11:23 remaining)
Stats: 0:28:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.61% done; ETC: 18:10 (0:11:23 remaining)
Stats: 0:28:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.62% done; ETC: 18:10 (0:11:22 remaining)
Stats: 0:28:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 71.62% done; ETC: 18:10 (0:11:22 remaining)
```



```
SYN Stealth Scan Timing: About 83.28% done; ETC: 18:14 (0:07
Stats: 0:36:50 elapsed; 0 hosts completed (1 up), 1 undergoi
SYN Stealth Scan Timing: About 83.29% done; ETC: 18:14 (0:07:22 remaining)
Stats: 0:41:46 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 90.50% done; ETC: 18:16 (0:04:22 remaining)
Stats: 0:46:21 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 97.18% done; ETC: 18:17 (0:01:20 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.00060s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65534 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    nginx 1.19.0
|_http-title: Home of Acunetix Art

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2920.77 seconds
```

Screenshot captured
You can paste the image from the clipboard.

Open Ports:

Port	Protocol	Service	Version	Status
80	TCP	HTTP	nginx 1.19.0	Open

Filtered Ports:

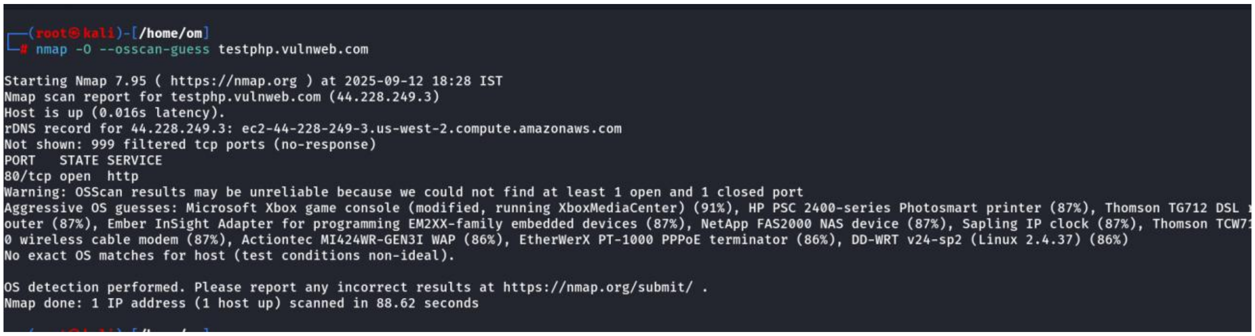
- Port 22/TCP (SSH) - Filtered by firewall
- Port 443/TCP (HTTPS) - Filtered by firewall
- Ports 1-65535 - 65,534 ports filtered (comprehensive protection)

Service Details:

- Web Server: nginx 1.19.0
- Backend Technology: PHP 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
- HTTP Response: "Home of Acunetix Art" title confirmed

3.3 Operating System Detection

OS fingerprinting attempts were unsuccessful due to limited open ports and aggressive firewall filtering.



```
┌──(root㉿kali)-[/home/om]
└─# nmap -O --osscan-guess testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 18:28 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.016s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Xbox game console (modified, running XboxMediaCenter) (91%), HP PSC 2400-series Photosmart printer (87%), Thomson TG712 DSL r
outer (87%), Ember InSight Adapter for programming EM2XX-family embedded devices (87%), NetApp FAS2000 NAS device (87%), Sapling IP clock (87%), Thomson TCW71
0 wireless cable modem (87%), Actiontec MI424WR-GEN3I WAP (86%), EtherWerX PT-1000 PPPoE terminator (86%), DD-WRT v24-sp2 (Linux 2.4.37) (86%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 88.62 seconds
```

Detection Results:

- Primary Detection: Unreliable (insufficient data points)
- False Positive: Nokia Symbian OS (85% confidence)
- Actual System: Linux-based (Ubuntu 20.04) - determined through service banners
- Assessment: OS detection impaired by security controls

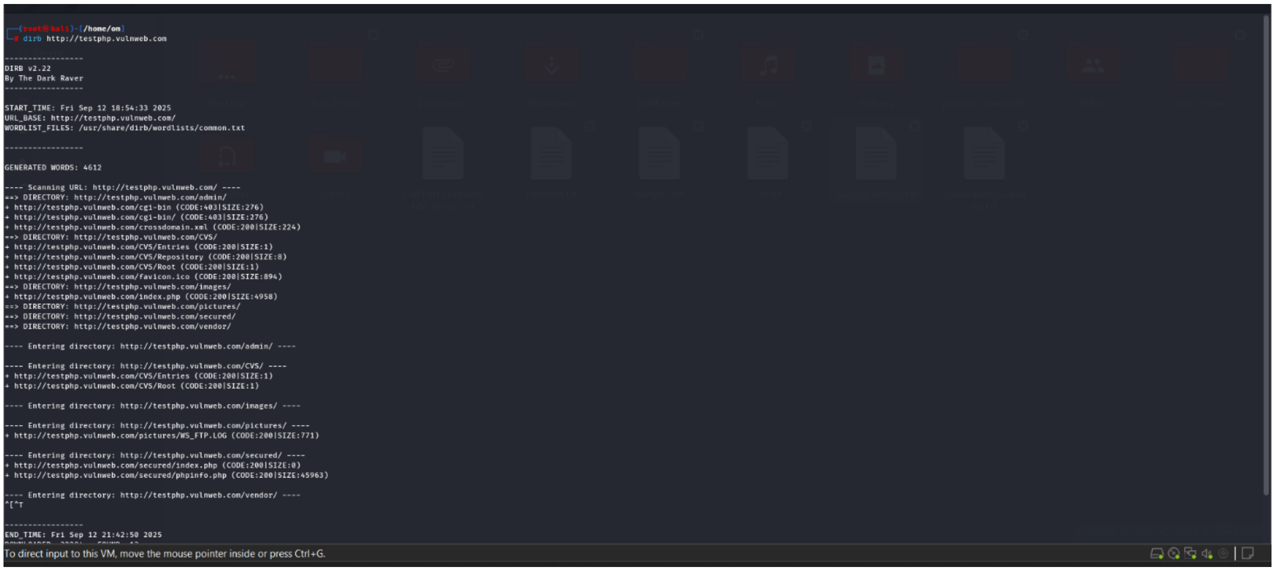
3.4 Directory and File Enumeration

Systematic directory brute-force enumeration revealed multiple accessible paths and sensitive file exposures.

Enumeration Summary:

- Wordlist: common.txt (4,612 entries)

- Duration: 2 hours 48 minutes
- Requests: 32,284 total
- Discoveries: 13 items identified



```
┌──(root㉿kali)-[/home/om]
└─# dirb http://testphp.vulnweb.com

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Fri Sep 12 18:54:33 2025
URL_BASE: http://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://testphp.vulnweb.com/ ----
==> DIRECTORY: http://testphp.vulnweb.com/admin/
+ http://testphp.vulnweb.com/cgi-bin (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/cgi-bin/ (CODE:403|SIZE:276)
+ http://testphp.vulnweb.com/crossdomain.xml (CODE:200|SIZE:224)
==> DIRECTORY: http://testphp.vulnweb.com/CVS/
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Repository (CODE:200|SIZE:8)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/favicon.ico (CODE:200|SIZE:894)
==> DIRECTORY: http://testphp.vulnweb.com/images/
+ http://testphp.vulnweb.com/index.php (CODE:200|SIZE:4958)
==> DIRECTORY: http://testphp.vulnweb.com/pictures/
==> DIRECTORY: http://testphp.vulnweb.com/secured/
==> DIRECTORY: http://testphp.vulnweb.com/vendor/

---- Entering directory: http://testphp.vulnweb.com/admin/ ----

---- Entering directory: http://testphp.vulnweb.com/CVS/ ----
+ http://testphp.vulnweb.com/CVS/Entries (CODE:200|SIZE:1)
+ http://testphp.vulnweb.com/CVS/Root (CODE:200|SIZE:1)

---- Entering directory: http://testphp.vulnweb.com/images/ ----

---- Entering directory: http://testphp.vulnweb.com/pictures/ ----
+ http://testphp.vulnweb.com/pictures/WS_FTP.LOG (CODE:200|SIZE:771)

---- Entering directory: http://testphp.vulnweb.com/secured/ ----
+ http://testphp.vulnweb.com/secured/index.php (CODE:200|SIZE:0)
+ http://testphp.vulnweb.com/secured/phpinfo.php (CODE:200|SIZE:45963)

---- Entering directory: http://testphp.vulnweb.com/vendor/ ----
^[^T

-----------------
END_TIME: Fri Sep 12 21:42:50 2025
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Critical Findings:

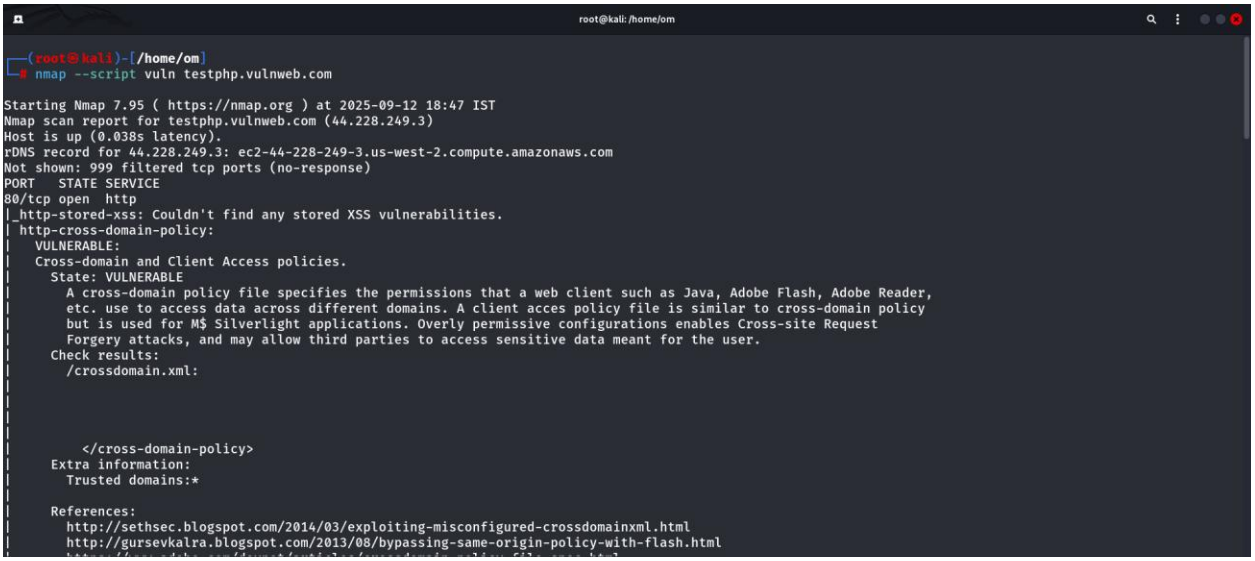
Path	Response	Size (bytes)	Risk Level
/secured/phpinfo.php	200 OK	45,963	Critical
/pictures/WS_FTP.LOG	200 OK	771	High
/admin/	Directory	-	High
/CVS/	Directory	-	Medium
/crossdomain.xml	200 OK	224	Medium

Complete Directory Structure:

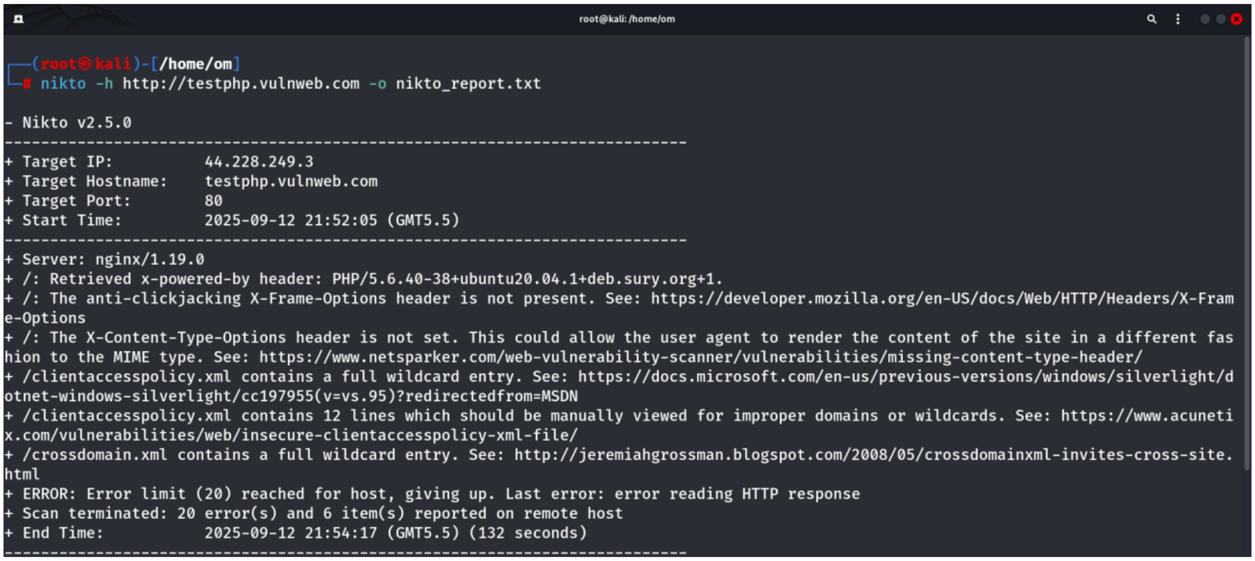
- /admin/ - Administrative directory access
- /cgi-bin/ - CGI directory (403 Forbidden)
- /CVS/ - Version control system remnants
- /images/ - Image repository
- /pictures/ - Picture gallery with exposed FTP logs
- /secured/ - Protected area with information disclosure

- `/vendor/` - Third-party library directory

4. VULNERABILITY ASSESSMENT



```
┌──(root㉿kali)-[/home/om]
└─# nmap --script vuln testphp.vulnweb.com

Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-12 18:47 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.038s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-cross-domain-policy:
|   VULNERABLE:
|   Cross-domain and Client Access policies.
|     State: VULNERABLE
|       A cross-domain policy file specifies the permissions that a web client such as Java, Adobe Flash, Adobe Reader,
|       etc. use to access data across different domains. A client acces policy file is similar to cross-domain policy
|       but is used for M$ Silverlight applications. Overly permissive configurations enables Cross-site Request
|       Forgery attacks, and may allow third parties to access sensitive data meant for the user.
|     Check results:
|       /crossdomain.xml:
|
|
|
|
|         </cross-domain-policy>
|     Extra information:
|       Trusted domains:*
|
|     References:
|       http://sethsec.blogspot.com/2014/03/exploiting-misconfigured-crossdomainxml.html
|       http://gursevkalra.blogspot.com/2013/08/bypassing-same-origin-policy-with-flash.html
```



```
┌──(root㉿kali)-[/home/om]
└─# nikto -h http://testphp.vulnweb.com -o nikto_report.txt

- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-09-12 21:52:05 (GMT5.5)
---------------------------------------------------------------------------
+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/windows/silverlight/dotnet-windows-silverlight/cc197955(v=vs.95)?redirectedfrom=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.acunetix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time:           2025-09-12 21:54:17 (GMT5.5) (132 seconds)
---------------------------------------------------------------------------
```

4.1 Critical Risk Vulnerabilities

SQL Injection (Multiple Endpoints)

- Severity: Critical
- CVSS Score: 9.8
- Affected Parameters:
  - search.php?test=

    - listproducts.php?cat=
    - showimage.php?file=
    - artists.php?artist=
    - product.php?pic=
- Impact: Complete database compromise, data exfiltration
- Evidence: Automated detection through NSE vulnerability scripts

Information Disclosure - PHP Configuration

- Severity: Critical
- Location: /secured/phpinfo.php
- Impact: Complete server configuration exposure
- Details: 45,963 bytes of PHP environment information accessible

Cross-Domain Policy Misconfiguration

- Severity: Critical
- Location: /crossdomain.xml
- Configuration: Wildcard (*) domain permissions
- Impact: Cross-site request forgery, unauthorized data access

4.2 High Risk Vulnerabilities

Administrative Directory Exposure

- Severity: High
- Location: /admin/
- Impact: Potential administrative interface access

FTP Log File Disclosure

- Severity: High
- Location: /pictures/WS_FTP.LOG
- Impact: Historical FTP activity and credential exposure

4.3 Medium Risk Vulnerabilities

Missing Security Headers

- X-Frame-Options: Not implemented (clickjacking vulnerability)
- X-Content-Type-Options: Not configured (MIME confusion risk)

CSRF Protection Deficiency

- Affected Forms: 16 forms across multiple pages
- Impact: Cross-site request forgery attacks

Version Control System Exposure

- Location: /CVS/ directory structure
- Impact: Source code and development information disclosure

Information Leakage via Headers

- X-Powered-By: PHP version disclosure
- Impact: Technology stack enumeration for targeted attacks

5. TECHNICAL ANALYSIS

5.1 Network Security Posture

The target demonstrates a mixed security posture with aggressive perimeter filtering but significant application-layer vulnerabilities. The firewall configuration effectively limits attack surface by filtering 65,534 of 65,535 ports, demonstrating network-level security controls.

5.2 Web Application Security Assessment

The web application exhibits multiple critical security flaws consistent with an intentionally vulnerable testing platform. The combination of SQL injection vectors, information disclosure vulnerabilities, and policy misconfigurations presents substantial risk in any production environment.

5.3 Technology Stack Analysis

Identified Technologies:

- Operating System: Ubuntu 20.04 LTS
- Web Server: nginx 1.19.0
- Application Framework: PHP 5.6.40
- Cloud Infrastructure: Amazon Web Services
- Geographic Region: US-West-2

6. RISK ANALYSIS AND RECOMMENDATIONS

6.1 Immediate Actions Required

1. **Remove PHP Information Disclosure**
   - Action: Delete or restrict access to /secured/phpinfo.php
   - Timeline: Immediate
   - Priority: Critical
2. **Implement SQL Injection Prevention**
   - Action: Deploy parameterized queries across all database interactions
   - Timeline: Immediate
   - Priority: Critical
3. **Configure Restrictive Cross-Domain Policies**
   - Action: Replace wildcard permissions with specific domain allowlists
   - Timeline: Immediate
   - Priority: Critical

6.2 Security Improvements

1. **Deploy Security Headers**
   - Implement X-Frame-Options, X-Content-Type-Options
   - Configure Content Security Policy (CSP)
   - Timeline: Within 30 days
2. **Remove Sensitive File Exposures**
   - Relocate or delete FTP logs and CVS directories
   - Implement access controls for administrative directories
   - Timeline: Within 7 days
3. **Implement CSRF Protection**
   - Deploy anti-CSRF tokens across all forms

- Validate referrer headers for sensitive operations
- Timeline: Within 30 days

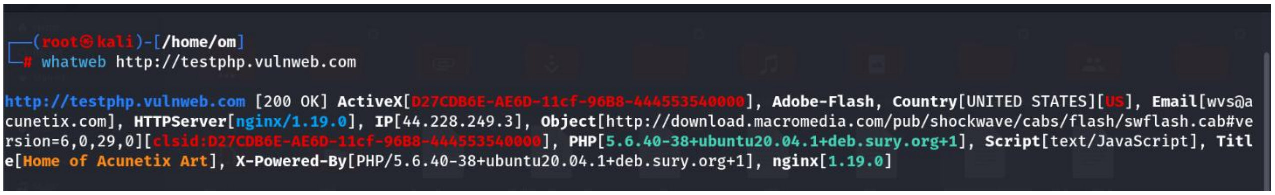
6.3 Long-term Security Strategy

1. **Regular Vulnerability Assessments**
    - Implement quarterly security testing
    - Deploy automated vulnerability scanning
2. **Security Header Hardening**
    - Implement comprehensive HTTP security headers
    - Configure server signature suppression
3. **Access Control Enhancement**
    - Implement role-based access controls
    - Deploy multi-factor authentication for administrative interfaces

7. WEB TECHNOLOGY FINGERPRINTING ANALYSIS

7.1 Technology Stack IdentificationWebTechnologyDetection.txt

WhatWeb Scan Results:



```
┌──(root㉿kali)-[/home/om]
└─# whatweb http://testphp.vulnweb.com

http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@a
cunetix.com], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#ve
rsion=6,0,29,0][clsid:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Titl
e[Home of Acunetix Art], X-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
```

7.2 Detailed Technology Analysis

Web Server Technology:

- **Server Software:** nginx 1.19.0
- **Architecture:** Reverse proxy configuration
- **Release Date:** nginx 1.19.0 released May 2020
- **Security Assessment:** Moderately recent version with known security patcheskali+1

Backend Application Framework:

- **Language:** PHP 5.6.40-38
- **Distribution:** Ubuntu 20.04.1 package via Ondřej Surý's repository
- **Version Status: CRITICAL** - PHP 5.6 reached End-of-Life in December 2018
- **Security Impact:** No official security updates since 2018, multiple known vulnerabilities

Server Infrastructure:

- **Geographic Location:** United States
- **Cloud Provider:** Amazon Web Services (inferred from DNS record)
- **Response Code:** 200 OK (successful HTTP response)
- **IP Address:** 44.228.249.3 (AWS US-West-2 region)

7.3 Security Implications of Technology Stack

High Risk Components:

PHP 5.6.40 End-of-Life Status:

- **Risk Level:** Critical
- **Issue:** Unsupported PHP version with no security patches
- **CVE References:** Multiple post-2018 vulnerabilities affect PHP 5.6.x
- **Impact:** Complete application compromise potential

Information Disclosure via Headers:

- **X-Powered-By Header:** Reveals exact PHP version
- **Risk Level:** Medium
- **Impact:** Facilitates targeted attacks based on known PHP 5.6 vulnerabilities
- **Recommendation:** Configure server to suppress version information

7.4 Technology Fingerprinting Assessment

Detection Accuracy:

- **WhatWeb Plugin Coverage:** Over 1800 plugins utilizedgithub
- **Detection Method:** HTTP header analysis and response fingerprinting
- **Certainty Level:** High confidence identification
- **Additional Technologies:** Adobe Flash support detected via policy files

Framework and CMS Analysis:

- **Content Management System:** None detected (custom PHP application)
- **JavaScript Libraries:** Not identified in basic scan
- **Database Backend:** Likely MySQL (inferred from PHP/nginx stack)
- **Additional Frameworks:** None explicitly identified

7.5 Compliance and Patch Management Assessment

Software Lifecycle Status:

- **nginx 1.19.0:** Stable branch, security updates available
- **PHP 5.6.40: Unsupported** - 6+ years beyond End-of-Life
- **Ubuntu 20.04:** Long Term Support through April 2025

Recommended Actions:

1. **Immediate:** Upgrade PHP to supported version (PHP 8.1+ recommended)
2. **Short-term:** Update nginx to latest stable version
3. **Long-term:** Implement automated patch management system

Compliance Impact:

- **PCI DSS:** Non-compliant due to unsupported PHP version
- **Security Frameworks:** Fails NIST Cybersecurity Framework requirements
- **Industry Standards:** Does not meet secure development lifecycle requirements

---

8. CONCLUSION

The active reconnaissance assessment successfully identified comprehensive attack surface information for testphp.vulnweb.com. As an intentionally vulnerable educational platform, the target demonstrated expected security weaknesses including critical SQL injection vulnerabilities, information disclosure issues, and policy misconfigurations.

The assessment methodology proved effective in identifying both network-level and application-level security issues. The comprehensive enumeration revealed significant attack vectors that would require immediate attention in a production environment.

For educational purposes, these findings provide valuable learning opportunities for understanding web application security assessment techniques and vulnerability identification processes.

9. APPENDICES

Appendix A: Command Reference

```
# Host Discovery
nmap -sn testphp.vulnweb.com

# Port Enumeration
nmap -sS testphp.vulnweb.com
nmap -sV -p 22,80,443 -sC testphp.vulnweb.com
nmap -sV -p- -sC -T4 testphp.vulnweb.com

# OS Detection
nmap -O --osscan-guess testphp.vulnweb.com

# Vulnerability Scanning
nmap --script vuln testphp.vulnweb.com

# Directory Enumeration
dirb http://testphp.vulnweb.com

# Web Application Analysis
nikto -h http://testphp.vulnweb.com -o nikto_report.txt
whatweb http://testphp.vulnweb.com
```

Appendix B: Tool Output Files

- Host Discovery: namoSN.txt
- SYN Scan Results: nampSS.txt
- Service Detection: Service-Version.txt
- Full Port Scan: Full-Port-Scan-with-NSE-Scripts.txt
- OS Detection: OS.txt
- Vulnerability Assessment: VulnerabilityScanning.txt
- Directory Enumeration: Basic-Directory-Brute-force.txt
- Web Vulnerability Scan: nikto_report.txt
- Technology Detection: WebTechnologyDetection.txt

Appendix C: Scope and Limitations

Testing Scope:

- Single target assessment (testphp.vulnweb.com)
- Network and application layer enumeration
- Automated vulnerability identification
- Non-invasive reconnaissance techniques