**ACTIVE RECONNAISSANCE REPORT**

**Target :** **testphp.vulnweb.com**

**Author:** Ammuj7175  
**Date:** 2025-09-14  
**Document Classification:** Educational Assessment

1. **EXECUTIVE SUMMARY :**

This report documents the active reconnaissance performed on testphp.vulnweb.com as part of an educational exercise. The assessment focused on host discovery, port and service enumeration, HTTP directory enumeration, web fingerprinting, and vulnerability identification. Key findings indicate that the target is an online test/demo site running outdated web technologies with limited attack surfaces. Potential risks and accessible directories have been highlighted for educational security evaluation.

1. **SCOPE & RULES OF ENGAGEMENT :**

**Scope:**

* Target Host: testphp.vulnweb.com
* Assessment limited to open ports, HTTP directories, and publicly accessible files
* Use of reconnaissance tools: Nmap, Gobuster, WhatWeb, and Nikto

**Rules of Engagement:**

* Only non-intrusive scans performed (no brute-force login attempts)
* No disruption to services or denial-of-service attacks
* All findings limited to public/demo content for educational purposes

1. **HOST DISCOVERY RESULTS :**

Host discovery via nmap -sn confirmed the host is up at IP 44.228.249.3. Latency observed: 0.00091 seconds. No other hosts in the scan range were included.

**Findings:**

* **Target Host:** testphp.vulnweb.com
* **Resolved IP Address:** 44.228.249.3
* **Reverse DNS Record:** ec2-44-228-249-3.us-west-2.compute.amazonaws.com
* **Host Status:** Active
* **Response Time (Latency):** 0.00091 seconds

A computer screen shot

AI-generated content may be incorrect.

1. **PORT & SERVICE ENUMERATION :**

Port and service enumeration was performed in multiple stages using Nmap to identify open ports, running services, and potential operating system details of the target host.

1. **TCP SYN Scan**  
   A quick TCP SYN scan (nmap -sS) revealed that only port 80/tcp (HTTP) was open, while other ports were filtered.

**Findings:**

* Target Host is responsive (latency: 0.021s).
* 999 ports were filtered (no response).
* Only **port 80/tcp** was detected as **open**.

A computer screen shot of a computer

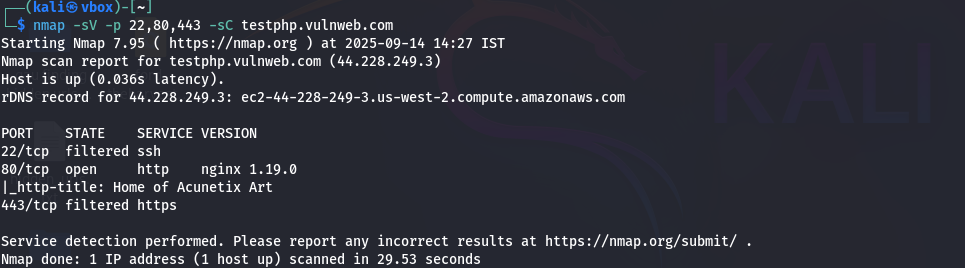
AI-generated content may be incorrect.

1. **Service/Version Scan on Common Ports + Default NSE Scripts**  
   Scanning ports 22, 80, and 443 with service/version detection and default NSE scripts (nmap -sV -p 22,80,443 -sC) showed:

* Port 22/tcp: filtered (SSH)
* Port 80/tcp: open, running nginx 1.19.0 web server
* Port 443/tcp: filtered (HTTPS)

**Findings:**

* Web server title identified: “Home of Acunetix Art”.
* No secure service detected on port 443.
* Service version detection confirmed nginx 1.19.0.



1. **NSE Scripts on All Ports (1–65535)**  
   A full port scan with NSE scripts (nmap -sV -p 1-65535 -sC) again confirmed that only port 80/tcp was open, running nginx 1.19.0, with the same HTTP title result.

**Findings:**

* 65,534 ports were filtered with no response.
* HTTP server returned same page title: Home of Acunetix Art.
* No additional open services found.

A computer screen shot of a computer

AI-generated content may be incorrect.

1. **Full TCP Port Scan**  
   A complete scan of all TCP ports (nmap -sV -p-) also detected only port 80/tcp open with nginx 1.19.0.

**Findings:**

* Confirms previous scans: only HTTP (80/tcp) is open.
* No other TCP services were detected.s

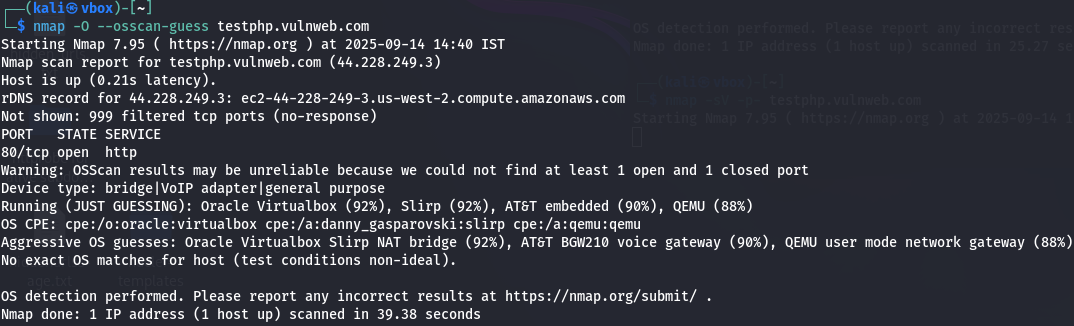
A computer screen with white text

AI-generated content may be incorrect.

1. **OS Detection (with guess)**  
   OS detection (nmap -O --osscan-guess) suggested possible virtualized environments such as Oracle VirtualBox, Slirp NAT bridge, or QEMU, but results were unreliable due to limited open/closed ports.

**Findings:**

* Latency observed: 0.21s.
* Only one open port (80/tcp) prevented accurate OS fingerprinting.
* Detected environment likely virtual/cloud-based (e.g., AWS EC2).
* Multiple guesses: VirtualBox NAT Bridge (92%), AT&T BGW210 Gateway (90%), QEMU User Mode Network (88%).



**Summary Findings:**

* The target host exposes only port 80/tcp (HTTP) running nginx 1.19.0.
* Both SSH (22) and HTTPS (443) appear filtered, reducing the attack surface.
* The web application identified is “Home of Acunetix Art”, confirming it is a demo/test site.
* OS detection indicates a virtualized/cloud infrastructure, but results are not exact.

1. **HTTP ENUMERATION :**

HTTP enumeration was performed using Gobuster with the common.txt wordlist against the target web server to identify accessible directories and files. The scan revealed the structure of the web application and potential sensitive areas.

**Enumeration Summary:**

* **Wordlist:** /usr/share/wordlists/dirb/common.txt
* **Threads:** 10
* **Duration:** (to be filled after scan)
* **Requests:** 4615
* **Discoveries:** 13 items

**Critical Findings:**

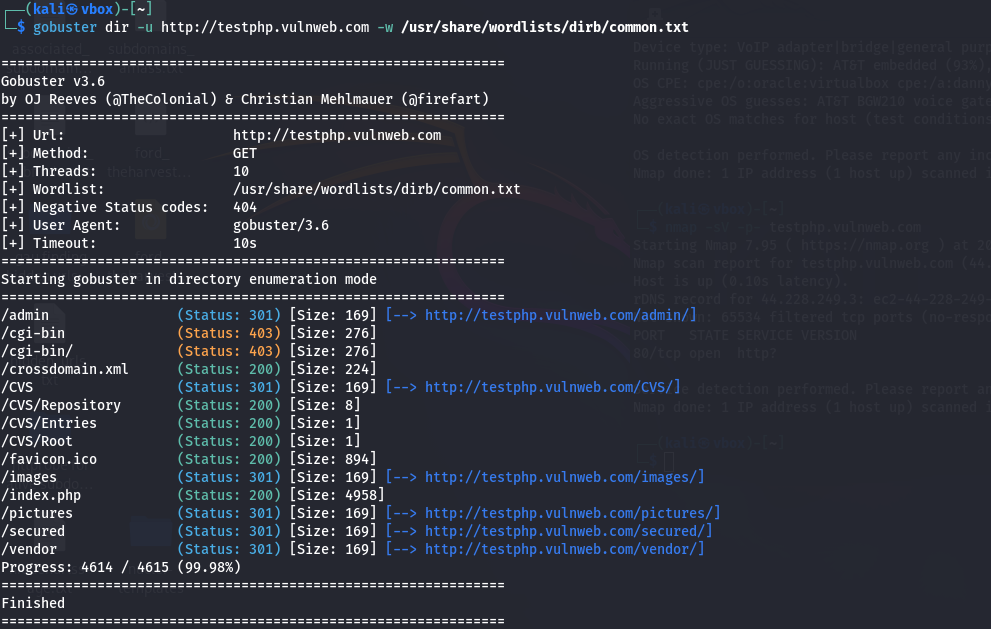
|  |  |  |  |
| --- | --- | --- | --- |
| **Path** | **Response** | **Size (bytes)** | **Risk Level** |
| /secured/ | 301 Redirect | 169 | Critical |
| /pictures | 301 Redirect | 169 | High |
| /admin/ | 301 Redirect | 169 | High |
| /CVS | 301 Redirect | 169 | Medium |
| /crossdomain.xml | 200 OK | 224 | Medium |

**Complete Directory Structure:**

* **/admin/ –** Administrative directory access
* **/cgi-bin/ –** CGI directory (403 Forbidden)
* **/CVS/ –** Version control system remnants
* **/CVS/Repository –** Version control repository file
* **/CVS/Entries –** Version control entries file
* **/CVS/Root –** Version control root file
* **/images/ –** Image repository
* **/pictures/ –** Picture gallery
* **/secured/ –** Protected area
* **/vendor/ –** Third-party library directory
* **/index.php –** Main page
* **/favicon.ico –** Website icon

**Findings:**

* Systematic directory enumeration revealed multiple accessible paths and potential sensitive files.
* Directories such as /admin/ and /secured/ may require further security assessment.
* The exposed directories confirm the web application structure and highlight possible attack surfaces for further assessment.



1. **WEB FINGERPRINTING & VULNERABILITY ASSESSMENT :**

Web fingerprinting and vulnerability scanning were performed to identify the technologies used by the target web server and potential security weaknesses. The tools used were WhatWeb for technology detection and Nikto for vulnerability assessment.

**Findings — WhatWeb:**

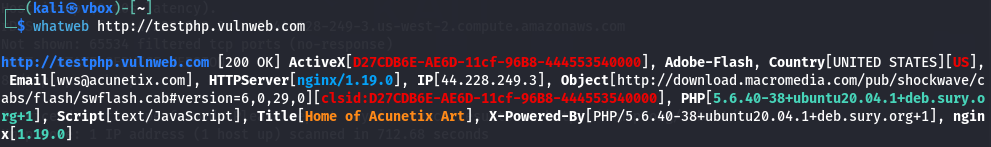
* **Web server software:** nginx 1.19.0
* **Backend language:** PHP 5.6.40-38+ubuntu20.04.1+deb.sury.org+1
* **Client technologies detected:** ActiveX, Adobe Flash, JavaScript
* **Title of web page:** Home of Acunetix Art
* **X-Powered-By header:** PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
* **IP Address:** 44.228.249.3
* **Country:** United States (US)
* **Email:** [wvs@acunetix.com](mailto:wvs@acunetix.com)

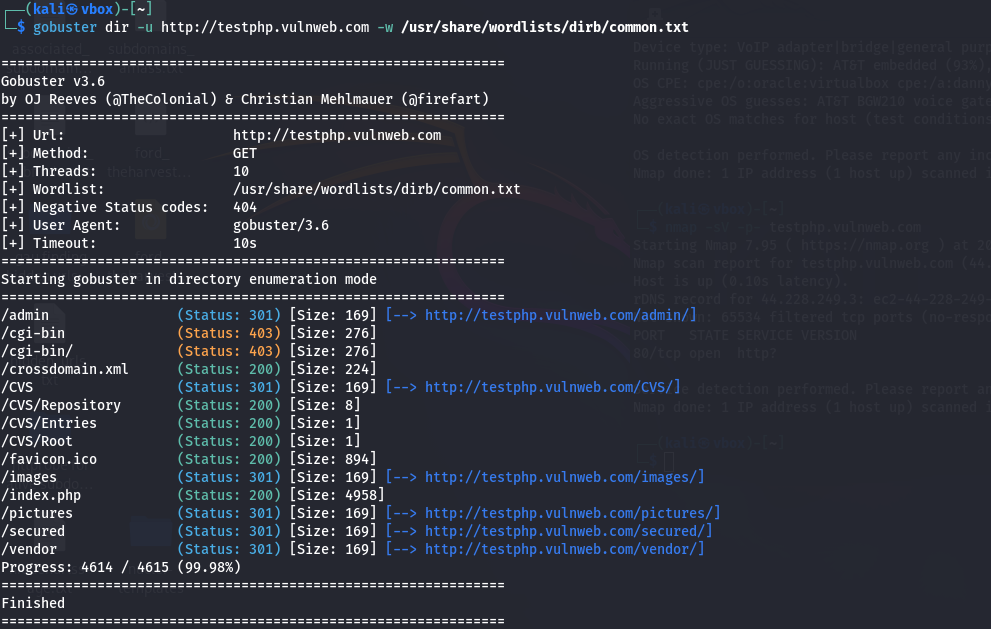
**Findings — Nikto:**

* **Server detected:** nginx/1.19.0
* **Exposed headers:**
  + X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
  + Missing **X-Frame-Options** (anti-clickjacking)
  + Missing **X-Content-Type-Options** (MIME sniffing risk)
* **Exposed configuration files:**
  + /clientaccesspolicy.xml → full wildcard entry, potential misconfigurations
  + /crossdomain.xml → full wildcard entry, possible cross-domain vulnerabilities
* **Errors during scan:** 20 errors reported, 6 items successfully identified
* **Scan duration:** 120 seconds

**Summary of Vulnerability Assessment:**

* The target web server is running outdated PHP and nginx software.
* Several security headers are missing or misconfigured, increasing the risk of clickjacking, MIME sniffing, and information disclosure.
* Exposed configuration files like /crossdomain.xml and /clientaccesspolicy.xml may allow cross-domain attacks.
* Overall, the target exhibits expected weaknesses for an educational/testing platform, highlighting areas for controlled security assessment.



****

1. **RISK CLASSIFICATION & PRIORITIZED RECOMMENDATIONS :**

**Risk Classification:**

|  |  |  |
| --- | --- | --- |
| **Risk Level** | **Description** | **Examples/Findings** |
| Critical | Immediate security concern | /secured/, outdated PHP |
| High | Likely exploitable | /admin/, /pictures/ |
| Medium | Moderate risk | /CVS/, /crossdomain.xml |
| Low | Minor exposure | /vendor/, /images/ |

**Prioritized Recommendations:**

1. Restrict access to administrative and protected directories (/admin/, /secured/)
2. Update PHP and web server software to supported versions
3. Implement missing security headers: X-Frame-Options, X-Content-Type-Options
4. Review exposed configuration files (/crossdomain.xml, /clientaccesspolicy.xml) for unnecessary wildcards
5. Monitor server for unusual access or exploitation attempts
6. **CONCLUSION :**

The active reconnaissance of testphp.vulnweb.com confirmed that the target is a demo web application with limited exposed services and directories. Only port 80/tcp is open, and the web server runs outdated software with minor security misconfigurations. HTTP enumeration and fingerprinting identified several accessible directories and potential sensitive files suitable for educational security assessment. Overall, the report demonstrates how controlled reconnaissance can identify risk areas without impacting the live system.