

Active Recon & Automated Web Scanning Report

Intern Details

Name: Ankit Vishwakarma

Assignment: Cyber Security Internship

Task Title: Web Application Scanning: Automated Vulnerability Discovery

Target Information

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

Target Type: Public Vulnerable Web Application

Scope Status: Explicitly allowed for security testing

Step 1 — Recon & Discovery

Nmap Host Discovery:

```
[~] (alfa㉿kali)-[~]
$ nmap -sn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 15:27 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 0.12 seconds
```

Command: **nmap -sn testphp.vulnweb.com**

Result: **Host alive**

Quick Scan:

```
[~] (alfa㉿kali)-[~]
$ nmap -sS testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 16:05 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.017s 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 15.37 seconds
```

Command: **nmap -sS testphp.vulnweb.com**

Open Port: **80 (HTTP)**

Service Detection:

```
[~] (alfa㉿kali)-[~]
$ nmap -sV -p 80 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 16:05 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.0010s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT      STATE SERVICE VERSION
80/tcp    filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

Command: **nmap -sV -p 80 testphp.vulnweb.com**

Service: Apache httpd

Web Fingerprinting

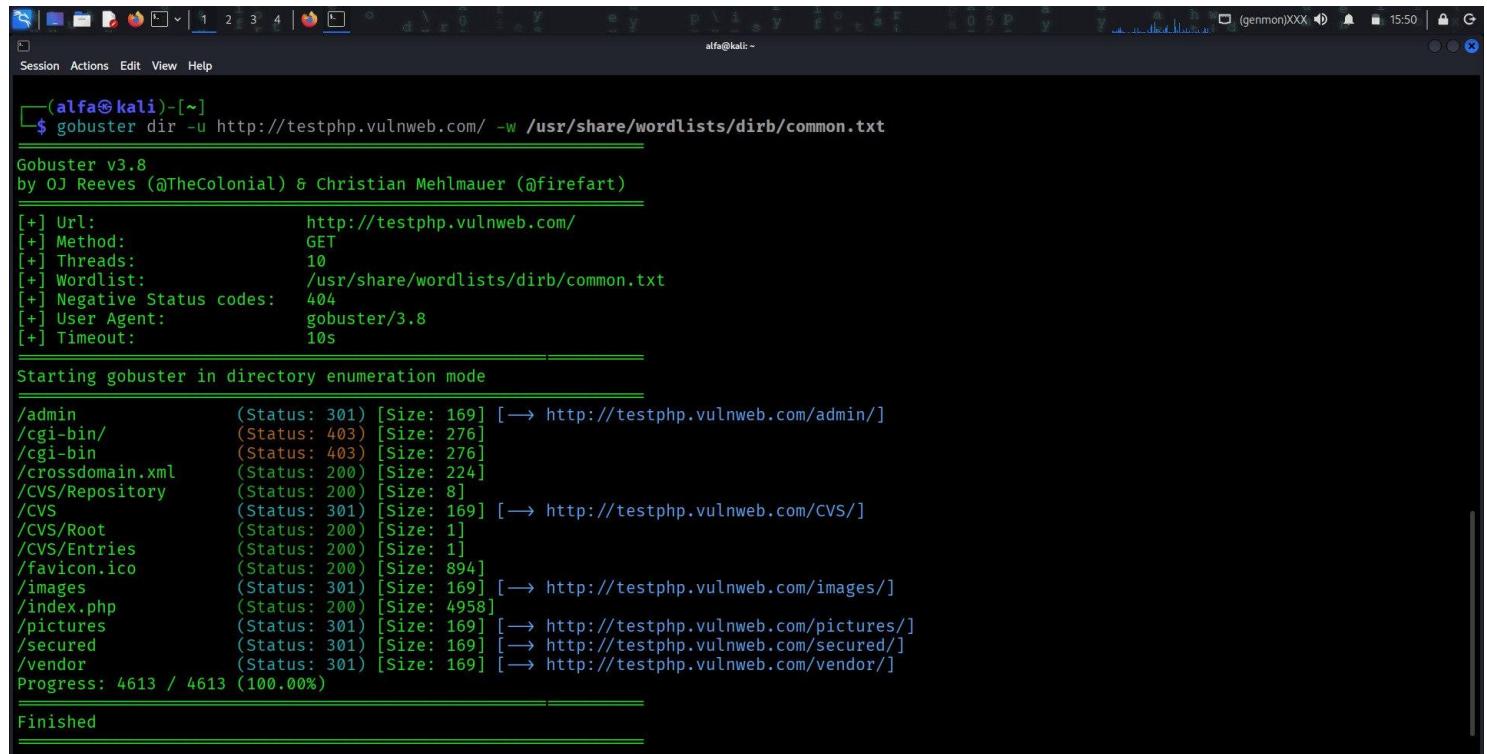
WhatWeb Scan:

```
[~] (alfa㉿kali)-[~]
$ whatweb testphp.vulnweb.com
http://testphp.vulnweb.com [200 OK] ActiveX[D27CDB6E-AE6D-11cf-96B8-444553540000], Adobe-Flash, Country[UNITED STATES][US], Email[wvs@acunetix.co
m], HTTPServer[nginx/1.19.0], IP[44.228.249.3], Object[http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6.0,29,0][clsi
d:D27CDB6E-AE6D-11cf-96B8-444553540000], PHP[5.6.40-38+ubuntu20.04.1+deb.sury.org+1], Script[text/JavaScript], Title[Home of Acunetix Art], X-Pow
ered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]
ERROR Opening: https://testphp.vulnweb.com - execution expired
```

Command: **whatweb testphp.vulnweb.com**

Technologies: **HTTPServer, PHP 5.6.40-38 + Ubuntu20.04.1, nginx/1.19.0**

Directory Enumeration



```
[~] (alfa㉿kali)-[~]
$ gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://testphp.vulnweb.com/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.8
[+] Timeout:      10s
Starting gobuster in directory enumeration mode
=====
/admin           (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/admin/]
/cgi-bin/        (Status: 403) [Size: 276]
/cgi-bin         (Status: 403) [Size: 276]
/crossdomain.xml (Status: 200) [Size: 224]
/CSV/Repository  (Status: 200) [Size: 8]
/CSV             (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CSV/]
/CSV/Root        (Status: 200) [Size: 1]
/CSV/Entries     (Status: 200) [Size: 1]
/favicon.ico    (Status: 200) [Size: 894]
/images          (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/images/]
/index.php       (Status: 200) [Size: 4958]
/pictures        (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/pictures/]
/secured         (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/secured/]
/vendor          (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/vendor/]
Progress: 4613 / 4613 (100.00%)
=====
Finished
```

Command:

gobuster dir -u http://testphp.vulnweb.com/ -w /usr/share/wordlists/dirb/common.txt

Important Directories: **admin/, images/, pictures/**

Light Automated Scans

Nikto Scan:

```
(alfa㉿kali)-[~]
$ nikto -h http://testphp.vulnweb.com -output nikto.txt
- Nikto v2.5.0
=====
+ Target IP:          44.228.249.3
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2025-11-30 15:50:46 (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:           2025-11-30 15:52:32 (GMT5.5) (106 seconds)

+ 1 host(s) tested
```

Command: **nikto -h http://testphp.vulnweb.com -output nikto.txt**

Findings: Outdated software, missing headers, phpinfo exposed.

Nuclei Scan:

```
[INF] Your current nuclei-templates v10.3.3 are outdated. Latest is v10.3.4
[INF] Successfully updated nuclei-templates (v10.3.4) to /home/alfa/.local/nuclei-templates. GoodLuck!

Nuclei Templates v10.3.4 Changelog


| TOTAL | ADDED | MODIFIED | REMOVED |
|-------|-------|----------|---------|
| 12    | 1     | 11       | 0       |


[WRN] Found 1 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v3.4.10 (outdated)
[INF] Current nuclei-templates version: v10.3.4 (latest)
[INF] New templates added in latest release: 0
[INF] Templates loaded for current scan: 8855
[INF] Executing 8853 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 2 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Automatic scan tech-detect: Templates clustered: 496 (Reduced 470 Requests)
[INF] Executing Automatic scan on 1 target[s]
[nginx-version] [http] [info] http://testphp.vulnweb.com ["nginx/1.19.0"]
[php-detect] [http] [info] http://testphp.vulnweb.com ["5.6.40"]
[tech-detect:dreamweaver] [http] [info] http://testphp.vulnweb.com
[tech-detect:nginx] [http] [info] http://testphp.vulnweb.com
[tech-detect:php] [http] [info] http://testphp.vulnweb.com
[waf-detect:nginxgeneric] [http] [info] http://testphp.vulnweb.com
[INF] Found 5 tags and 4 matches on detection templates on http://testphp.vulnweb.com [wappalyzer: 4, detection: 6]
[INF] Executing 70 templates on http://testphp.vulnweb.com
[INF] Using Interactsh Server: oast.site
[nginx-version] [http] [info] http://testphp.vulnweb.com ["nginx/1.19.0"]
[php-detect] [http] [info] http://testphp.vulnweb.com ["5.6.40"]
[INF] Scan completed in 3m. 8 matches found.
```

Command: nuclei -u http://testphp.vulnweb.com -as -o nuclei.txt -c 10

Findings: Header issues, outdated components, possible SQL injection points.

ZAP Scan:

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size	Resp. Header	Size	Resp. Body
234	30/11/25, 4:47:20 pm	30/11/25, 4:47:20 pm	GET	http://testphp.vulnweb.com/favicon.ico	200	OK	511 ms	241 bytes		894 bytes	
235	30/11/25, 4:47:23 pm	30/11/25, 4:47:23 pm	GET	http://testphp.vulnweb.com/secured/newuser.php?n...	200	OK	248 ms	221 bytes		415 bytes	
236	30/11/25, 4:47:24 pm	30/11/25, 4:47:24 pm	GET	http://testphp.vulnweb.com/cart.php	200	OK	460 ms	222 bytes		4,903 bytes	
237	30/11/25, 4:47:25 pm	30/11/25, 4:47:25 pm	GET	http://testphp.vulnweb.com/style.css	200	OK	487 ms	239 bytes		5,482 bytes	
238	30/11/25, 4:47:25 pm	30/11/25, 4:47:26 pm	GET	http://testphp.vulnweb.com/images/logo.gif	200	OK	240 ms	240 bytes		6,660 bytes	
239	30/11/25, 4:47:26 pm	30/11/25, 4:47:26 pm	GET	http://testphp.vulnweb.com/favicon.ico	200	OK	235 ms	241 bytes		894 bytes	
240	30/11/25, 4:47:27 pm	30/11/25, 4:47:27 pm	POST	http://testphp.vulnweb.com/search.php?test=query	200	OK	242 ms	222 bytes		2,442 bytes	
241	30/11/25, 4:47:27 pm	30/11/25, 4:47:27 pm	GET	http://testphp.vulnweb.com/userinfo.php	200	OK	512 ms	222 bytes		5,523 bytes	
242	30/11/25, 4:47:28 pm	30/11/25, 4:47:28 pm	POST	http://testphp.vulnweb.com/search.php?test=query	200	OK	478 ms	222 bytes		2,442 bytes	
243	30/11/25, 4:47:29 pm	30/11/25, 4:47:29 pm	GET	http://testphp.vulnweb.com/style.css	200	OK	476 ms	239 bytes		5,482 bytes	
244	30/11/25, 4:47:29 pm	30/11/25, 4:47:29 pm	GET	http://testphp.vulnweb.com/images/logo.gif	200	OK	237 ms	240 bytes		6,660 bytes	
247	30/11/25, 4:47:31 pm	30/11/25, 4:47:31 pm	GET	http://testphp.vulnweb.com/AJAX	301	Moved Permanent...	237 ms	207 bytes		169 bytes	
248	30/11/25, 4:47:31 pm	30/11/25, 4:47:31 pm	GET	http://testphp.vulnweb.com/	200	OK	465 ms	222 bytes		4,958 bytes	
249	30/11/25, 4:47:32 pm	30/11/25, 4:47:32 pm	GET	http://testphp.vulnweb.com/AJAX	200	OK	393 ms	222 bytes		4,236 bytes	
250	30/11/25, 4:47:33 pm	30/11/25, 4:47:34 pm	GET	http://testphp.vulnweb.com/styles.css	404	Not Found	470 ms	155 bytes		153 bytes	
251	30/11/25, 4:47:35 pm	30/11/25, 4:47:35 pm	POST	http://testphp.vulnweb.com/search.php?test=query	200	OK	237 ms	222 bytes		2,442 bytes	
253	30/11/25, 4:47:37 pm	30/11/25, 4:47:38 pm	POST	http://testphp.vulnweb.com/search.php?test=query	200	OK	486 ms	222 bytes		2,442 bytes	
254	30/11/25, 4:47:38 pm	30/11/25, 4:47:38 pm	GET	http://testphp.vulnweb.com/AJAX/index.php	200	OK	464 ms	222 bytes		4,236 bytes	
256	30/11/25, 4:47:39 pm	30/11/25, 4:47:40 pm	GET	http://testphp.vulnweb.com/AJAX/styles.css	200	OK	498 ms	237 bytes		562 bytes	
257	30/11/25, 4:47:40 pm	30/11/25, 4:47:40 pm	GET	http://testphp.vulnweb.com/Flash	301	Moved Permanent...	253 ms	208 bytes		169 bytes	
258	30/11/25, 4:47:40 pm	30/11/25, 4:47:40 pm	POST	http://testphp.vulnweb.com/userinfo.php	200	OK	493 ms	221 bytes		233 bytes	
259	30/11/25, 4:47:40 pm	30/11/25, 4:47:41 pm	GET	http://testphp.vulnweb.com/AJAX/styles.css	200	OK	492 ms	237 bytes		562 bytes	
260	30/11/25, 4:47:43 pm	30/11/25, 4:47:43 pm	GET	http://testphp.vulnweb.com/Userinfo.php?name=abc	200	OK	259 ms	222 bytes		5,523 bytes	

Note: Scan report uploaded in Assignment-5 repository with this report.

Findings:

- Missing Critical Security Headers (High Risk)**
- Information Disclosure – Server Fingerprinting (Medium Risk)**
- Lack of HTTPS / HSTS Enforcement (High Risk)**
- Directory and Endpoint Exposure (Medium Risk)**
- Outdated Frontend Libraries (Medium Risk)**
- Cookie Misconfiguration (Medium – High Risk).**

Conclusion

This assignment improved practical skills in reconnaissance, scanning, fingerprinting, directory enumeration, and vulnerability identification using multiple industry tools such as Nmap, Nikto, Dirb, gobuster, Nuclei, and OWASP ZAP.