

# Assignment: Web Application Scanning - Automated Vulnerability Discovery

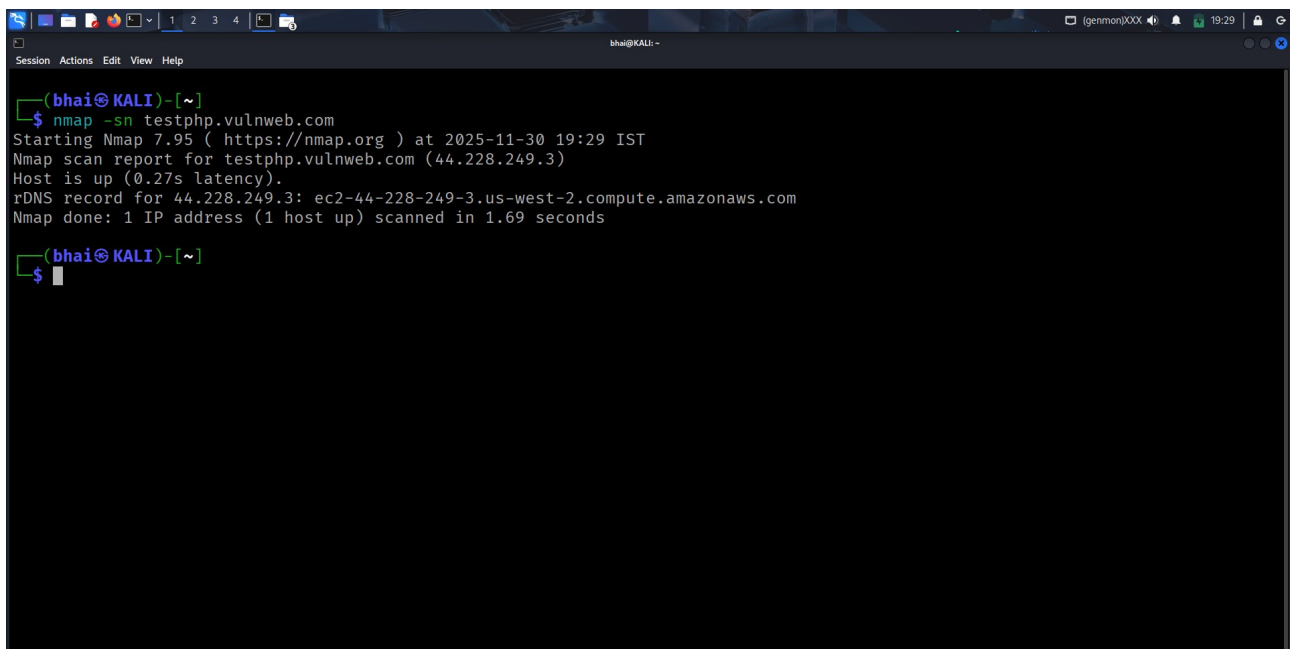
---

## ◆ Step 1 — Recon & Discovery

### 1. Host Discovery

#### Command

```
nmap -sn testphp.vulnweb.com
```

A screenshot of a terminal window on a Kali Linux system. The terminal shows the execution of the command 'nmap -sn testphp.vulnweb.com'. The output indicates that the host is up and provides the IP address 44.228.249.3 and the rDNS record ec2-44-228-249-3.us-west-2.compute.amazonaws.com. The terminal window has a dark background with green and white text. The top of the window shows the title bar with 'bhai@KALI: ~' and some system icons on the right.

```
(bhai@KALI)-[~]  
$ nmap -sn testphp.vulnweb.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 19:29 IST  
Nmap scan report for testphp.vulnweb.com (44.228.249.3)  
Host is up (0.27s 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 1.69 seconds  
  
(bhai@KALI)-[~]  
$
```

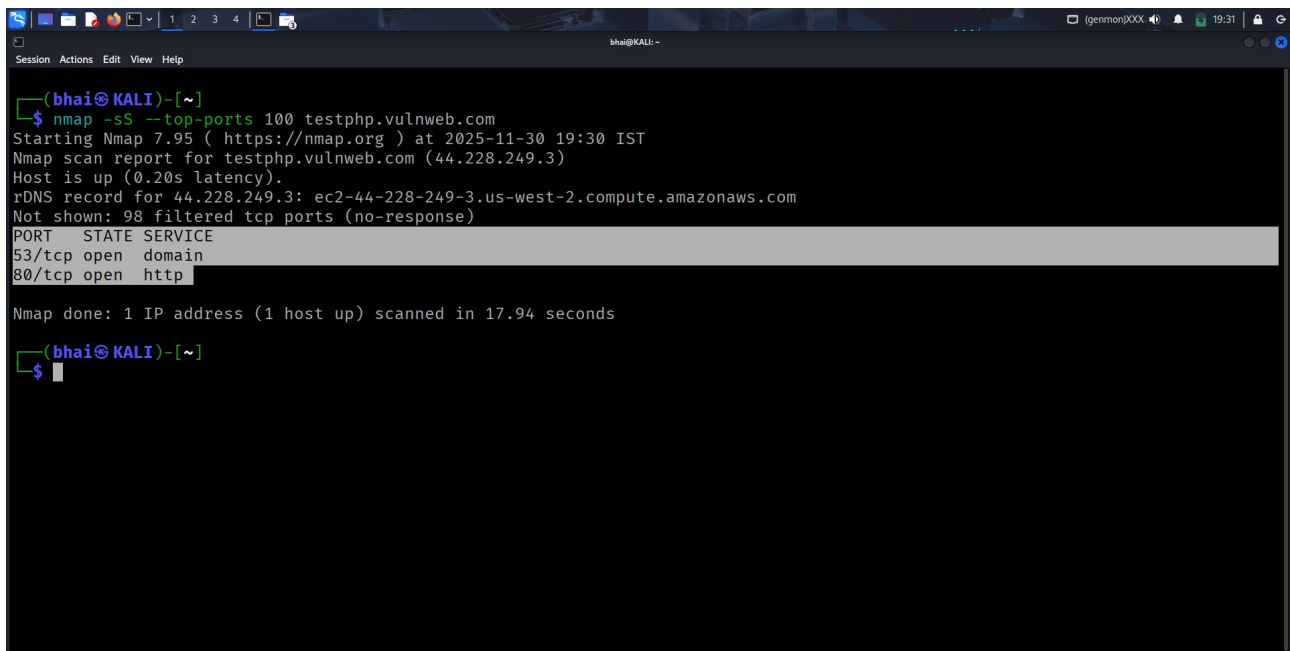
*Host discovery result.*

---

## 2. Port & Service Scan

### Command

```
nmap -sS --top-ports 100 testphp.vulnweb.com
```



```
(bhai@KALI)-[~]
$ nmap -sS --top-ports 100 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 19:30 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.20s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 98 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds

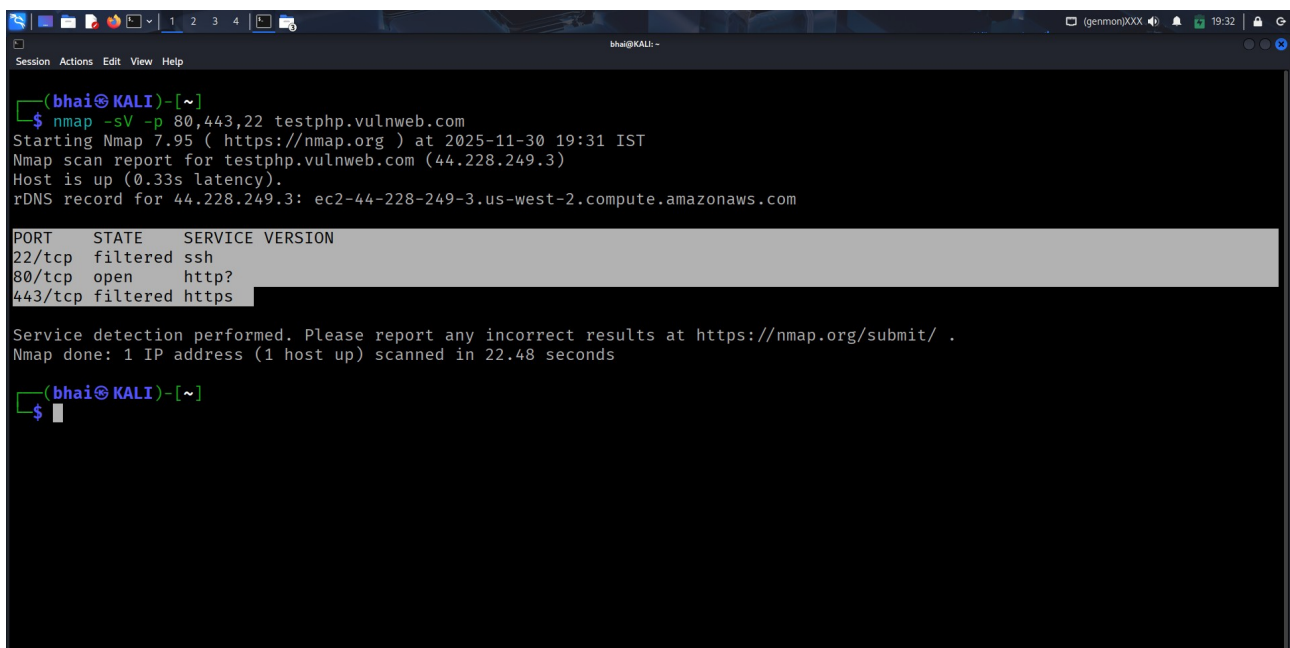
(bhai@KALI)-[~]
$
```

*Quick port scan result.*

---

### Command (Version detection on open ports)

```
nmap -sV -p 80,443,22 testphp.vulnweb.com
```



```
(bhai@KALI)-[~]
$ nmap -sV -p 80,443,22 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 19:31 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.33s 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?
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 22.48 seconds

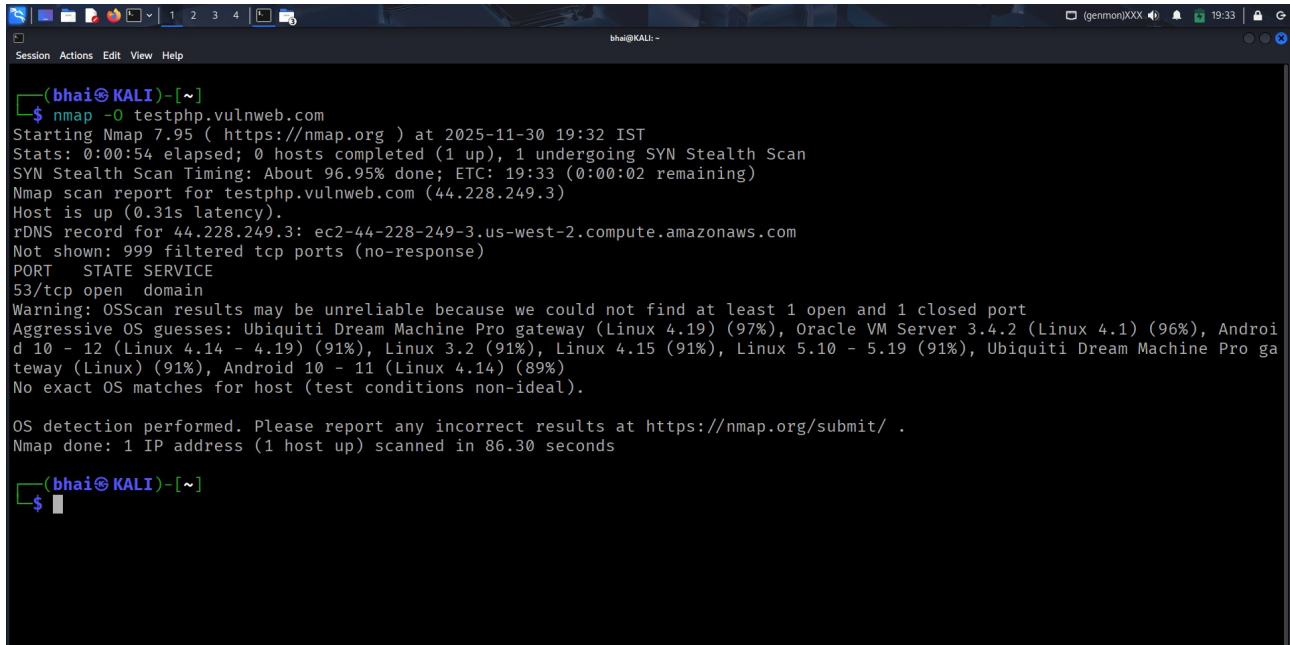
(bhai@KALI)-[~]
$
```

Service version scan.

---

## Command (OS detection)

`nmap -O testphp.vulnweb.com`



```
(bhai@KALI)-[~]
$ nmap -O testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 19:32 IST
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 96.95% done; ETC: 19:33 (0:00:02 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.31s 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
53/tcp    open  domain
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Ubiquiti Dream Machine Pro gateway (Linux 4.19) (97%), Oracle VM Server 3.4.2 (Linux 4.1) (96%), Android 10 - 12 (Linux 4.14 - 4.19) (91%), Linux 3.2 (91%), Linux 4.15 (91%), Linux 5.10 - 5.19 (91%), Ubiquiti Dream Machine Pro gateway (Linux) (91%), Android 10 - 11 (Linux 4.14) (89%)
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 86.30 seconds

(bhai@KALI)-[~]
$
```

OS detection output.

---

## ◆ Step 2 — Web Fingerprinting

### 1. WhatWeb

#### Command

whatweb <http://testphp.vulnweb.com>

```
Session Actions Edit View Help

(bhai@KALI)-[~]
$ 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@acunetix.com], 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][clsid: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-Powered-By[PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1], nginx[1.19.0]

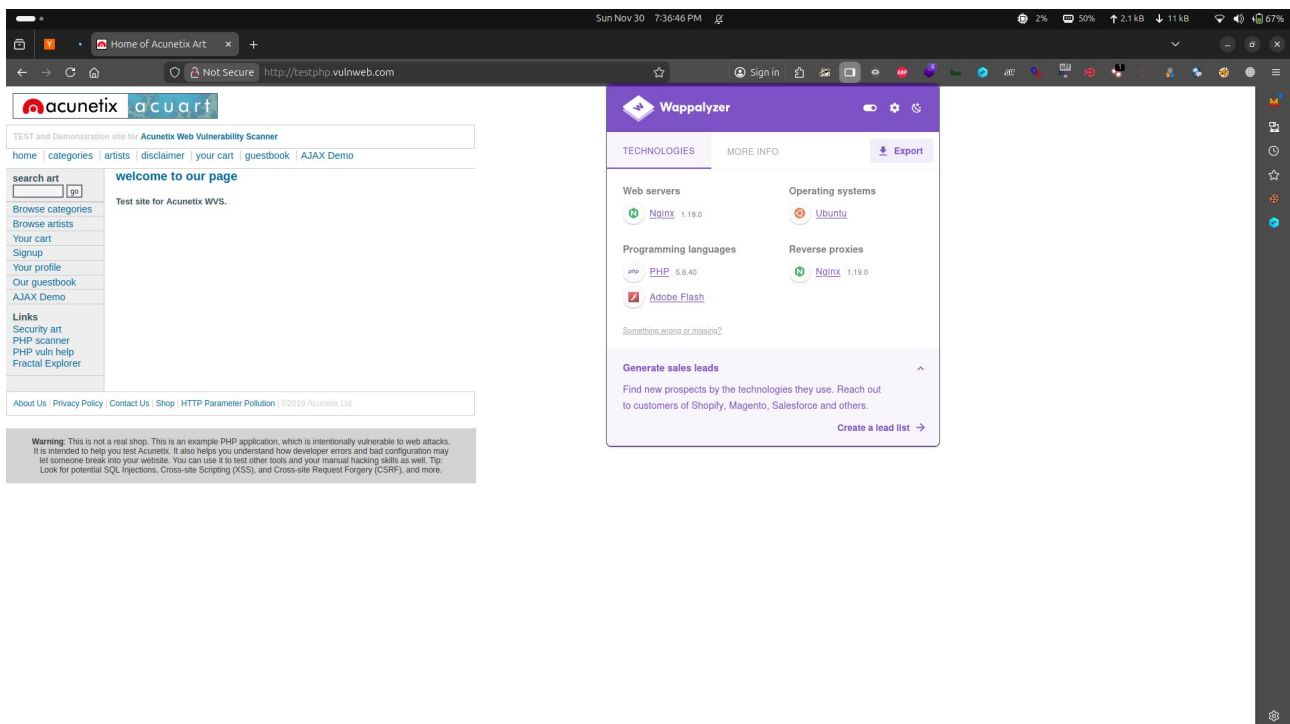
(bhai@KALI)-[~]
$
```

Web fingerprinting result.

## 2. Wappalyzer

Install Chrome/Firefox extension → open:

<http://testphp.vulnweb.com>



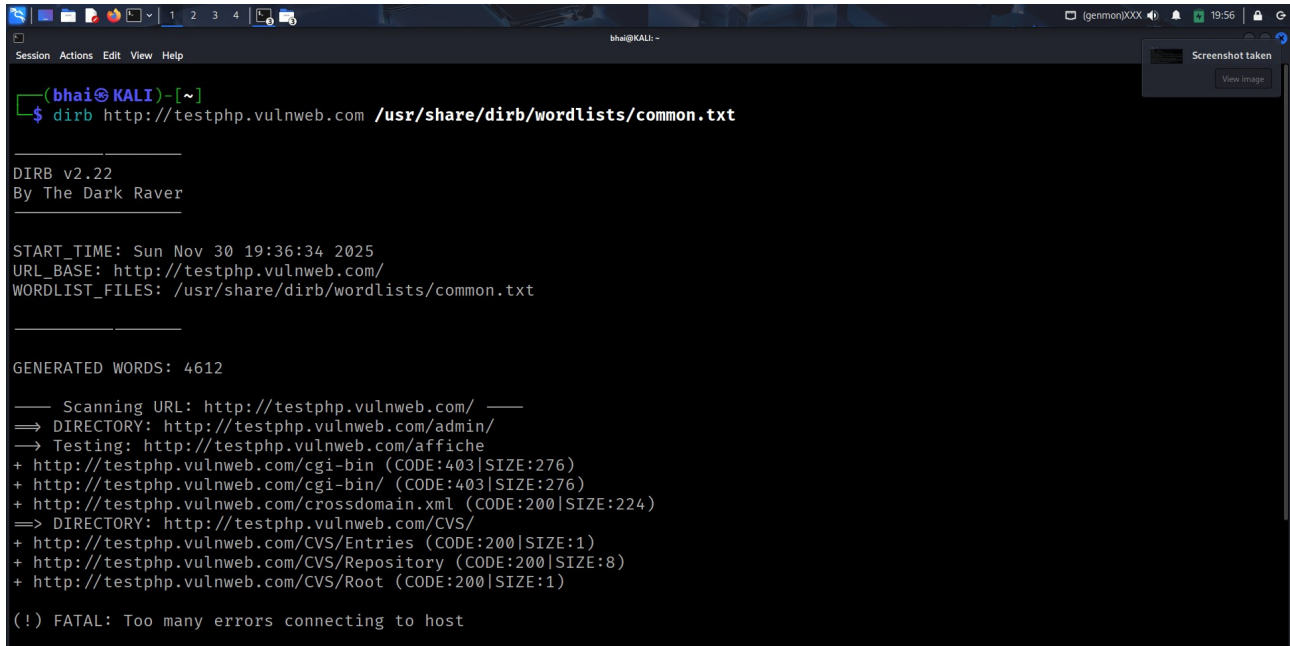
Wappalyzer tech detection.

# ◆ Step 3 — Directory Discovery

## Dirb

### Command

```
dirb http://testphp.vulnweb.com /usr/share/dirb/wordlists/common.txt
```



```
(bhai@KALI)-[~]
$ dirb http://testphp.vulnweb.com /usr/share/dirb/wordlists/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Sun Nov 30 19:36:34 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/
-> Testing: http://testphp.vulnweb.com/affiche
+ 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)

(!) FATAL: Too many errors connecting to host
```

*Directory brute-force results.*

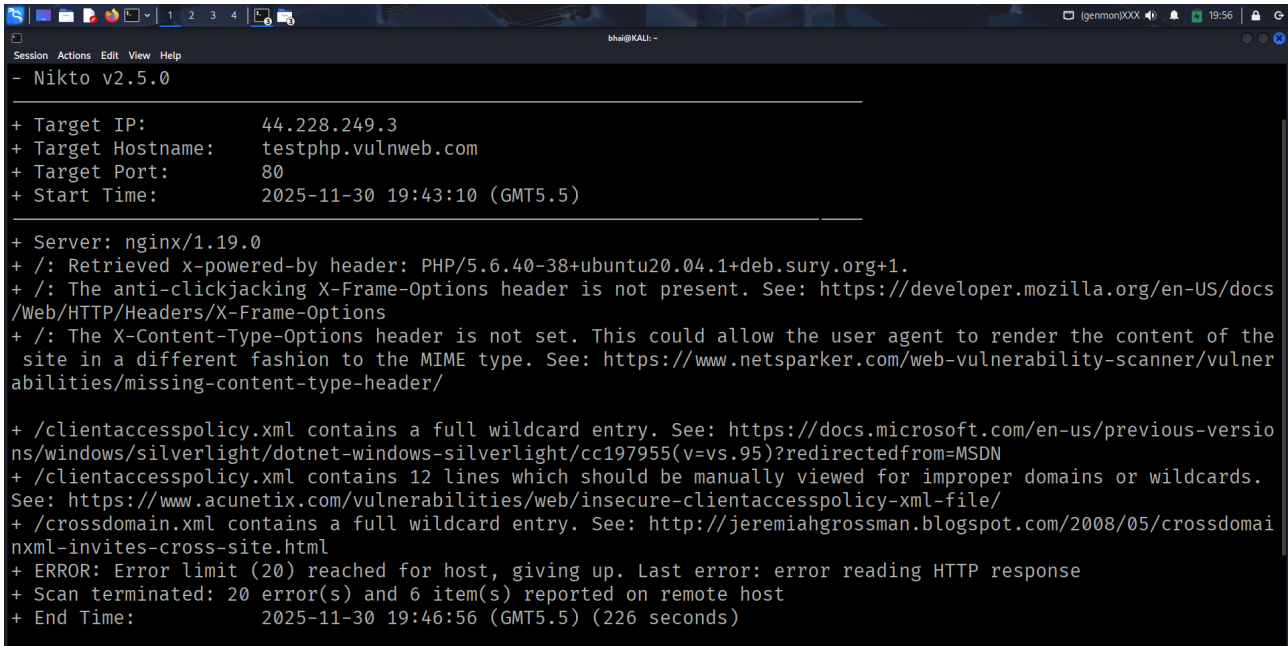
---

# ◆ Step 4 — Light Automated Scans

## 1. Nikto

### Command

```
nikto -h http://testphp.vulnweb.com -o 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 19:43:10 (GMT5.5)

+ Server: nginx/1.19.0
+ /: Retrieved x-powered-by header: PHP/5.6.40-38ubuntu20.04.1+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 19:46:56 (GMT5.5) (226 seconds)
```

*Nikto scan output.*

---

## 2. Nuclei

### Command

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

```
Session Actions Edit View Help
bhai@KALI: ~
(bhai@KALI)-[~]
$ nuclei -u http://testphp.vulnweb.com -as -o nuclei.txt -c 10

  _____
 /  _  _  _  \
|  _ \| | | | |
| |_) | | | | |
|  _ \| | | | |
|_| \_|_|_|_|_|
v3.4.10
projectdiscovery.io

[INF] nuclei-templates are not installed, installing...
[INF] Successfully installed nuclei-templates at /home/bhai/.local/nuclei-templates
[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]
[INF] Found 0 tags and 0 matches on detection templates on http://testphp.vulnweb.com [wappalyzer: 0, detection: 0]
[INF] Scan completed in 1m. No results found.

(bhai@KALI)-[~]
$
```

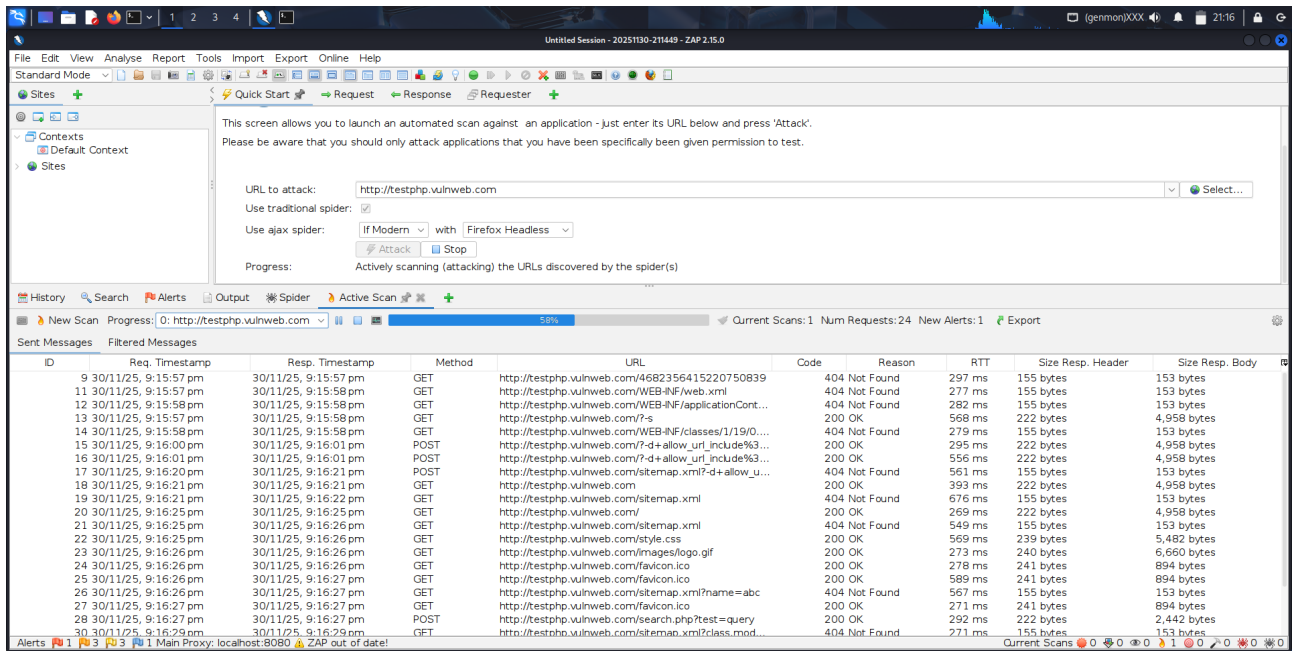
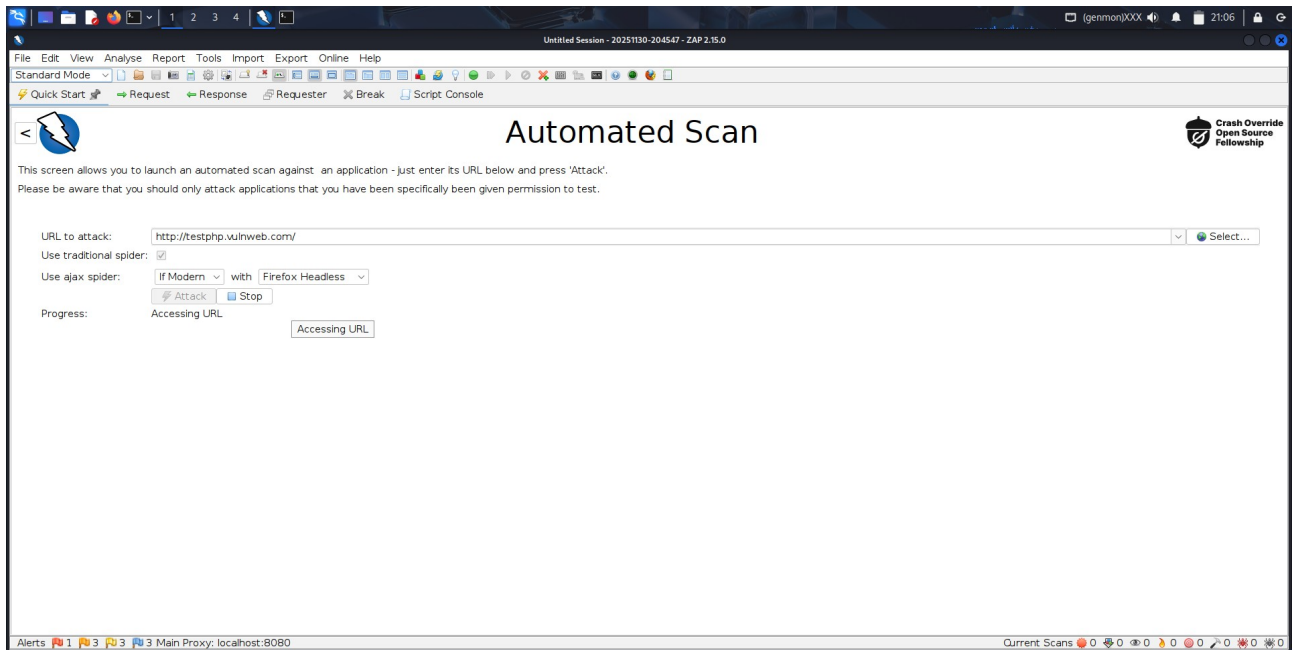
*Nuclei scan findings.*

---

### 3. OWASP ZAP Baseline Scan

#### Command

```
zap-baseline.py -t http://testphp.vulnweb.com -r zap_baseline.html
```







```
Session Actions Edit View Help
bhai@KALI: ~

(bhai@KALI)~[~]
$ wpscan --url http://example-wordpress-site.com

WordPress Security Scanner by the WPScan Team
Version 3.8.28

@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[i] Updating the Database ...
[i] Update completed.

Scan Aborted: The url supplied 'http://example-wordpress-site.com/' seems to be down (Could not resolve hostname)
```

```
Session Actions Edit View Help
bhai@KALI: ~

Scan Aborted: The remote website is up, but does not seem to be running WordPress.

(bhai@KALI)~[~]
$ wpscan --url https://wpscan.com/test --enumerate u

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The target appears to be hosted on WordPress.com. Scanning such site is not supported.

(bhai@KALI)~[~]
$
```

```
Session Actions Edit View Help
bhai@KALI: ~
(bhai@KALI)~[~]
$ wpscan --url https://vulnerable-wp.speedyp.net/ --enumerate u,ap,at

WordPress Security Scanner by the WPScan Team
Version 3.8.28
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

Scan Aborted: The url supplied 'https://vulnerable-wp.speedyp.net/' seems to be down (Could not resolve hostna
me)

(bhai@KALI)~[~]
$
```

*WordPress scan results.*

---