

Active Recon & Web Enumeration Report

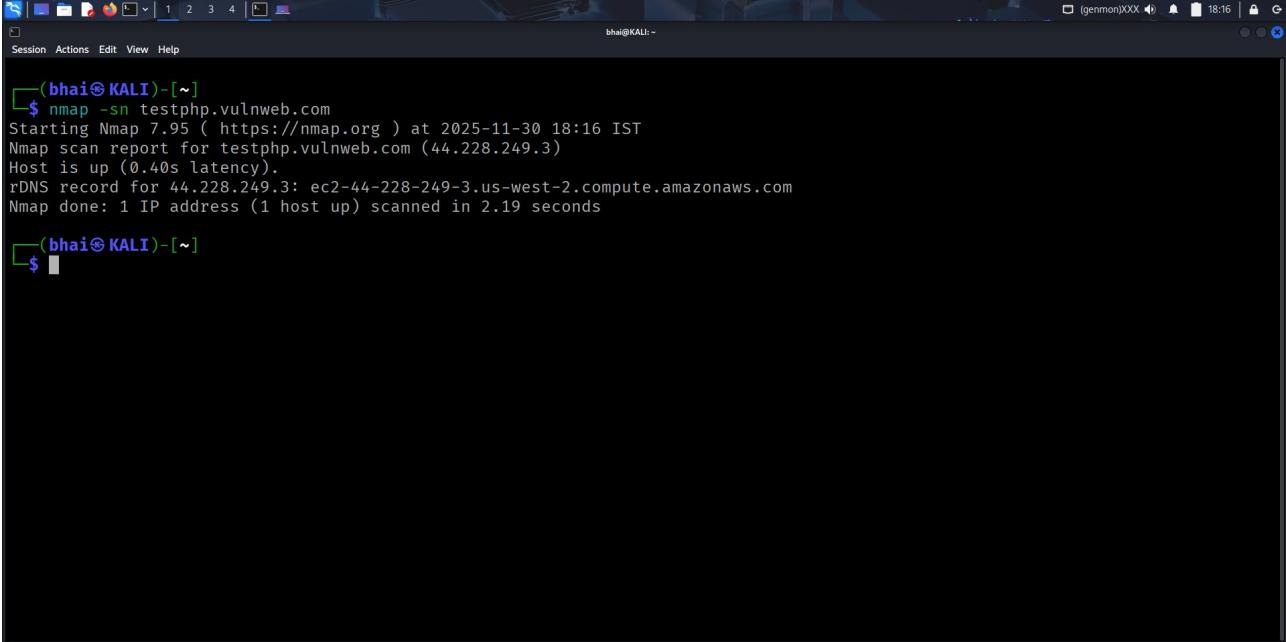
Target: testphp.vulnweb.com

1. Host Discovery

Checked if the target is alive and resolved its IP.

Command Used:

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



The screenshot shows a terminal window on a Kali Linux system. The title bar indicates the session is named '(bhai@KALI)'. The command entered is '\$ nmap -sn testphp.vulnweb.com'. The output shows the Nmap version (7.95), the start time (2025-11-30 18:16 IST), the target host (testphp.vulnweb.com at 44.228.249.3), and the fact that the host is up with 0.40s latency. It also shows the rDNS record for the IP and the completion message: 'Nmap done: 1 IP address (1 host up) scanned in 2.19 seconds'.

```
(bhai@KALI)-[~]
$ nmap -sn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:16 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.40s 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 2.19 seconds

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

Result: Host is alive.

2. Nmap Port & Service Scanning

A) Quick SYN Scan

```
nmap -sS testphp.vulnweb.com
```

```
(bhai㉿KALI)-[~]
$ nmap -sS testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:17 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.11s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 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 29.48 seconds
```

B) Version & Default Scripts on Common Ports

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

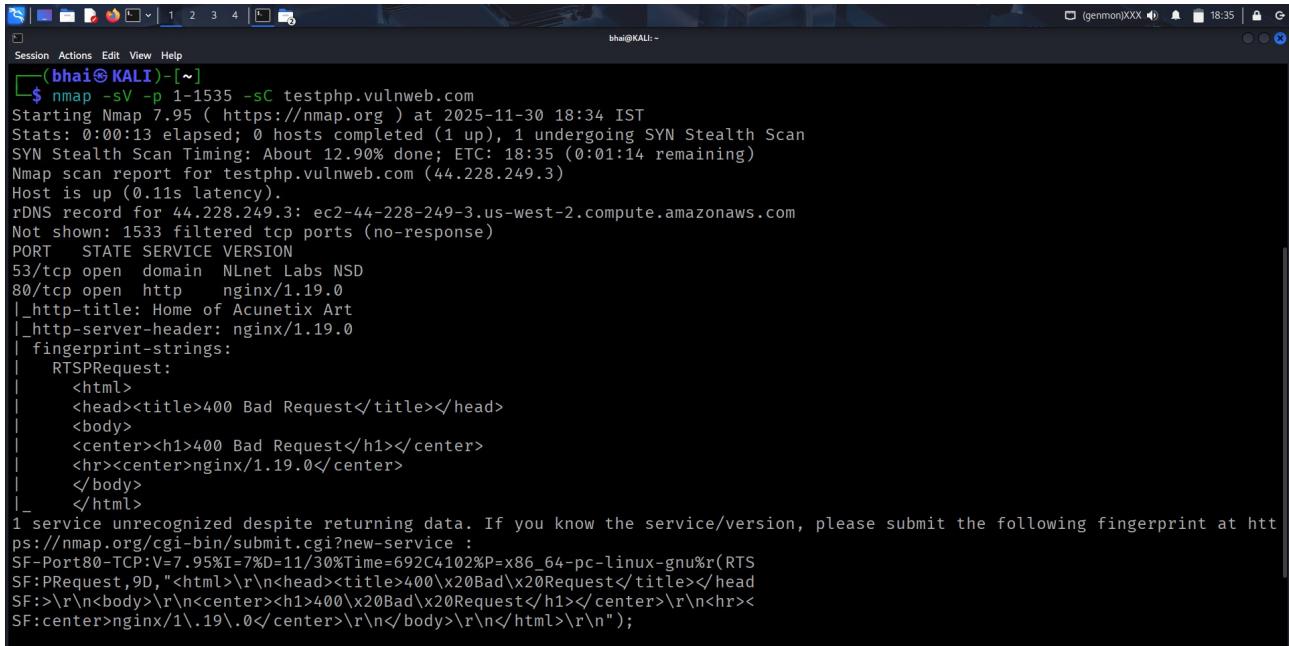
```
(bhai㉿KALI)-[~]
$ nmap -sV -p 22,80,443 -sC testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:19 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.28s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com

PORT      STATE     SERVICE VERSION
22/tcp    filtered ssh
80/tcp    open      http?
|_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 34.42 seconds
```

C) Service + NSE Scan on All Ports

```
nmap -sV -p 1-1535 -sC testphp.vulnweb.com
```

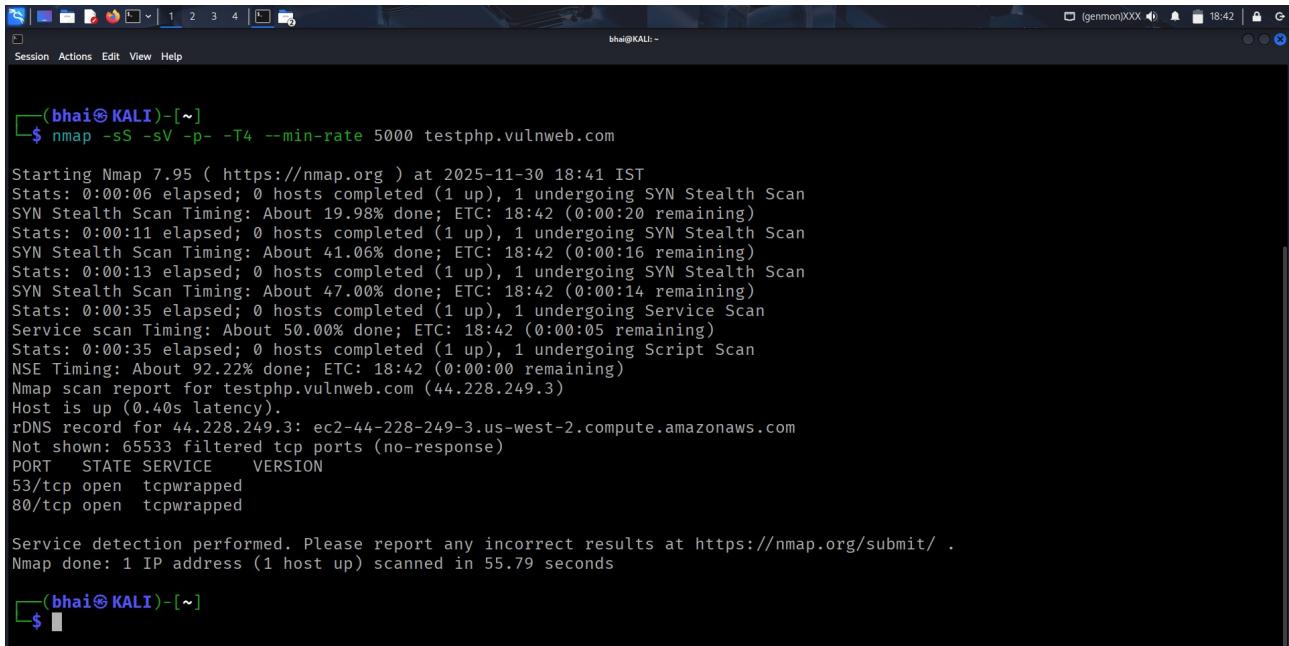


```
bhai@KALI: ~
$ nmap -sV -p 1-1535 -sC testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:34 IST
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.90% done; ETC: 18:35 (0:01:14 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.11s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 1533 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  NLnet Labs NSD
80/tcp    open  http    nginx/1.19.0
|_http-title: Home of Acunetix Art
|_http-server-header: nginx/1.19.0
| fingerprint-strings:
|   RTSPRequest:
|     <html>
|       <head><title>400 Bad Request</title></head>
|       <body>
|         <center><h1>400 Bad Request</h1></center>
|         <hr><center>nginx/1.19.0</center>
|       </body>
|     </html>
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port80-TCP:V=7.95%I=7%D=11/30%Time=692C4102%P=x86_64-pc-linux-gnu%r(RTS
SF:PRequest,9D,"<html>\r\n<head><title>400\x20Bad\x20Request</title></head>
SF:>\r\n<body>\r\n<center><h1>400\x20Bad\x20Request</h1></center>\r\n<hr><
SF:center>nginx/1\.\.19.\.0</center>\r\n</body>\r\n</html>\r\n");

```

D) Full TCP Port Scan

```
nmap -sV -p- -T4 --min-rate 5000 testphp.vulnweb.com
```



```
bhai@KALI: ~
$ nmap -sS -sV -p- -T4 --min-rate 5000 testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:41 IST
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.98% done; ETC: 18:42 (0:00:20 remaining)
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.06% done; ETC: 18:42 (0:00:16 remaining)
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.00% done; ETC: 18:42 (0:00:14 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 18:42 (0:00:05 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.22% done; ETC: 18:42 (0:00:00 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.40s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
80/tcp    open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.79 seconds

```

E) OS Detection (If Allowed)

```
nmap -O --osscan-guess testphp.vulnweb.com
```

```

(bhai㉿KALI)-[~]
$ nmap -O --osscan-guess testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:44 IST
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.23s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: router|specialized|phone|general purpose
Running (JUST GUESSING): Ubiquiti embedded (95%), Linux 4.X (95%), Oracle VM Server 3.X (95%), Google Android 10.X|11.X|12.X (91%)
OS CPE: cpe:/o:linux:linux_kernel:4.19 cpe:/o:oracle:vm_server:3.4.2 cpe:/o:linux:linux_kernel:4.1 cpe:/o:linux:linux_kernel:4 cpe:/o:google:android:10 cpe:/o:google:android:11 cpe:/o:google:android:12 cpe:/o:linux:linux_kernel:4.14
Aggressive OS guesses: Ubiquiti Dream Machine Pro gateway (Linux 4.19) (95%), Oracle VM Server 3.4.2 (Linux 4.1) (95%), Android 10 - 12 (Linux 4.14 - 4.19) (91%), Android 10 - 11 (Linux 4.14) (91%), Linux 3.2 (89%), Linux 4.15 (89%), Linux 5.10 - 5.19 (89%), Ubiquiti Dream Machine Pro gateway (Linux) (89%), Crestron XPanel control system (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 50.81 seconds

```

3. Open Ports & Services

Port	Status	Service
22	filtered	ssh
53	open	domain
80	open	http
443	filtered	https

4. NSE Script Findings

nmap -sV -sC testphp.vulnweb.com

```
bhai@KALI:~$ nmap -sV -sC testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-30 18:53 IST
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.90% done; ETC: 18:54 (0:00:26 remaining)
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.53s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain      NLnet Labs NSD
80/tcp    open  tcpwrapped
|_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 138.04 seconds

bhai@KALI:~$
```

5. HTTP Directory Enumeration (Dirb)

Brute-forced web directories.

Basic Scan

```
dirb https://testphp.vulnweb.com
```

```
bhai@KALI:~$ dirb https://testphp.vulnweb.com

DIRB v2.22
By The Dark Raver

START_TIME: Sun Nov 30 18:56:52 2025
URL_BASE: https://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

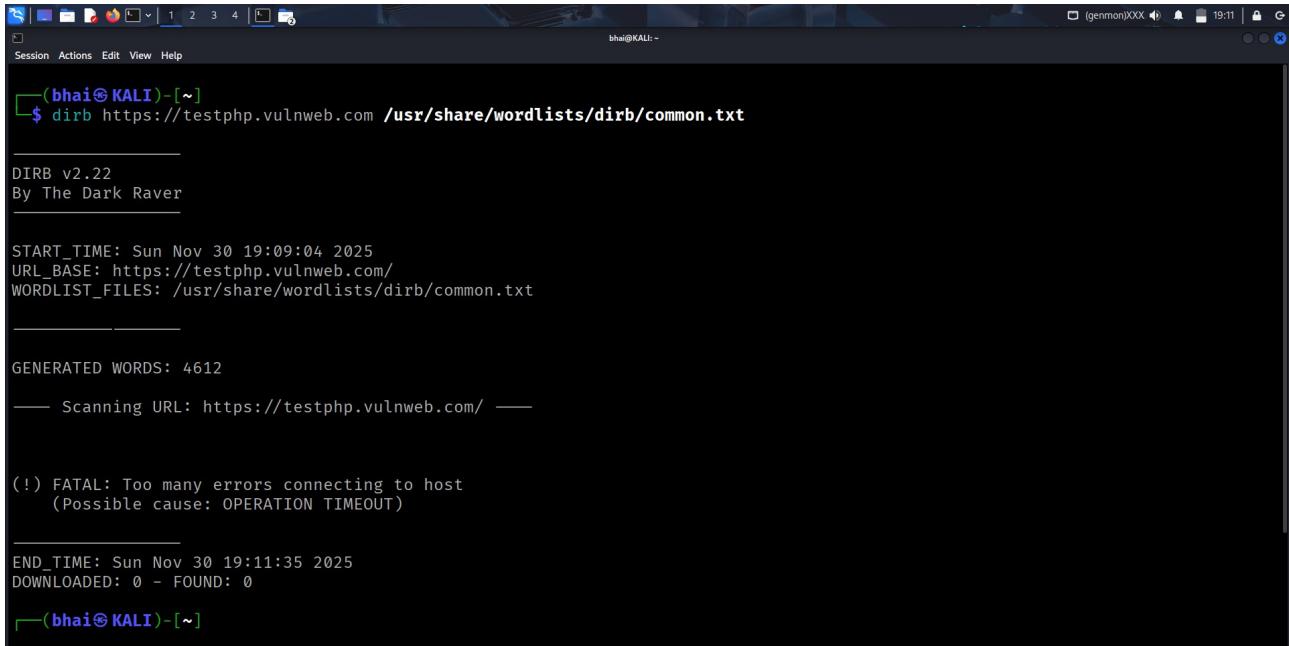
GENERATED WORDS: 4612
--- Scanning URL: https://testphp.vulnweb.com/ ---
(!) FATAL: Too many errors connecting to host
(Possible cause: OPERATION TIMEOUT)

END_TIME: Sun Nov 30 18:59:23 2025
DOWNLOADED: 0 - FOUND: 0

bhai@KALI:~$
```

With Common Wordlist

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



A terminal window titled '(bhai㉿KALI)-[~]' showing the output of a DIRB scan against the URL 'https://testphp.vulnweb.com'. The output includes the version information 'DIRB v2.22' and 'By The Dark Raver', the start time 'START_TIME: Sun Nov 30 19:09:04 2025', the URL base 'URL_BASE: https://testphp.vulnweb.com', and the wordlist file 'WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt'. It also shows the number of generated words (4612) and the scanning progress. A fatal error message '(!) FATAL: Too many errors connecting to host (Possible cause: OPERATION TIMEOUT)' is displayed. The end time is 'END_TIME: Sun Nov 30 19:11:35 2025' and the download count is 'DOWNLOADED: 0 - FOUND: 0'.

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

DIRB v2.22
By The Dark Raver

START_TIME: Sun Nov 30 19:09:04 2025
URL_BASE: https://testphp.vulnweb.com/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

GENERATED WORDS: 4612
— Scanning URL: https://testphp.vulnweb.com/ ——
(!) FATAL: Too many errors connecting to host
(Possible cause: OPERATION TIMEOUT)

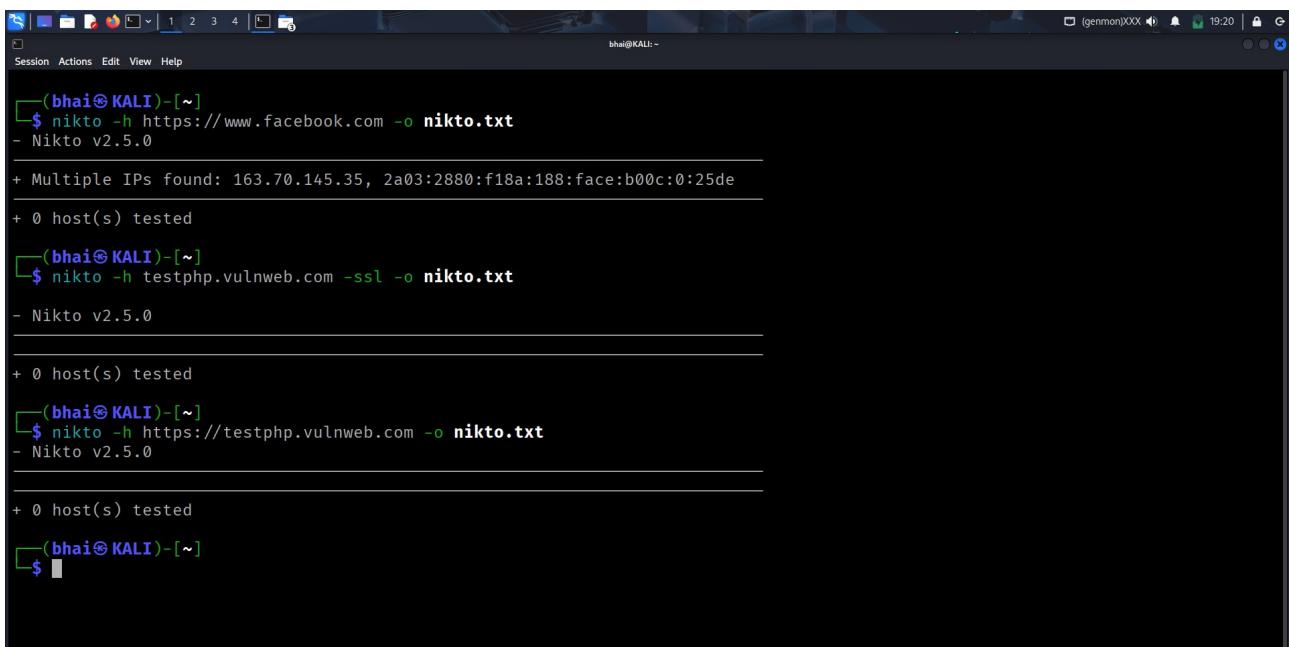
END_TIME: Sun Nov 30 19:11:35 2025
DOWNLOADED: 0 - FOUND: 0

(bhai㉿KALI)-[~]
```

6. Web Fingerprinting & Vulnerability Checks

WhatWeb Scan

```
whatweb https://testphp.vulnweb.com
```



A terminal window titled '(bhai㉿KALI)-[~]' showing the output of a WhatWeb scan against three different URLs: 'https://www.facebook.com', 'https://testphp.vulnweb.com', and 'https://testphp.vulnweb.com'. The output shows the version of Nikto used (v2.5.0) and the number of hosts tested (0). The results for each host are listed below.

```
$ whatweb https://testphp.vulnweb.com

(bhai㉿KALI)-[~]
$ nikto -h https://www.facebook.com -o nikto.txt
- Nikto v2.5.0
+ Multiple IPs found: 163.70.145.35, 2a03:2880:f18a:188:face:b00c:0:25de
+ 0 host(s) tested

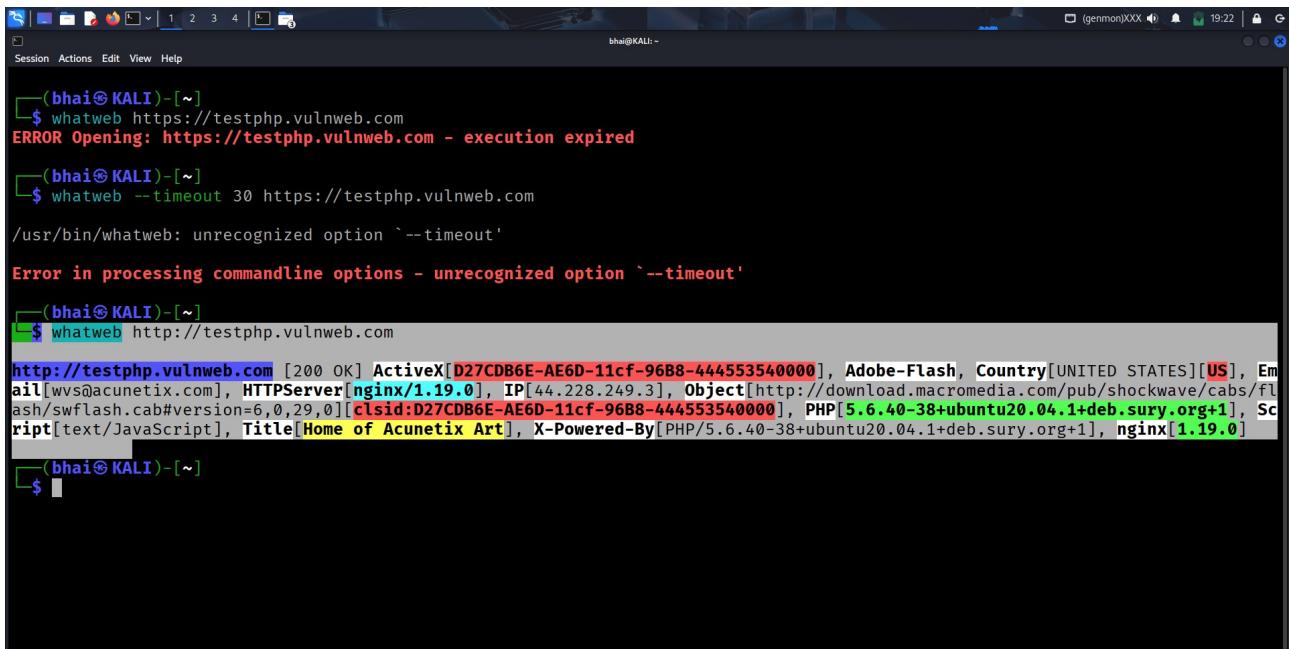
(bhai㉿KALI)-[~]
$ nikto -h testphp.vulnweb.com -ssl -o nikto.txt
- Nikto v2.5.0
+ 0 host(s) tested

(bhai㉿KALI)-[~]
$ nikto -h https://testphp.vulnweb.com -o nikto.txt
- Nikto v2.5.0
+ 0 host(s) tested

(bhai㉿KALI)-[~]
$
```

Nikto Scan

```
nikto -h https://testphp.vulnweb.com -o nikto.txt
```



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `nikto -h https://testphp.vulnweb.com -o nikto.txt`. The output of the scan is displayed in the terminal. Key findings include:

- An error message: `ERROR Opening: https://testphp.vulnweb.com - execution expired`.
- A warning about an unrecognized option: `/usr/bin/whatweb: unrecognized option '--timeout'`.
- An error message from whatweb: `Error in processing cmdline options - unrecognized option '--timeout'`.
- Information about the target website: `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]`.

7. Conclusion

- Target is alive and reachable.
- Open ports identified with service versions.
- HTTP enumeration discovered 0 directories.
- Nikto revealed basic web fingerprints.
- No exploitation performed, only safe active recon.