Assignment: Web Application Scanning - Automated Vulnerability Discovery

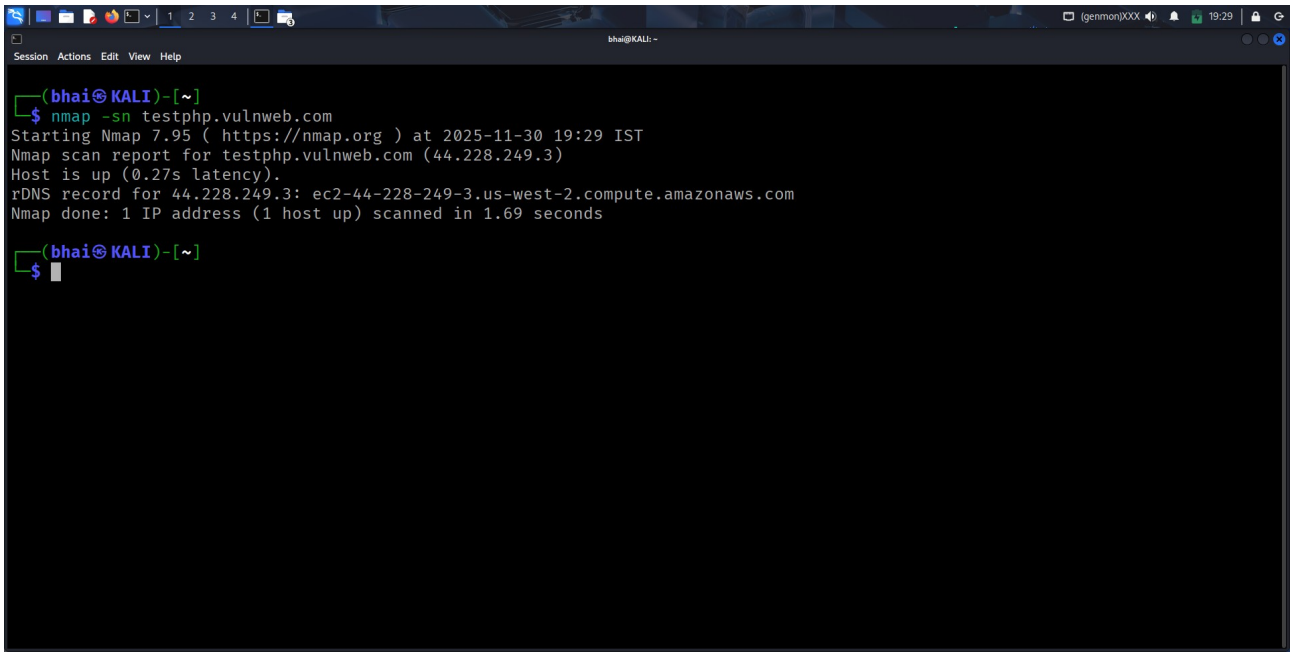
---

🔷 Step 1 — Recon & Discovery

1. Host Discovery

Command

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



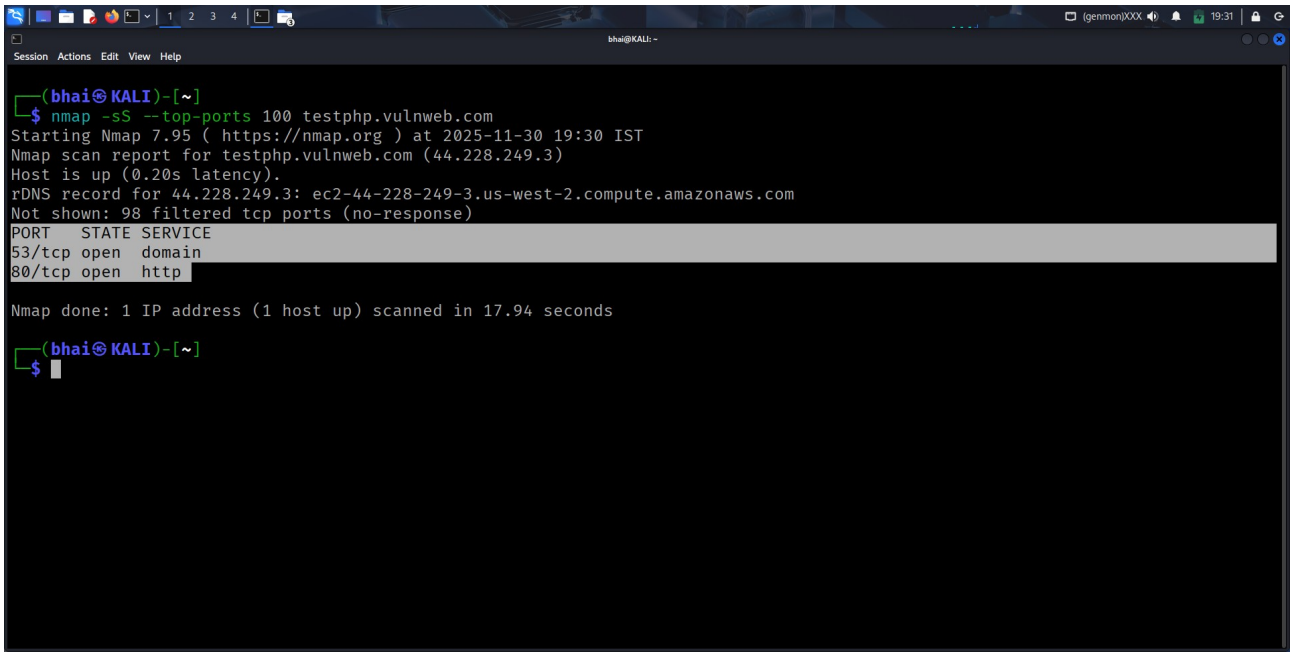
Host discovery result.

---

2. Port & Service Scan

Command

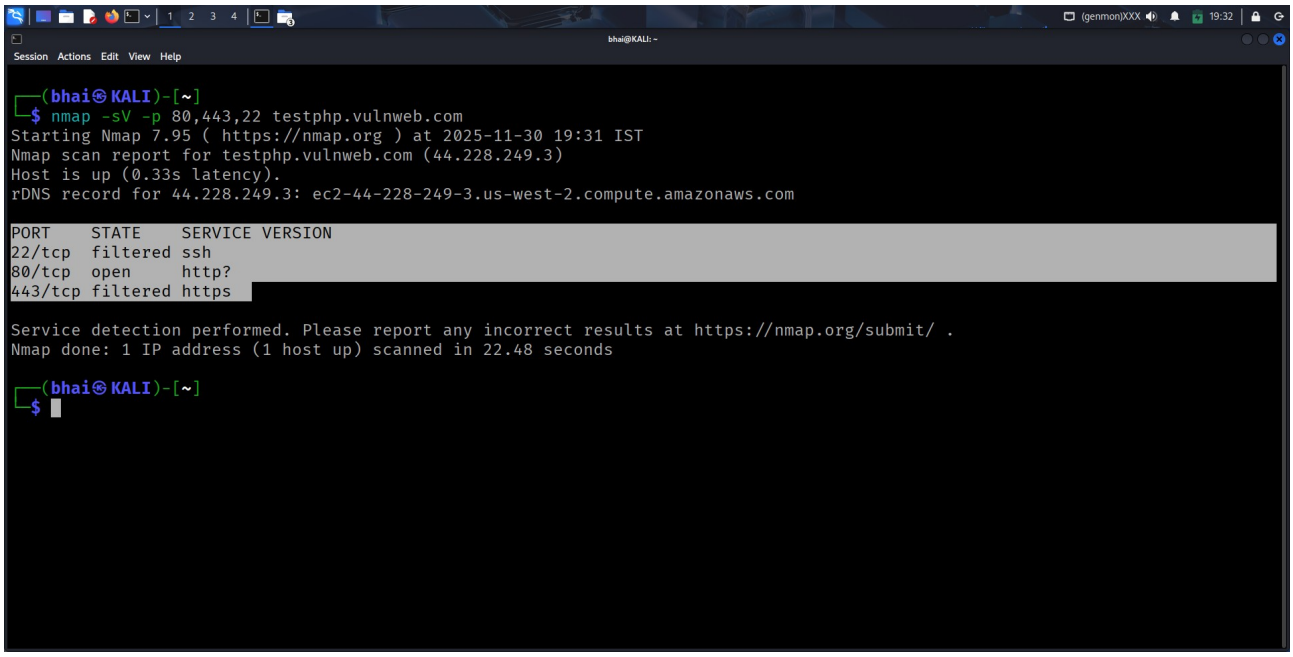
`nmap -sS --top-ports 100 testphp.vulnweb.com`



Quick port scan result.

Command (Version detection on open ports)

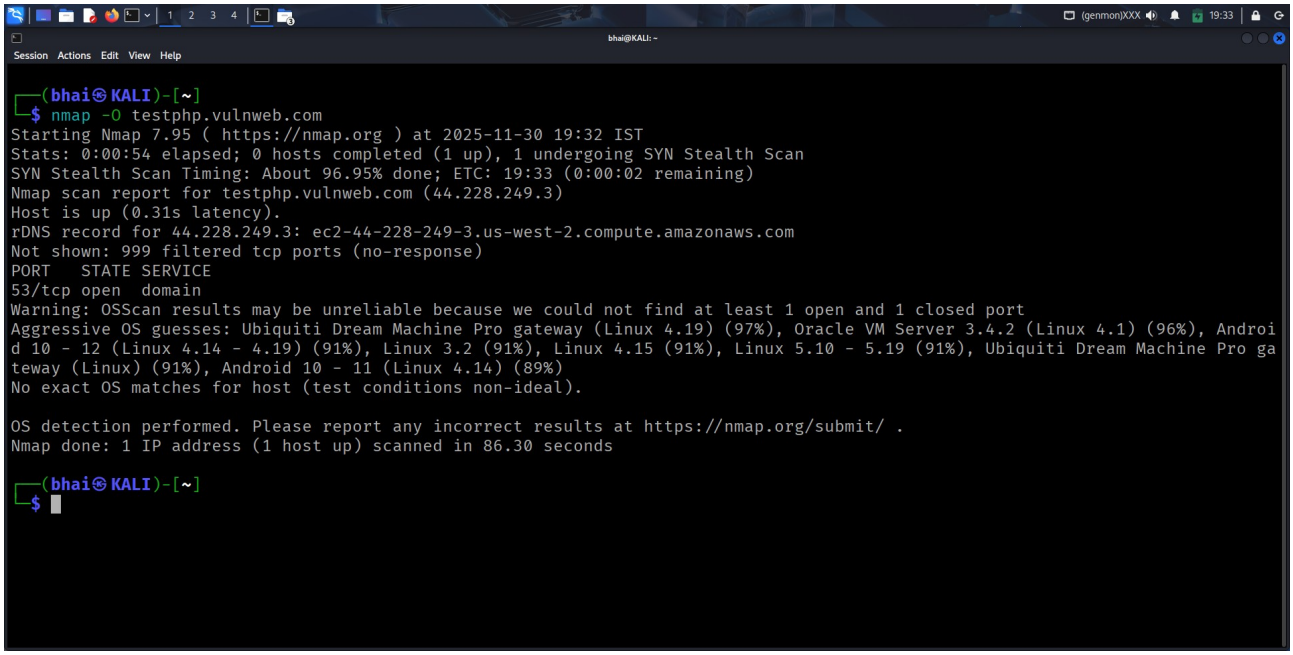
`nmap -sV -p 80,443,22 testphp.vulnweb.com`



Service version scan.

Command (OS detection)

`nmap -O testphp.vulnweb.com`



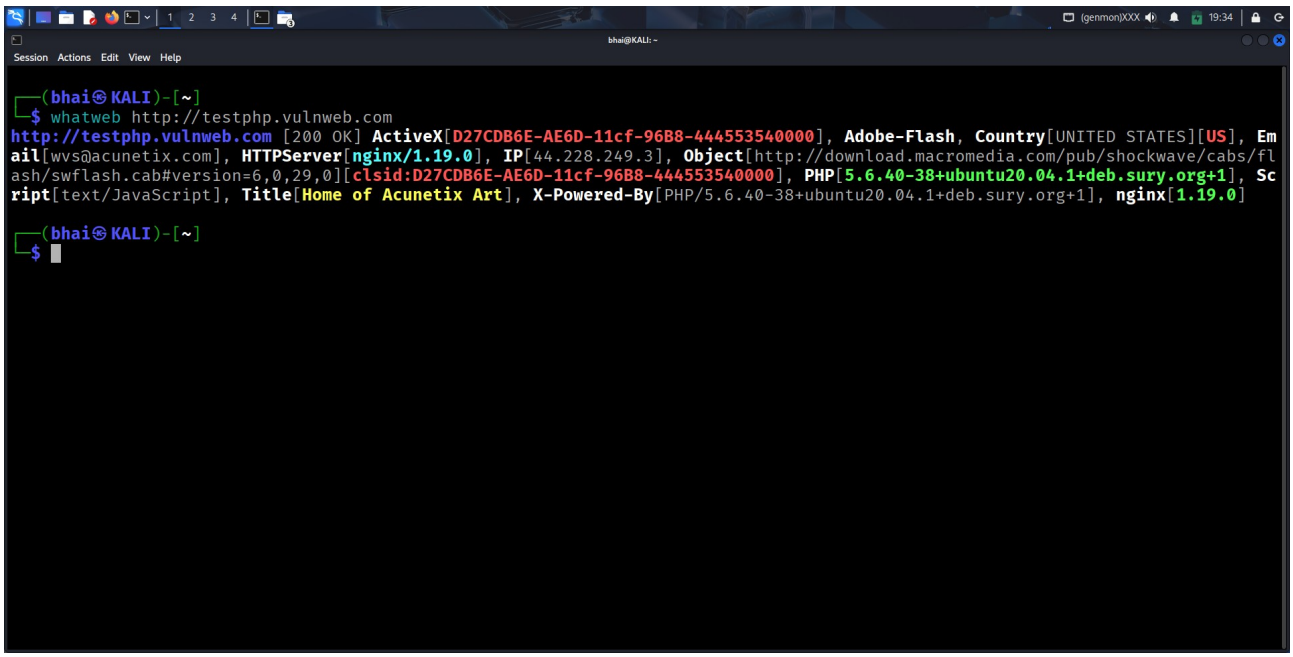
OS detection output.

🔷 Step 2 — Web Fingerprinting

1. WhatWeb

Command

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



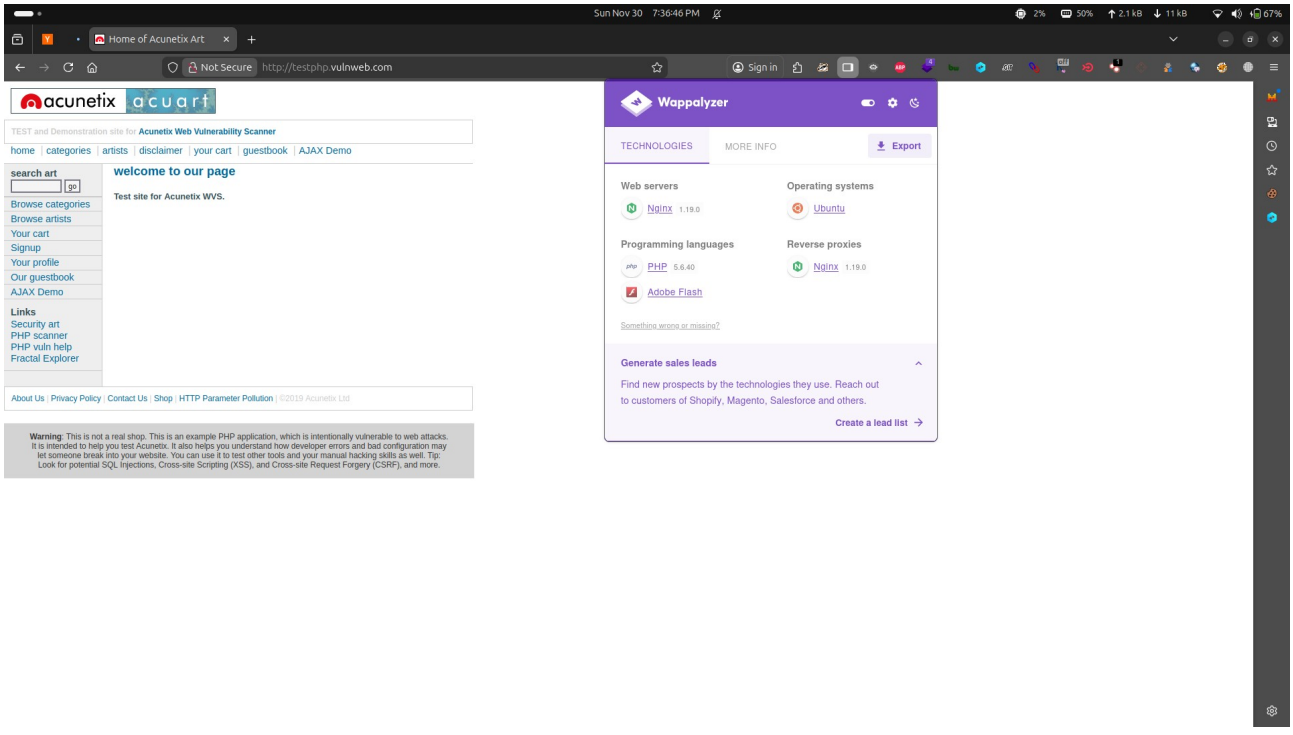
Web fingerprinting result.

---

2. Wappalyzer

Install Chrome/Firefox extension → open:

http://testphp.vulnweb.com



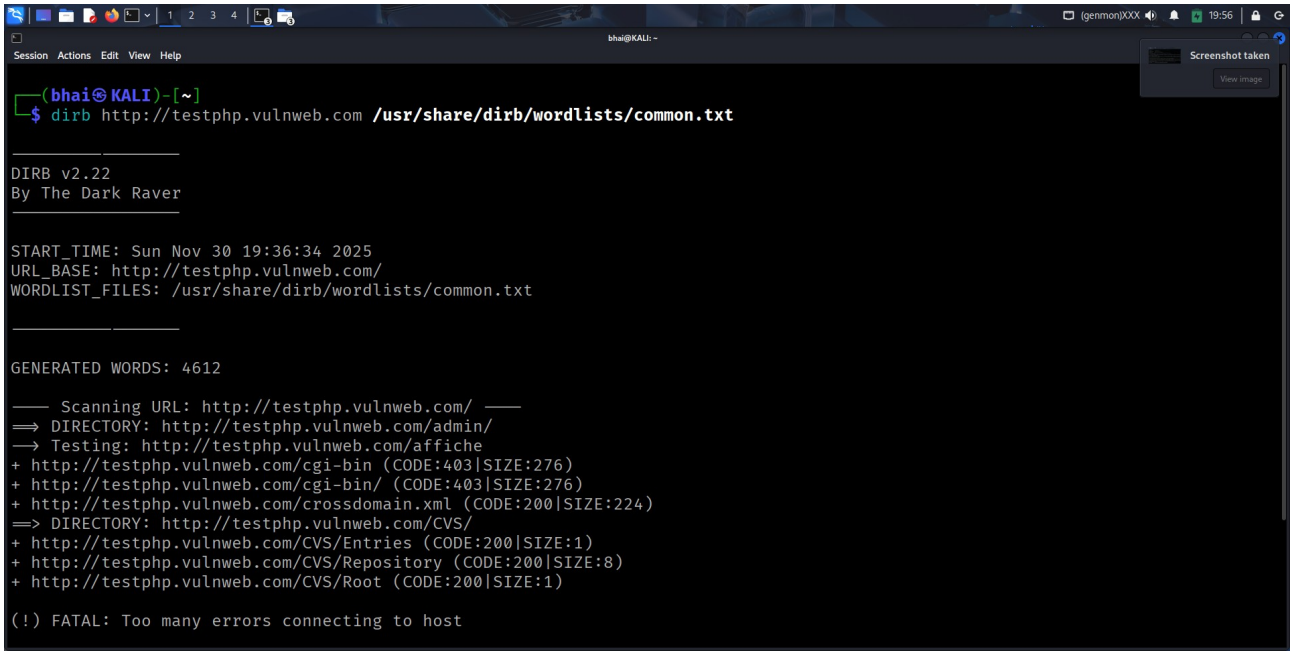
Wappalyzer tech detection.

🔷 Step 3 — Directory Discovery

Dirb

Command

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



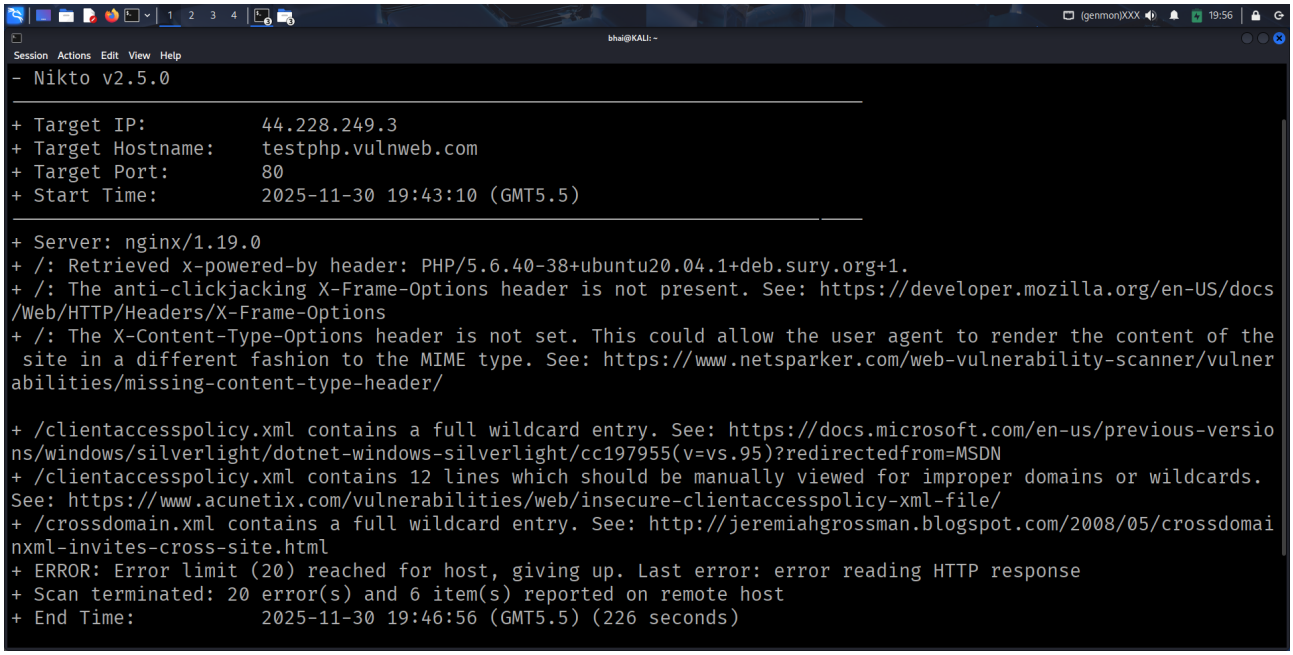
Directory brute-force results.

🔷 Step 4 — Light Automated Scans

1. Nikto

Command

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



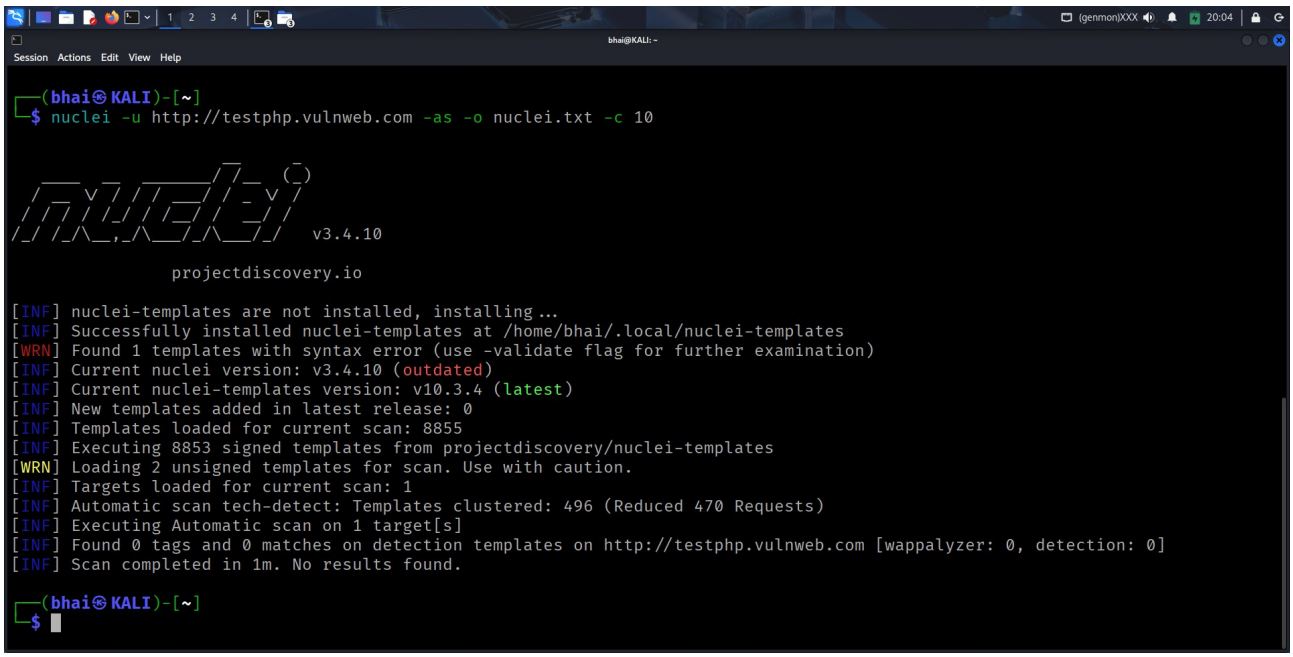
Nikto scan output.

---

2. Nuclei

Command

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



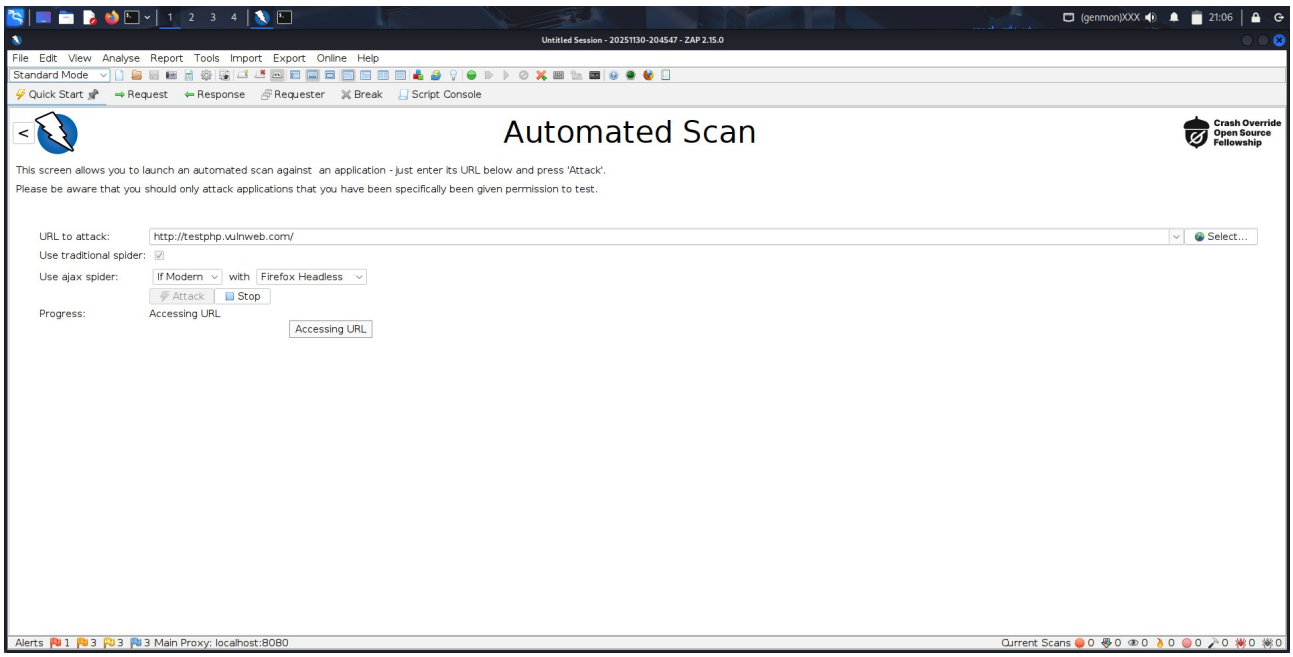
Nuclei scan findings.

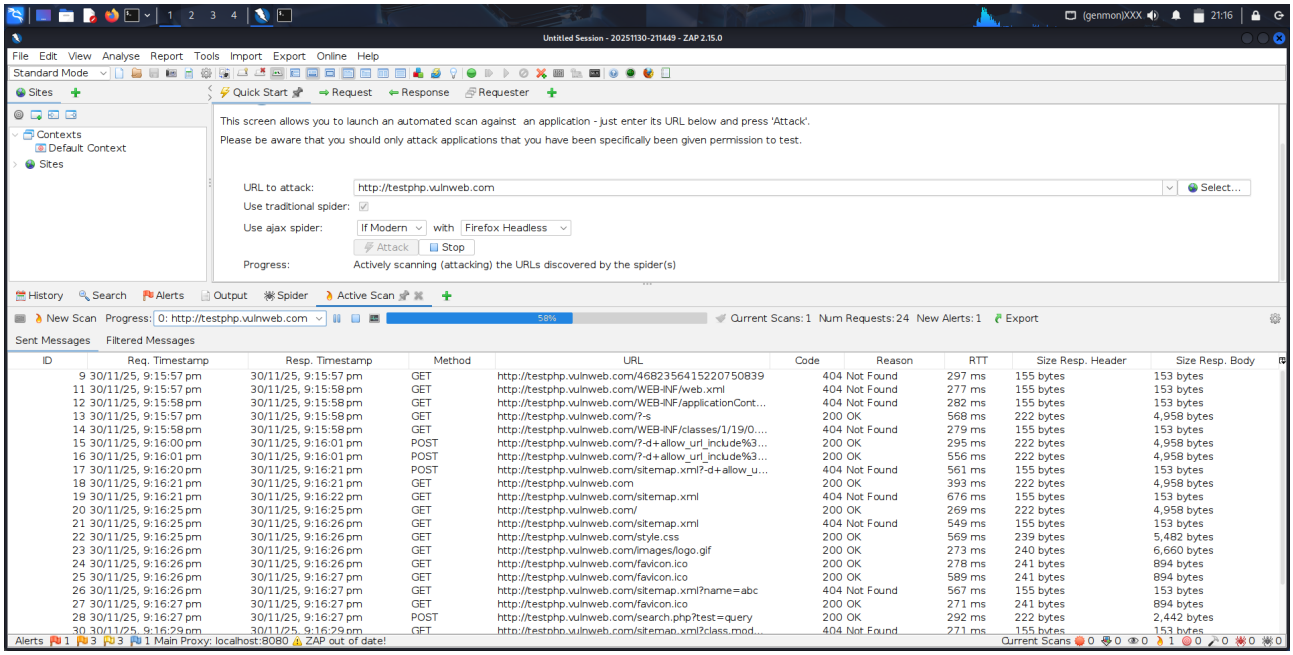
---

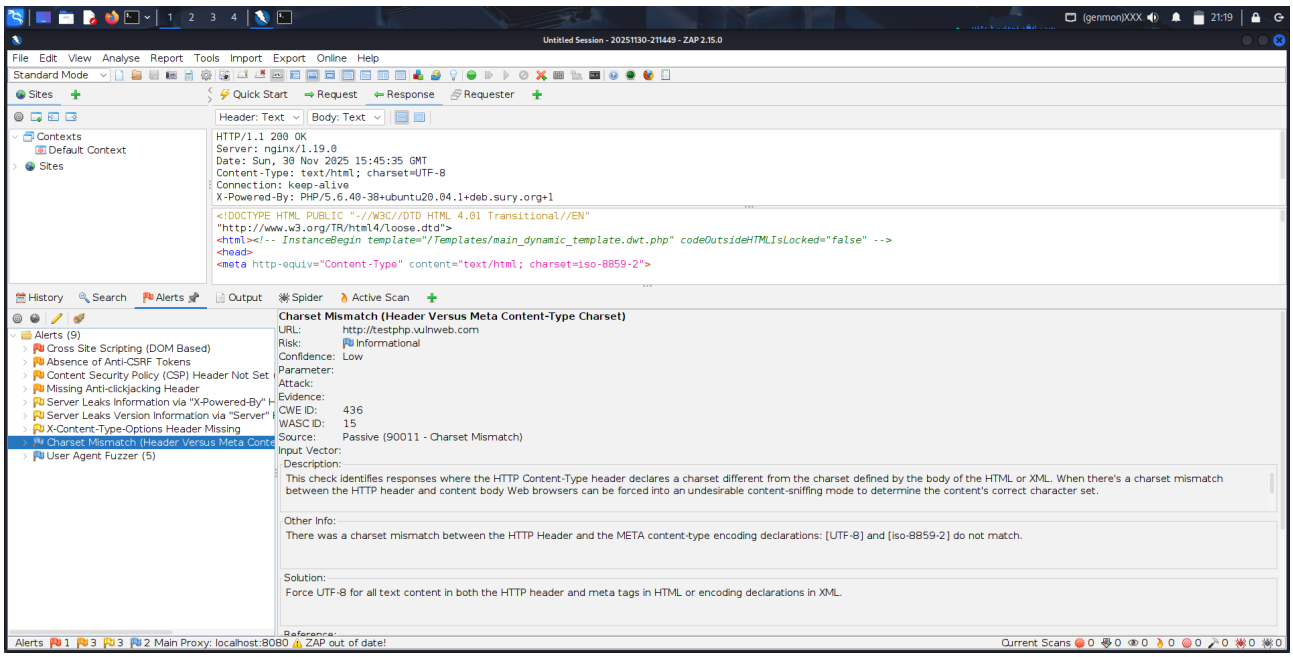
3. OWASP ZAP Baseline Scan

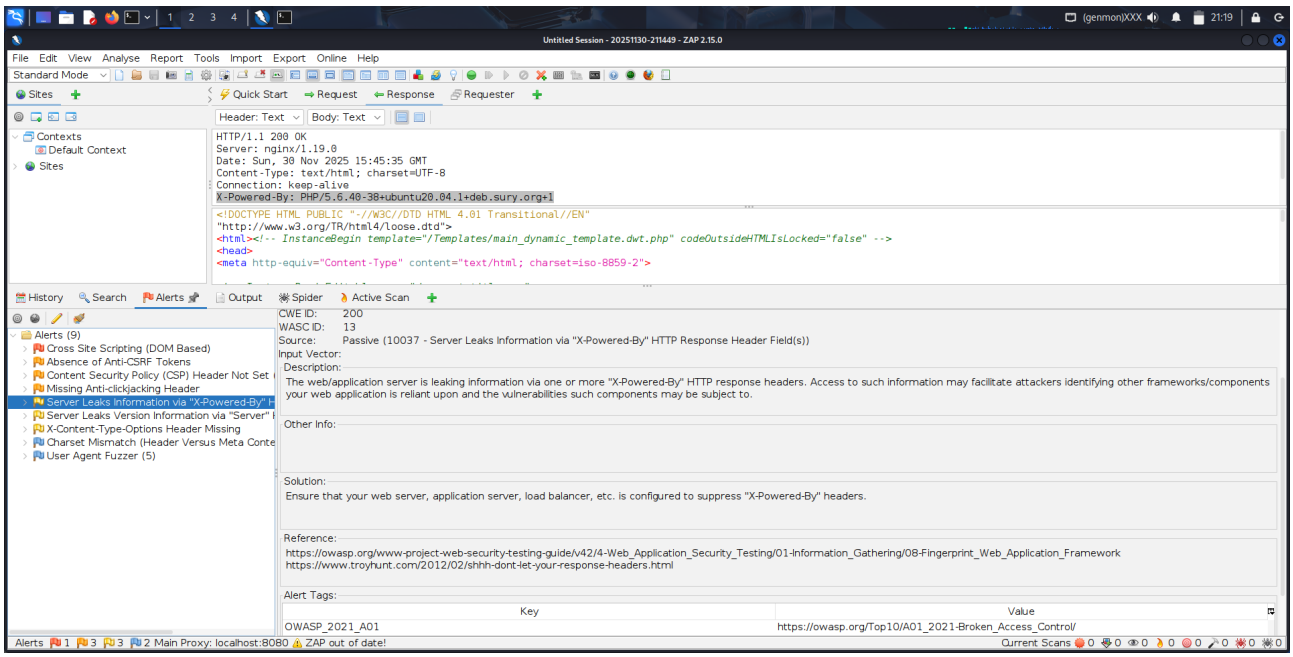
Command

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


Untitled Session - 20251130-204547 - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Quick Start
Request
Response
Requester
Break
Script Console
Automated Scan
Crash Override Open Source Fellowship
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://testphp.vulnweb.com/
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox Headless
Attack
Stop
Progress:
Accessing URL
Accessing URL
Alerts 1 3 3 3 Main Proxy: localhost:8080
Current Scans 0 0 0 0 0 0 0 0 0


Untitled Session - 20251130-211449 - ZAP 2.15.0
File Edit View Analyse Report Tools Import Export Online Help
Standard Mode
Sites
Quick Start
Request
Response
Requester
Contexts
Default Context
Sites
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.
Please be aware that you should only attack applications that you have been specifically been given permission to test.
URL to attack:
http://testphp.vulnweb.com
Select...
Use traditional spider:
Use ajax spider:
If Modern
with
Firefox Headless
Attack
Stop
Progress:
Actively scanning (attacking) the URLs discovered by the spider(s)
History
Search
Alerts
Output
Spider
Active Scan
New Scan
Progress:
0: http://testphp.vulnweb.com
58%
Current Scans: 1
Num Requests: 24
New Alerts: 1
Export
Sent Messages
Filtered Messages
ID
Req. Timestamp
Resp. Timestamp
Method
URL
Code
Reason
RTT
Size Resp. Header
Size Resp. Body
9 30/11/25, 9:15:57 pm 30/11/25, 9:15:57 pm GET http://testphp.vulnweb.com/4682356415220750839 404 Not Found 297 ms 155 bytes 153 bytes
11 30/11/25, 9:15:57 pm 30/11/25, 9:15:58 pm GET http://testphp.vulnweb.com/WEB-INF/web.xml 404 Not Found 277 ms 155 bytes 153 bytes
12 30/11/25, 9:15:58 pm 30/11/25, 9:15:58 pm GET http://testphp.vulnweb.com/WEB-INF/applicationCont... 404 Not Found 282 ms 155 bytes 153 bytes
13 30/11/25, 9:15:57 pm 30/11/25, 9:15:58 pm GET http://testphp.vulnweb.com/?-s 200 OK 568 ms 222 bytes 4,958 bytes
14 30/11/25, 9:15:58 pm 30/11/25, 9:15:58 pm GET http://testphp.vulnweb.com/WEB-INF/classes/1/19/0.... 404 Not Found 279 ms 155 bytes 153 bytes
15 30/11/25, 9:16:00 pm 30/11/25, 9:16:01 pm POST http://testphp.vulnweb.com/?-d+allow_url_include%3... 200 OK 295 ms 222 bytes 4,958 bytes
16 30/11/25, 9:16:01 pm 30/11/25, 9:16:01 pm POST http://testphp.vulnweb.com/?-d+allow_url_include%3... 200 OK 556 ms 222 bytes 4,958 bytes
17 30/11/25, 9:16:20 pm 30/11/25, 9:16:21 pm POST http://testphp.vulnweb.com/sitemap.xml?-d+allow_u... 404 Not Found 561 ms 155 bytes 153 bytes
18 30/11/25, 9:16:21 pm 30/11/25, 9:16:21 pm GET http://testphp.vulnweb.com 200 OK 393 ms 222 bytes 4,958 bytes
19 30/11/25, 9:16:21 pm 30/11/25, 9:16:22 pm GET http://testphp.vulnweb.com/sitemap.xml 404 Not Found 676 ms 155 bytes 153 bytes
20 30/11/25, 9:16:25 pm 30/11/25, 9:16:25 pm GET http://testphp.vulnweb.com/ 200 OK 269 ms 222 bytes 4,958 bytes
21 30/11/25, 9:16:25 pm 30/11/25, 9:16:26 pm GET http://testphp.vulnweb.com/sitemap.xml 404 Not Found 549 ms 155 bytes 153 bytes
22 30/11/25, 9:16:25 pm 30/11/25, 9:16:26 pm GET http://testphp.vulnweb.com/style.css 200 OK 569 ms 239 bytes 5,482 bytes
23 30/11/25, 9:16:26 pm 30/11/25, 9:16:26 pm GET http://testphp.vulnweb.com/images/logo.gif 200 OK 273 ms 240 bytes 6,660 bytes
24 30/11/25, 9:16:26 pm 30/11/25, 9:16:26 pm GET http://testphp.vulnweb.com/favicon.ico 200 OK 278 ms 241 bytes 894 bytes
25 30/11/25, 9:16:26 pm 30/11/25, 9:16:27 pm GET http://testphp.vulnweb.com/favicon.ico 200 OK 589 ms 241 bytes 894 bytes
26 30/11/25, 9:16:26 pm 30/11/25, 9:16:27 pm GET http://testphp.vulnweb.com/sitemap.xml?name=abc 404 Not Found 567 ms 155 bytes 153 bytes
27 30/11/25, 9:16:27 pm 30/11/25, 9:16:27 pm GET http://testphp.vulnweb.com/favicon.ico 200 OK 271 ms 241 bytes 894 bytes
28 30/11/25, 9:16:27 pm 30/11/25, 9:16:27 pm POST http://testphp.vulnweb.com/search.php?test=query 200 OK 292 ms 222 bytes 2,442 bytes
30 30/11/25, 9:16:29 pm 30/11/25, 9:16:29 pm GET http://testphp.vulnweb.com/sitemap.xml?class.mod... 404 Not Found 271 ms 155 bytes 153 bytes
Alerts 1 3 3 1 Main Proxy: localhost:8080 ZAP out of date!
Current Scans 0 0 0 1 0 0 0 0 0





ZAP baseline scan report generated.

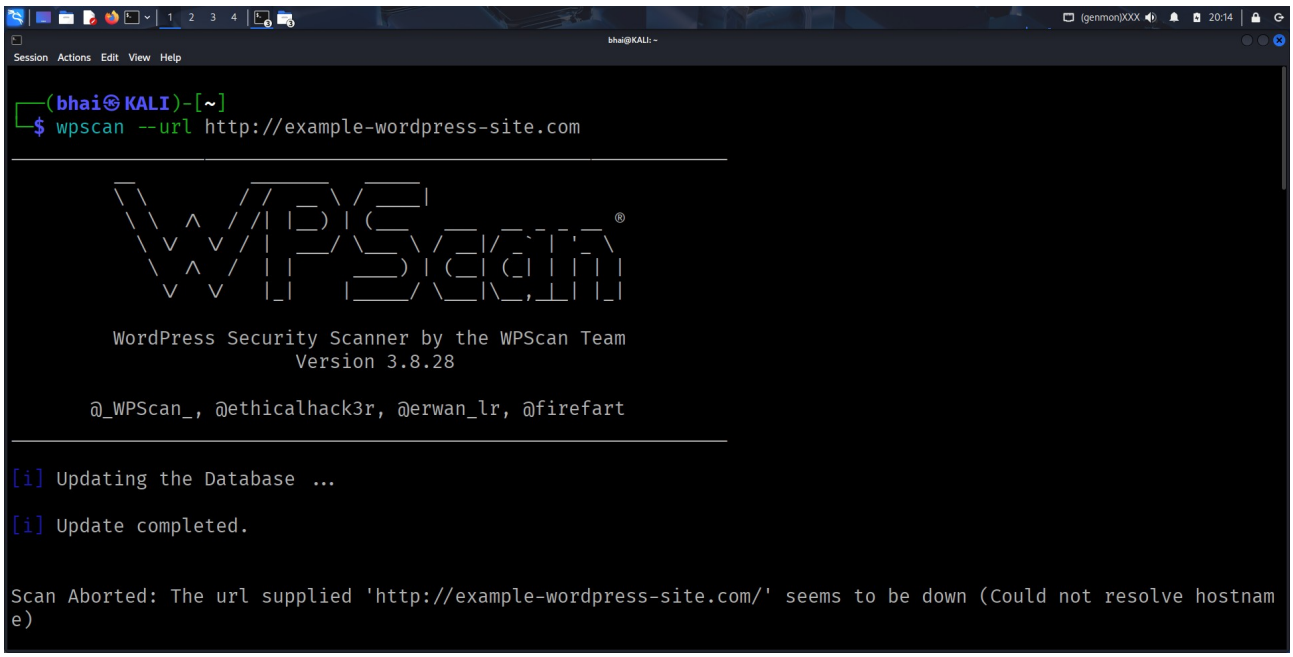
---

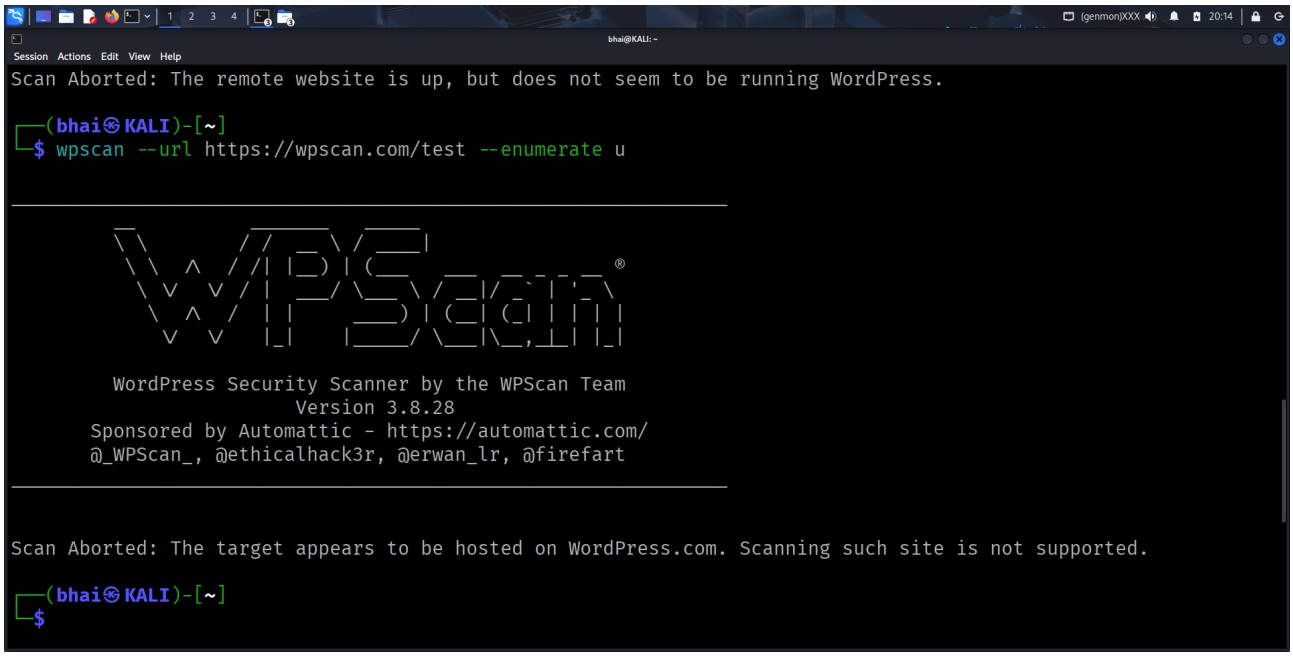
4. WPScan

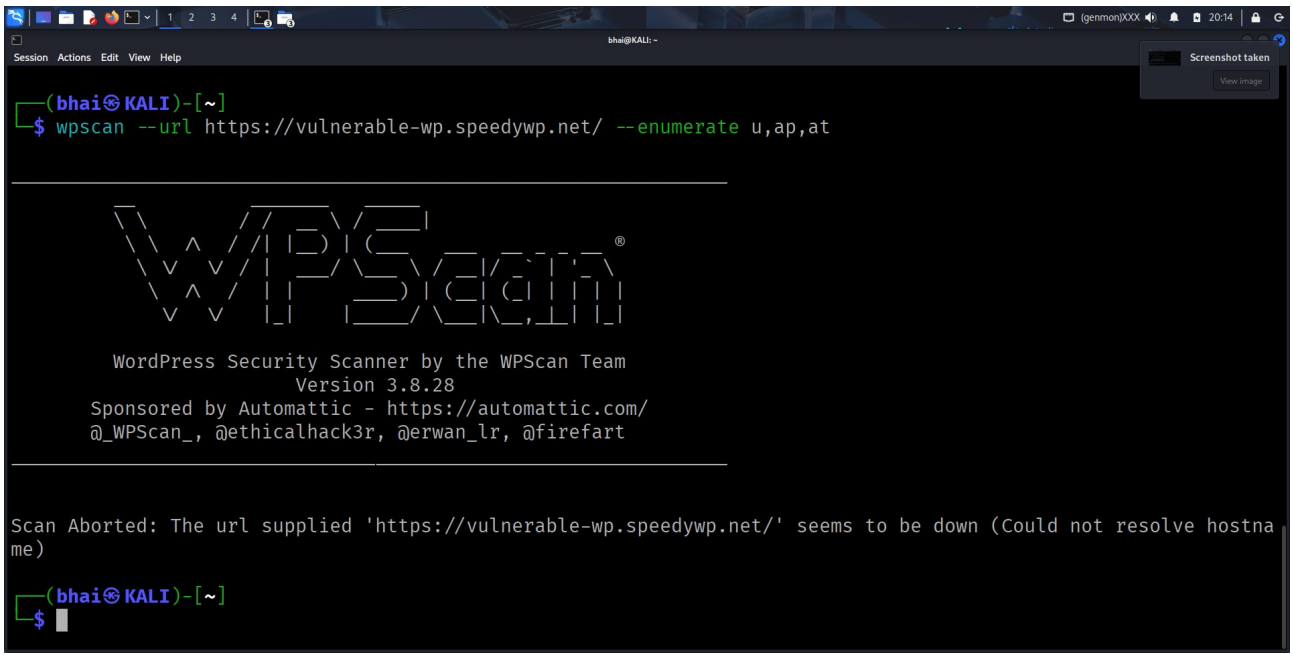
testphp.vulnweb.com is **not WordPress**

Command

```
wpscan --url http://example-wordpress-site.com
```


bhai@KALI: ~
Session Actions Edit View Help
(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)


bhai@KALI: ~
Session Actions Edit View Help
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)-[~]
$



WordPress scan results.
