

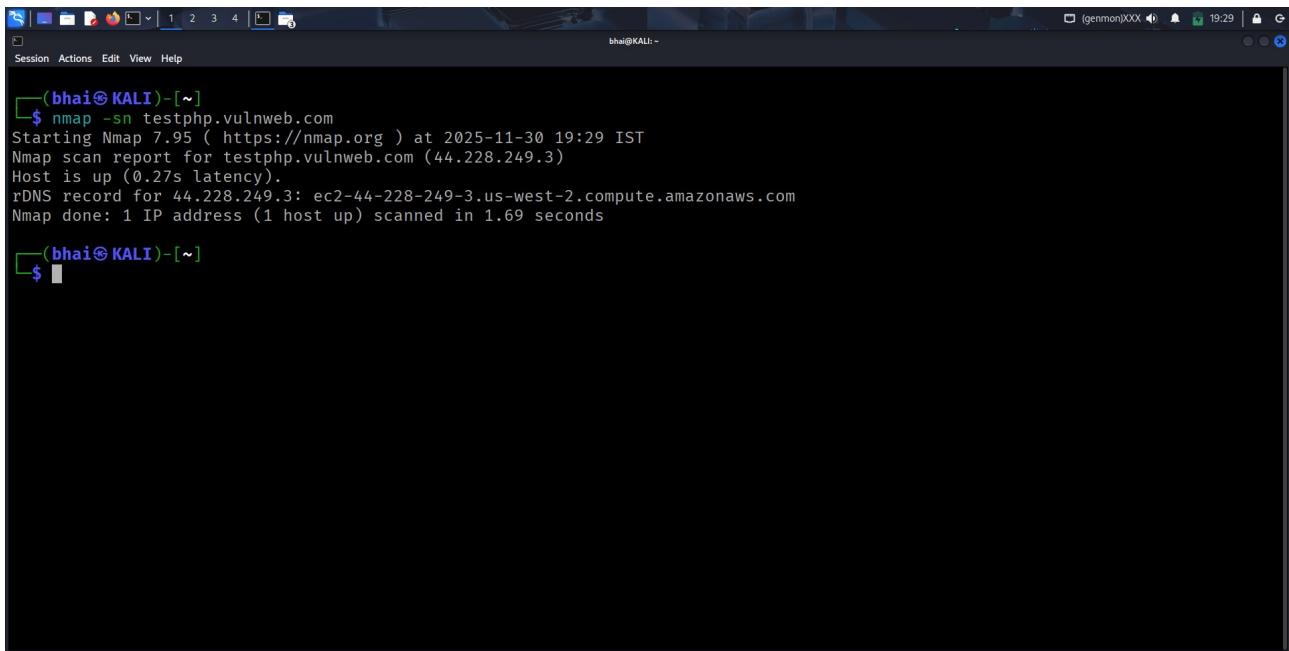
Assignment: Web Application Scanning - Automated Vulnerability Discovery

◆ Step 1 — Recon & Discovery

1. Host Discovery

Command

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



The screenshot shows a terminal window on a Kali Linux system. The user has run the command `nmap -sn testphp.vulnweb.com`. The output indicates that the host is up at IP address 44.228.249.3, which is an AWS EC2 instance. The scan took 1.69 seconds.

```
(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

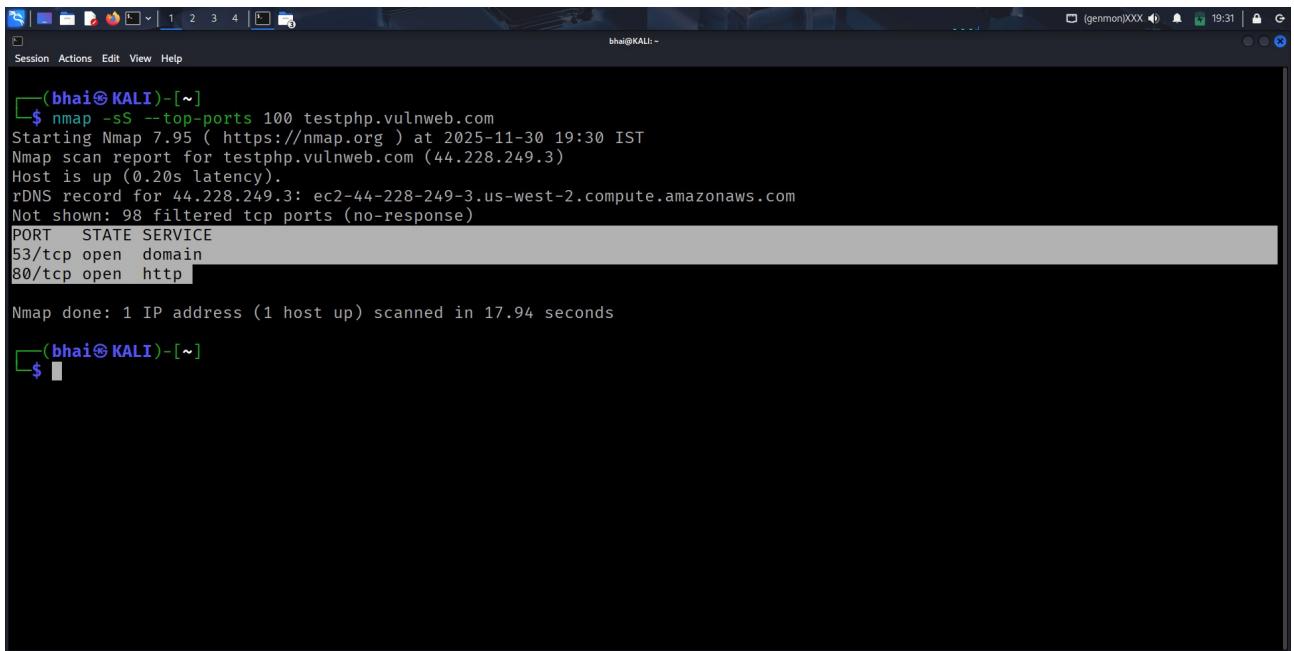
(bhai㉿KALI)-[~]
$
```

Host discovery result.

2. Port & Service Scan

Command

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



The screenshot shows a terminal window titled '(bhai㉿KALI)-[~]' running on a Kali Linux system. The user has run the command 'nmap -sS --top-ports 100 testphp.vulnweb.com'. The output indicates that the host is up and shows two open ports: 53/tcp (domain) and 80/tcp (http). The scan took 17.94 seconds.

```
(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

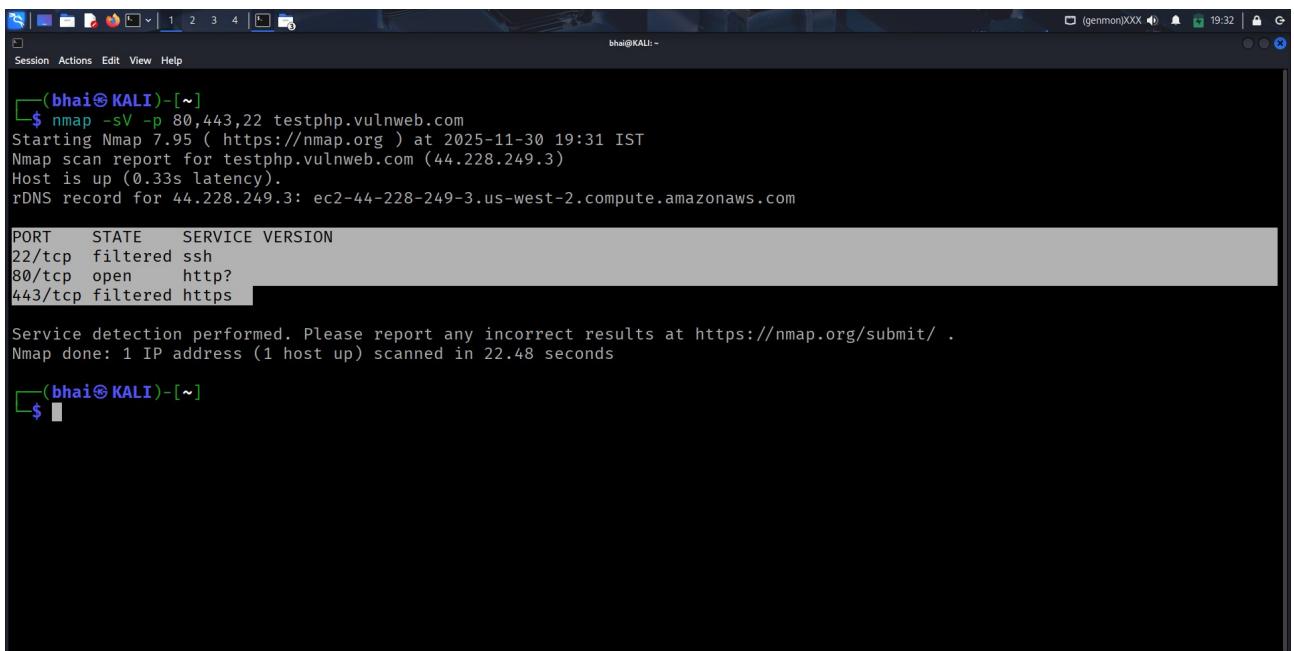
Nmap done: 1 IP address (1 host up) scanned in 17.94 seconds

(bhai㉿KALI)-[~]
$
```

Quick port scan result.

Command (Version detection on open ports)

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



The screenshot shows a terminal window titled '(bhai㉿KALI)-[~]' running on a Kali Linux system. The user has run the command 'nmap -sV -p 80,443,22 testphp.vulnweb.com'. The output shows version detection results for three ports: 22/tcp (filtered ssh), 80/tcp (open http), and 443/tcp (filtered https). The scan took 22.48 seconds.

```
(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
```

The screenshot shows a terminal window titled '(bhai@KALI)-[~]' with the command \$ nmap -O testphp.vulnweb.com. The output details a SYN Stealth Scan of the host testphp.vulnweb.com (44.228.249.3). It reports that the host is up with 0.31s latency. An rDNS record for ec2-44-228-249-3.us-west-2.compute.amazonaws.com is shown. A table lists open ports: 53/tcp open domain. A warning about OS scan reliability is present, followed by aggressive OS guesses including Ubiquiti Dream Machine Pro gateway, Oracle VM Server, and various Linux distributions. The scan concludes with OS detection performed and a total duration of 86.30 seconds.

```
(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
```

```
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], Em ail[lws@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], Sc ript[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]

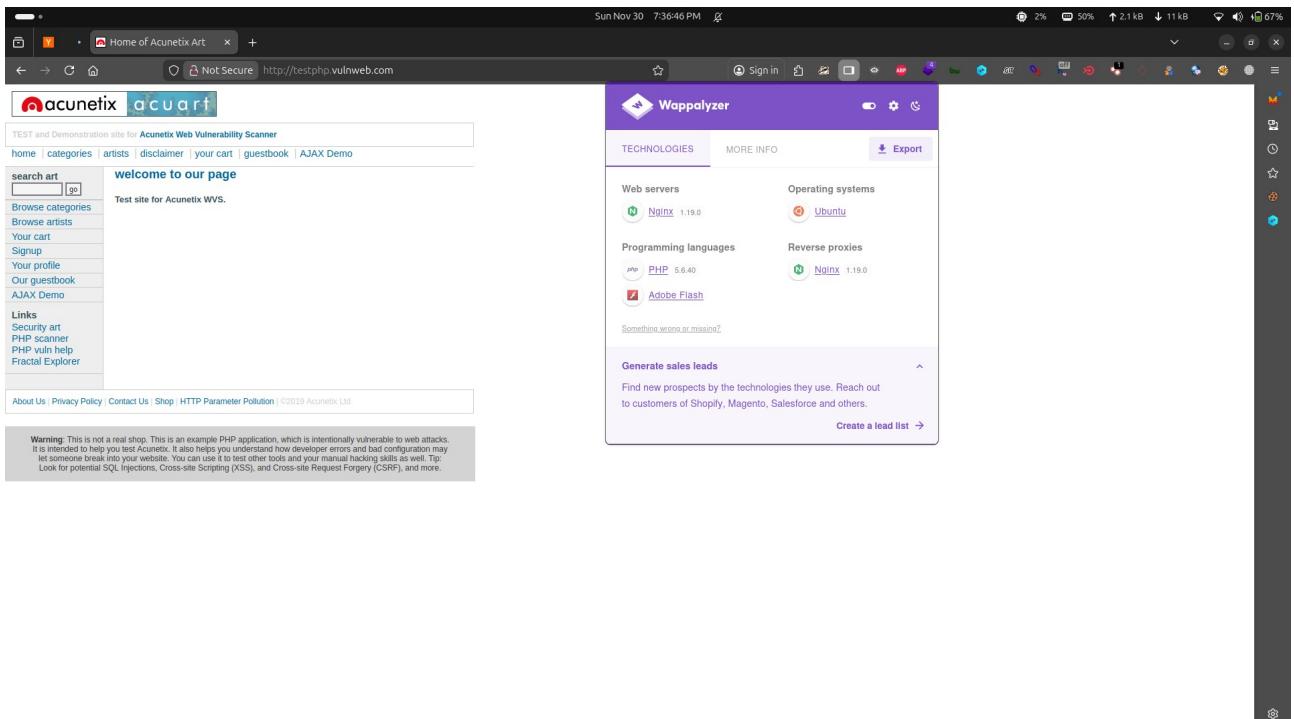
(bhai@KALI)-[~]
$
```

Web fingerprinting result.

2. Wappalyzer

Install Chrome/Firefox extension → open:

<http://testphp.vulnweb.com>



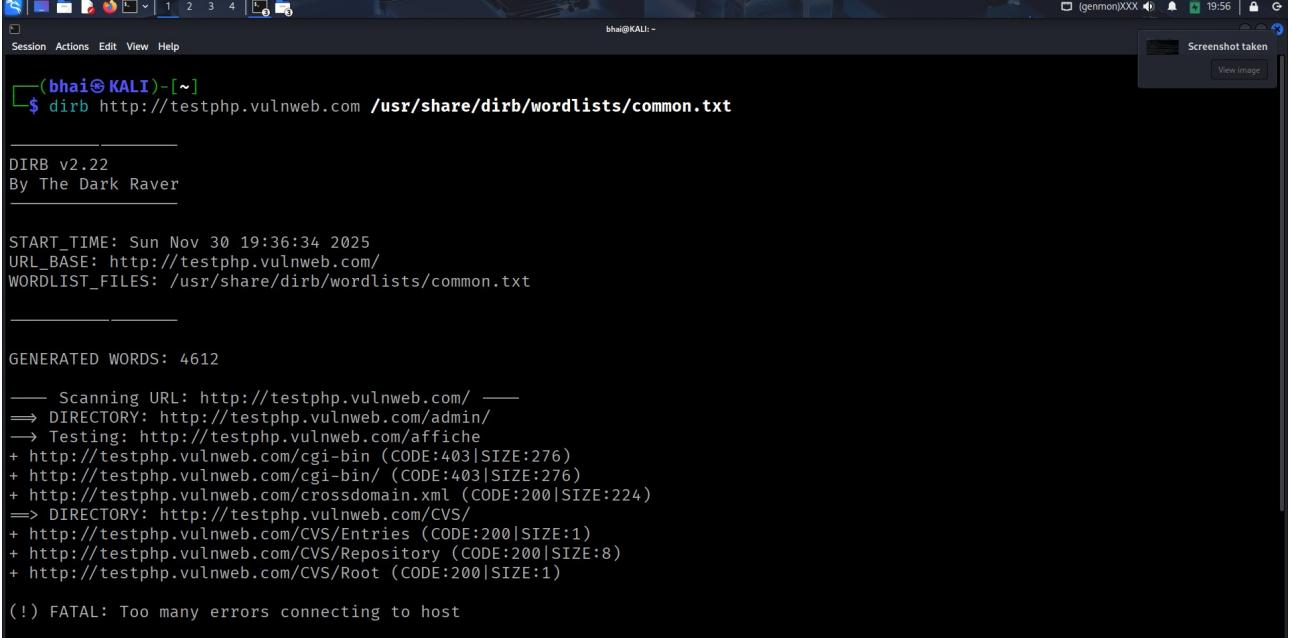
Wappalyzer tech detection.

◆ Step 3 — Directory Discovery

Dirb

Command

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



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal window has a dark background and light-colored text. It displays the output of the Dirb command. The output includes the version information (DIRB v2.22), the start time (Sun Nov 30 19:36:34 2025), the URL base, the wordlist file used, and the generated words count (4612). The main part of the output shows the results of the directory scan, including successful directory finds (like /admin/ and /CVS/) and testing results for various files like cgi-bin and crossdomain.xml. A fatal error message at the end indicates too many errors connecting to the host.

```
(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
```

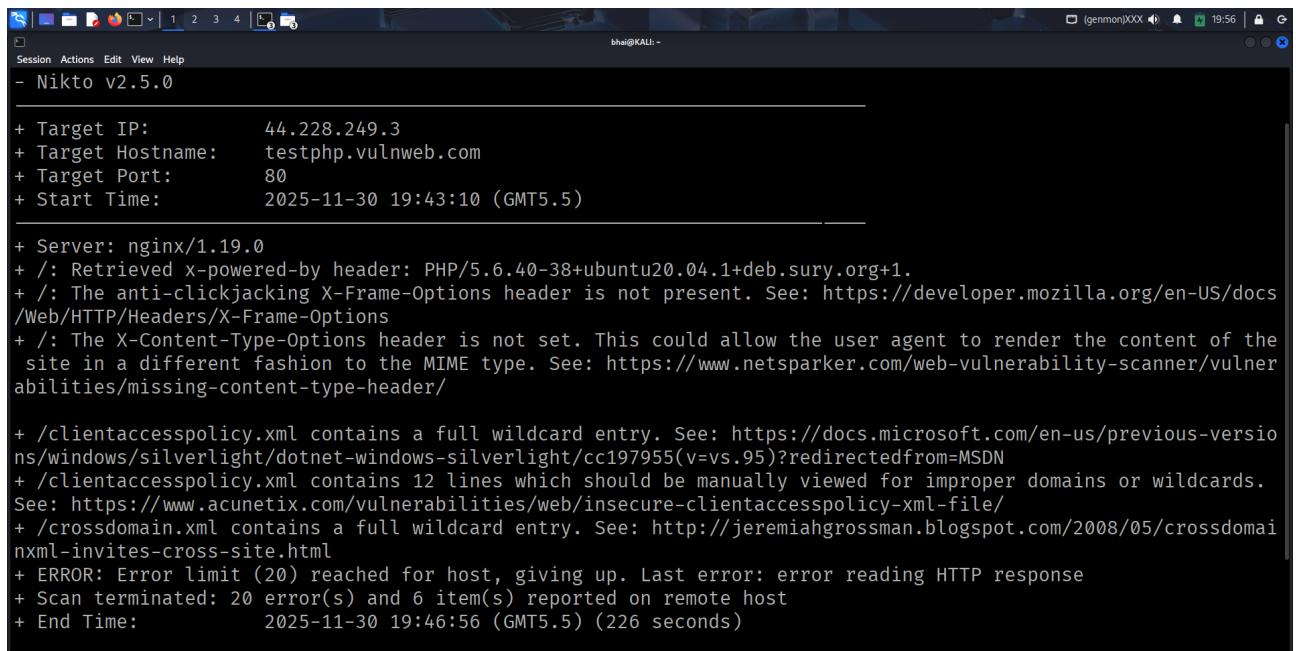
Directory brute-force results.

◆ Step 4 — Light Automated Scans

1. Nikto

Command

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



The screenshot shows a terminal window titled 'Session Actions Edit View Help' with the command 'nikto -h http://testphp.vulnweb.com -o nikto.txt'. The output is as follows:

```
bhai@Kali:~$ 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/5.6.40-38+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/crossdomain-xml-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
```

Nuclei scan findings.

3. OWASP ZAP Baseline Scan

Command

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

The screenshot shows the ZAP 2.15.0 interface with the title bar "Untitled Session - 20251130-204547 - ZAP 2.15.0". The menu bar includes File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and Standard Mode. Below the menu is a toolbar with icons for Quick Start, Request, Response, Requester, Break, and Script Console. A logo for "Crash Override Open Source Fellowship" is in the top right. The main area has a heading "Automated Scan" and a sub-instruction "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 given permission to test." On the left, there's a "URL to attack:" field containing "http://testphp.vulnweb.com/", a "Use traditional spider:" checkbox checked, a "Use ajax spider:" dropdown set to "If Modern with Firefox Headless", and a "Progress:" status bar showing "Accessing URL". At the bottom, there are "Alerts" and "Current Scans" sections.

The screenshot shows the ZAP interface with the following details:

- File Edit View Analyse Report Tools Import Export Online Help**
- Standard Mode**
- Sites** (selected)
- Contexts**: Default Context
- URL to attack:** `http://testphp.vulnweb.com`
- Use traditional spider:**
- Use ajax spider:** If Modern with Firefox Headless
- Attack** and **Stop** buttons
- Progress:** Actively scanning (attacking) the URLs discovered by the spider(s)
- History**, **Search**, **Alerts**, **Output**, **Spider**, **Active Scan** tabs
- New Scan Progress:** 0 / http://testphp.vulnweb.com
- Current Scans:** 1 Num Requests: 24 New Alerts: 1
- Export** button
- Sent Messages** and **Filtered Messages** buttons
- Table of Scan Results:** Headers include ID, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size, Resp. Header, and Size, Resp. Body.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size	Resp. Header	Size	Resp. Body
9	3/01/25, 9:15:57 pm	30/11/25, 9:15:57 pm	GET	http://testphp.vulnweb.com/v4682356415220750839	404	Not Found	297 ms	155 bytes		153 bytes	
11	3/01/25, 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	3/01/25, 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	3/01/25, 9:15:57 pm	30/11/25, 9:15:58 pm	GET	http://testphp.vulnweb.com/?	200	OK	569 ms	256 bytes		4,958 bytes	
14	3/01/25, 9:16:50 pm	30/11/25, 9:16:50 pm	GET	http://testphp.vulnweb.com/WEB-INF/classes/10/0/...	404	Not Found	279 ms	155 bytes		153 bytes	
15	3/01/25, 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	3/01/25, 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	3/01/25, 9:16:20 pm	30/11/25, 9:16:21 pm	POST	http://testphp.vulnweb.com/stitemap.xml?d=allow_u...	404	Not Found	561 ms	155 bytes		153 bytes	
18	3/01/25, 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	3/01/25, 9:16:21 pm	30/11/25, 9:16:22 pm	GET	http://testphp.vulnweb.com/stitemap.xml	404	Not Found	676 ms	155 bytes		153 bytes	
20	3/01/25, 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	3/01/25, 9:16:25 pm	30/11/25, 9:16:26 pm	GET	http://testphp.vulnweb.com/stitemap.xml	404	Not Found	549 ms	155 bytes		153 bytes	
22	3/01/25, 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	3/01/25, 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	3/01/25, 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	3/01/25, 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	3/01/25, 9:16:26 pm	30/11/25, 9:16:27 pm	GET	http://testphp.vulnweb.com/stitemap.xml?name=abc	404	Not Found	567 ms	155 bytes		153 bytes	
27	3/01/25, 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	3/01/25, 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	3/01/25, 9:16:29 pm	30/11/25, 9:16:29 pm	GET	http://testphp.vulnweb.com/stitemap.xml?class.mod...	404	Not Found	271 ms	155 bytes		153 bytes	

Header: Text | Body: Text

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 30 Nov 2025 15:45:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1-deb.sury.org+1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

Charset Mismatch (Header Versus Meta Content-Type Charset)
URL: http://testphp.vulnweb.com
Risk: Informational
Confidence: Low
Parameter:
Attack:
Evidence:
CWE ID: 436
WASC ID: 15
Source: Passive (90011 - Charset Mismatch)
Input Vector:
Description:
This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set.
Other Info:
There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-2] do not match.
Solution:
Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.

Reference:

Alerts 9 | 1 3 3 | 2 Main Proxy: localhost:8080 | ZAP out of date!

Header: Text | Body: Text

HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 30 Nov 2025 15:45:35 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1-deb.sury.org+1

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html><!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php" codeOutsideHTMLIsLocked="false" -->
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

Cross Site Scripting (DOM Based)
Absence of Anti-CSRF Tokens
Content Security Policy (CSP) Header Not Set
Missing Anti-clickjacking Header
Server Leaks Version Information via "Server":
X-Content-Type-Options Header Missing
Charset Mismatch (Header Versus Meta Content-Type)
User Agent Fuzzer (5)

CWE ID: 200
WASC ID: 13
Source: Passive (10037 - Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s))
Input Vector:
Description:
The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Other Info:
Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Solution:
Reference:
Alert Tags:

Key	Value
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/

Alerts 9 | 1 3 3 | 2 Main Proxy: localhost:8080 | ZAP out of date!

ZAP baseline scan report generated.

4. WPScan

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

Command

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


```
bhai@KALI:~$ wpscan --url https://vulnerable-wp.speedywp.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, @firegart

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

bhai@KALI:~$
```

WordPress scan results.