Ex. No.: 4 **Date:** 20 . 09 . 2024

SQL INJECTION LAB

Aim:

To do 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

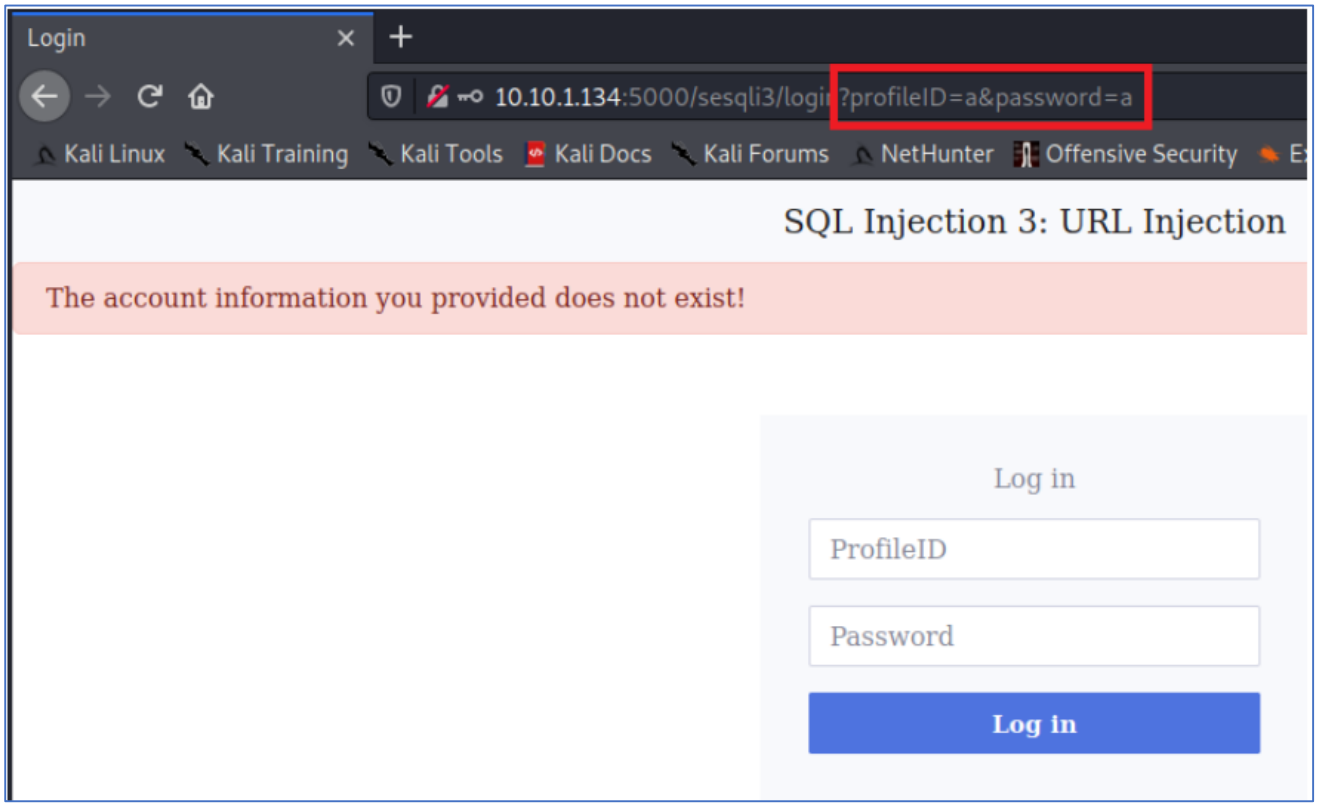
   c) URL Injection

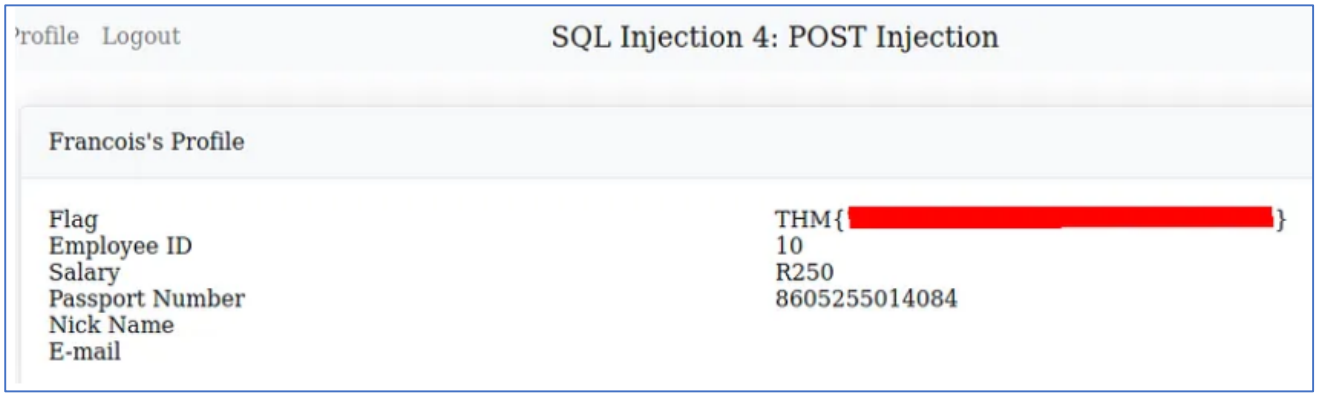
   d) POST Injection

   e) UPDATE Statement
4. Perform broken authentication of login forms with blind SQL injection to extract admin password
5. Perform UNION-based SQL injection and exploit the vulnerable book search function to retrieve the flag

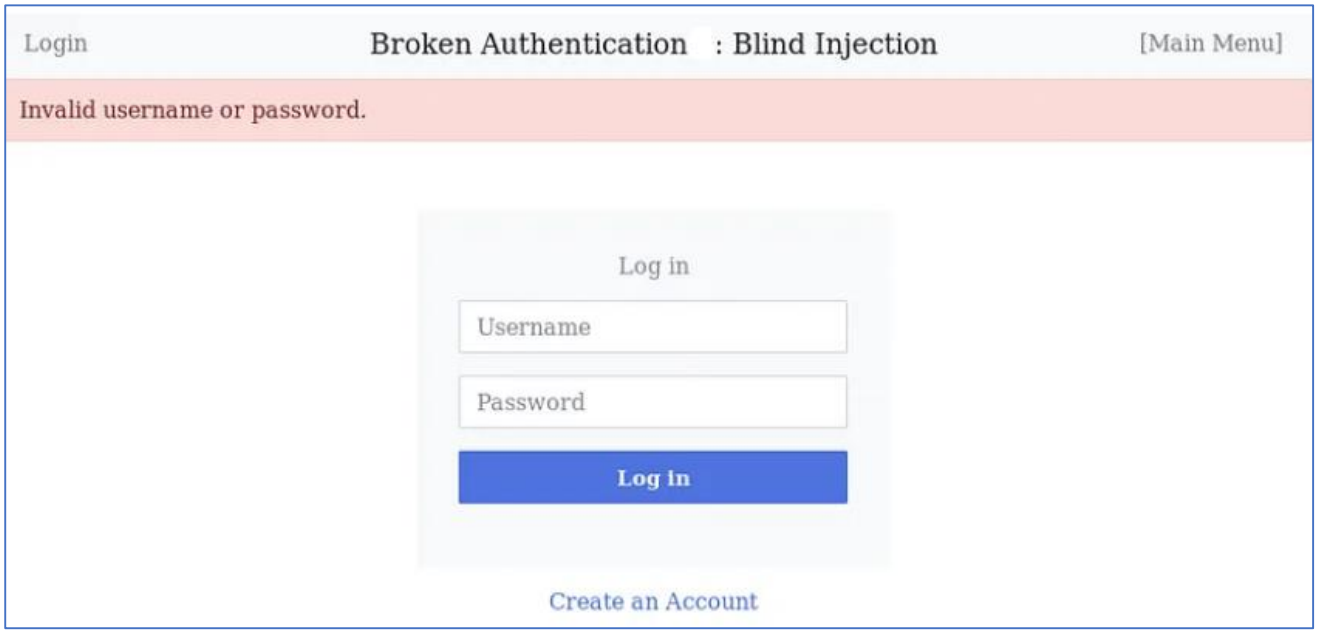
Output:

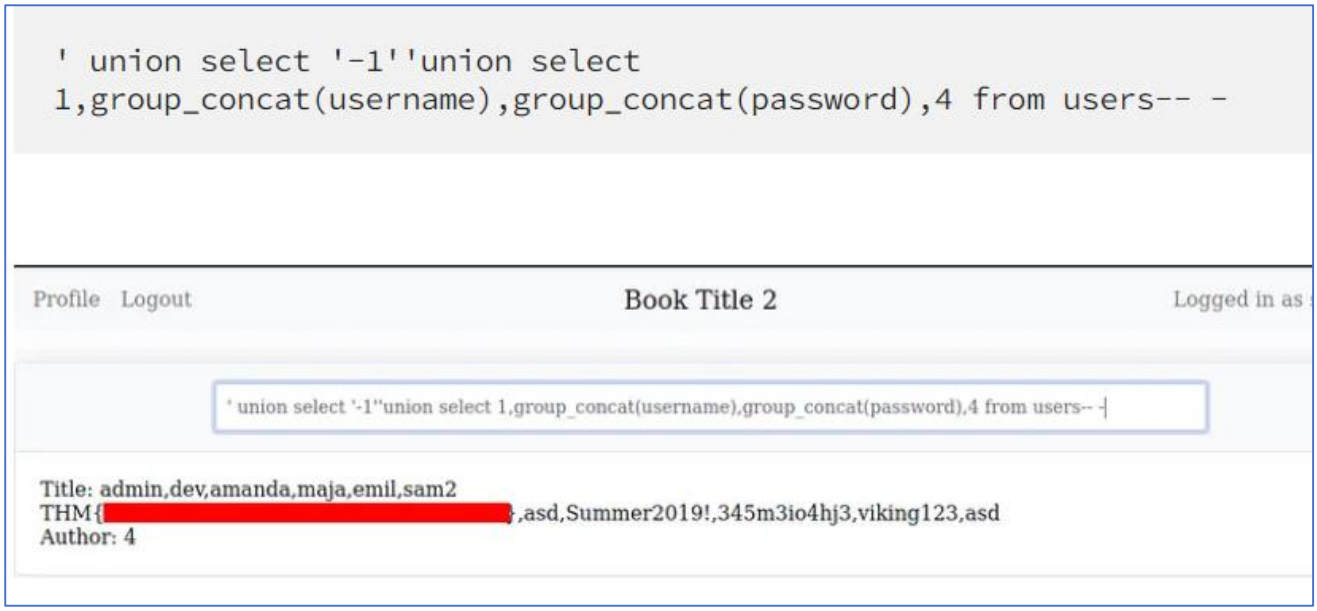

Log in
a' or 1=1 --
Log in
Profile Logout
SQL Injection 2: Input Box String
Francois's Profile
Flag
Employee ID
Salary
Passport Number
Nick Name
E-mail
THM{[redacted]}
10
R250
8605255014084


Login
10.10.1.134:5000/sesqli3/logi?profileID=a&password=a
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
SQL Injection 3: URL Injection
The account information you provided does not exist!
Log in
ProfileID
Password
Log in


rofile Logout
SQL Injection 4: POST Injection
Francois's Profile
Flag
Employee ID
Salary
Passport Number
Nick Name
E-mail
THM{[redacted]}
10
R250
8605255014084


SQL Injection 5: UPDATE Statement
Log in
10
Log in
Home
Edit Profile
Logout
SQL Injection 5: UPDATE Statement
Francois's Profile
Employee ID
Salary
Passport Number
Nick Name
E-mail
10
R250
8605255014084





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