

Ex. No.: 4

Date:20/08/2024

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
5. password
6. Perform UNION-based SQL injection and exploit the vulnerable book
7. search function to retrieve the flag

Output:

The screenshot shows the TryHackMe SQL Injection Lab interface. The browser address bar displays tryhackme.com/r/room/sqlilab. The page header includes navigation links (Dashboard, Learn, Complete, Other), a search bar, and a 'Go Premium' button. The main content area features a 'SQL Injection Lab' title, a brief description, and a 'Start AttackBox' button. Below this, a list of tasks is displayed, each with a green checkmark indicating completion. The tasks are:

- Task 1: Introduction
- Task 2: Introduction to SQL Injection: Part 1
- Task 3: Introduction to SQL Injection: Part 2
- Task 4: Vulnerable Startup: Broken Authentication
- Task 5: Vulnerable Startup: Broken Authentication 2
- Task 6: Vulnerable Startup: Broken Authentication 3 (Blind Injection)
- Task 7: Vulnerable Startup: Vulnerable Notes
- Task 8: Vulnerable Startup: Change Password
- Task 9: Vulnerable Startup: Book Title
- Task 10: Vulnerable Startup: Book Title 2

At the bottom, a table provides room statistics:

Created by	Room Type	Users in Room	Created
Fafa	Free Room. Anyone can deploy virtual machines in the room (without being subscribed!)	39,777	1393 days ago

Messages

Executed Query:

Query 1:
SELECT id, username FROM users WHERE username = " union select 1,group_concat(password) fr

Log in

admin'-- {

admin'-- -

Password

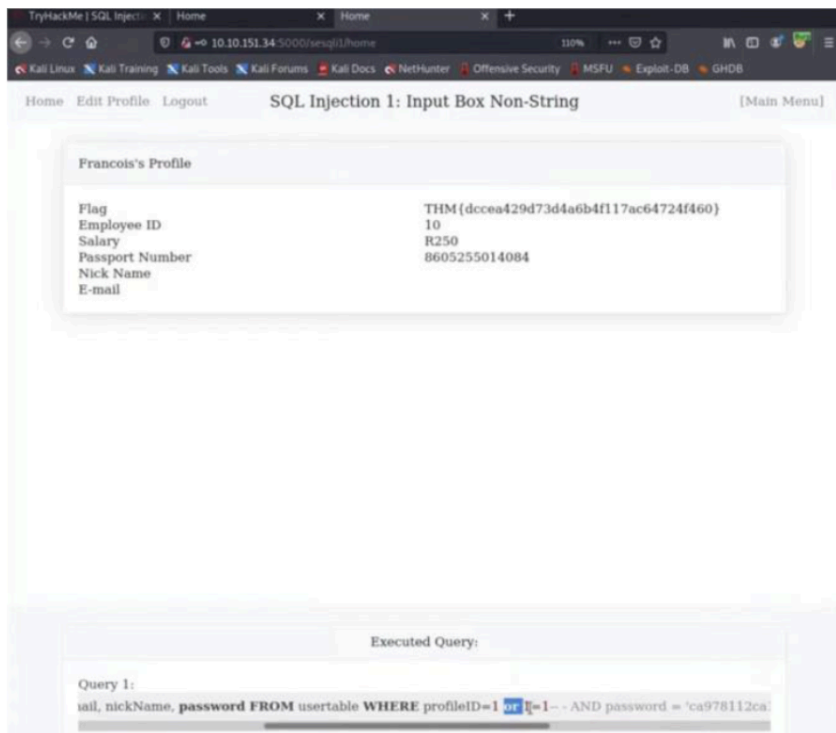
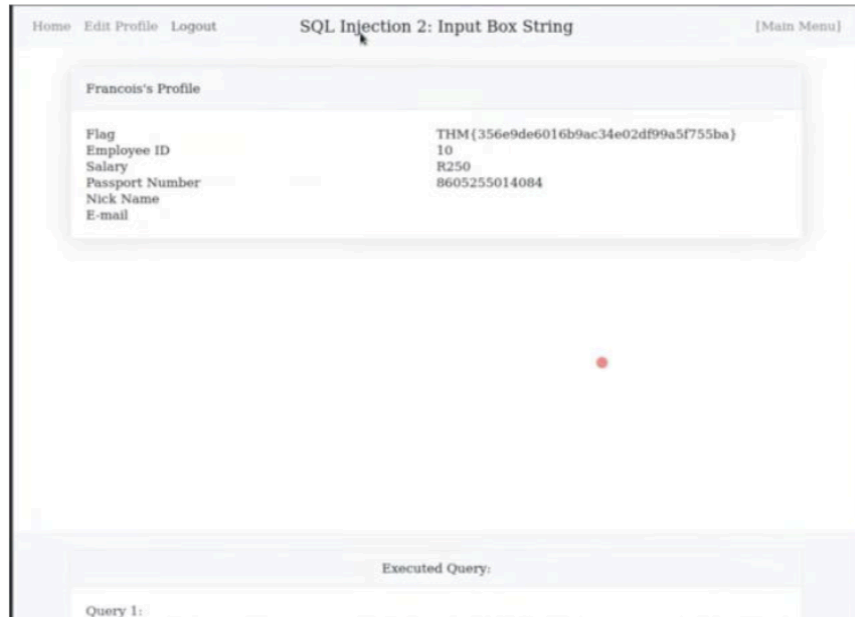
Log in

Create an Account

Executed Query:

Query 1:
SELECT username FROM users WHERE username=?
Parameters:
admin'-- -

Query 2:
INSERT INTO users (username, password) VALUES (?, ?)
Parameters:
admin'-- -, aaa



Result:

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