

**NAME:V.VENSELVAM**

**Ex. No: 4**

**ROLL NO:231901061**

## **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 Attack Box to run the instance of Kali Linux 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:

## SQL INJECTION LAB

The screenshot displays the TryHackMe SQL Injection Lab interface. At the top, the navigation bar includes the TryHackMe logo, links to Dashboard, Learn, Compete, and Other, and buttons for Access Machines, Go Premium, and a user profile icon. A tooltip indicates that pressing and holding the Esc key will exit full screen. The main header shows the path 'Learn > SQL Injection Lab' and the lab title 'SQL Injection Lab' with a description: 'Understand how SQL injection attacks work and how to exploit this vulnerability.' The lab is rated 'Easy' and takes '0 min'. Below this, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', a like count of 1348, and an 'Options' dropdown. A green progress bar indicates 'Room completed (100%)'. The task list on the right includes seven tasks, all marked as completed with green checkmarks: 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)), and Task 7 (Vulnerable Startup: Vulnerable Notes). A chat icon is visible in the bottom right corner.

TryHackMe Dashboard Learn Compete Other

Access Machines Go Premium 1

To exit full screen, press and hold Esc

Learn > SQL Injection Lab

### SQL Injection Lab

Understand how SQL injection attacks work and how to exploit this vulnerability.

Easy 0 min

Share your achievement Start AttackBox Help Save Room 1348 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

**Result:**

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