

**Name: SASIKUMAR.B**

**Ex. No: 4**

**Roll no:231901047**

## **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 'SQL Injection' lab interface. At the top, a dark header bar contains the lab title 'SQL Injection' with a sub-description 'Learn how to detect and exploit SQL Injection vulnerabilities'. It also shows a difficulty level of 'Medium' and a time limit of '30 min'. Below the header, a row of buttons includes 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', a notification for '4589' likes, and an 'Options' dropdown. A green progress bar indicates 'Room completed (100%)'. The main content area lists ten tasks, each with a green checkmark indicating completion: Task 1 (Brief), Task 2 (What is a Database?), Task 3 (What is SQL?), Task 4 (What is SQL Injection?), Task 5 (In-Band SQLi), Task 6 (Blind SQLi - Authentication Bypass), Task 7 (Blind SQLi - Boolean Based), Task 8 (Blind SQLi - Time Based), Task 9 (Out-of-Band SQLi), and Task 10 (Remediation). Each task bar has a downward arrow on the right side.

**Result:**

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