

Name: UDAYA SANKAR C

Ex. No: 4

Roll no:231901058

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 a user profile section with 'Access Machines', a search icon, a notification bell, a 'Go Premium' button, a '1' badge, and a user initial 'U'. The main header area shows the path 'Learn > SQL Injection Lab' and the lab title 'SQL Injection Lab' with a sub-description 'Understand how SQL injection attacks work and how to exploit this vulnerability.' It also indicates the difficulty as 'Easy' and the estimated time as '0 min'. A green bar below the header states 'Room completed (100%)'. The main content area lists seven tasks, each with a green checkmark icon and a dropdown arrow: 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. A small circular icon is visible in the bottom right corner.

Result:

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