

Name: MOHAMED ARSATH A

Ex. No: 4

Roll no:231901030

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 on the TryHackMe platform. The top navigation bar includes links for 'Dashboard', 'Learn', 'Compete', and 'Other', along with a 'Go Premium' button and a user profile icon. The main header area features the 'SQL Injection Lab' title, a brief description, and a difficulty level of 'Easy' with an estimated time of '0 min'. A list of tasks is presented below, each with a green checkmark indicating completion. The tasks are: 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; Task 9: Vulnerable Startup: Book Title. A green bar at the bottom of the task list indicates 'Room completed (100%)'. The interface is dark-themed with a light green accent color.

TryHackMe

Dashboard Learn Compete Other

Access Machines Go Premium 1

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
- Task 8 Vulnerable Startup: Change Password
- Task 9 Vulnerable Startup: Book Title

Result:

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