

Ex. No.: 4

Date:

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

The screenshot shows the TryHackMe web application interface for the 'SQL Injection' room. The header includes navigation links like 'Dashboard', 'Learn', 'Complete', and 'Other', along with a 'Go Premium' button. The main content area features a 'SQL Injection' title, a brief description, and a list of 10 tasks. The tasks are: 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. The room is created by 'tryhackme' and '000gic', and it is a 'Free Room' where anyone can deploy virtual machines. The interface also shows the number of users in the room (164,494) and the creation date (1141 days ago). The bottom of the screen displays a Windows taskbar with various application icons and system information like 'P 500 05%' and '20:32 18-11-2024'.

tryhackme.com/r/room/sqlinjection

TryHackMe

Dashboard Learn Complete Other

Access Machines Go Premium

SQL Injection

Learn how to detect and exploit SQL injection vulnerabilities

Medium 30 min

Share your achievement Start AttackBox Help Save Room 4584 Options

Room completed (100%)

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

Task 10: Remediation

Created by tryhackme 000gic

Room Type Free Room. Anyone can deploy virtual machines in the room (without being subscribed)

Users in Room 164,494

Created 1141 days ago

English (India) English (India)

To switch input methods, press Windows key + space.

P 500 05%

Search

ENG IN

20:32 18-11-2024

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