TryHackMe SQL Injection Lab - Beginner's Guide

What is SQL Injection?

SQL Injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It can be used to bypass login pages, extract data, and even gain admin access.

Hacker Mindset

Think like a curious child:

- What if I type weird things into the login box?

- Can I break the system logic?

- What if it gives me an error?

- Is it showing me too much information?

Tools Needed

- Web browser with DevTools (Inspect Element)

- TryHackMe account (free)

- Burp Suite Community Edition (for interception - optional)

- Notepad for taking notes

Step-by-Step Lab Instructions

1. Go to https://tryhackme.com/room/sqlinjectionlm and join the room.

2. Click 'Start Machine' to boot the target.

3. Access the public IP in your browser.

4. You'll see a login page. Try injecting in the username:

   - Username: ' OR 1=1 --

   - Password: (leave blank)

5. If successful, you're in without credentials!

6. Try different payloads like:

   - ' UNION SELECT NULL, NULL --

   - ' AND 1=1 --

   - ' AND 1=2 --

Common Payloads

- ' OR 1=1 --

- ' AND 1=1 --

- ' UNION SELECT NULL, NULL --

- admin' --

How to Fix SQLi

- Use Prepared Statements / Parameterized Queries

- Input Validation (Whitelist inputs)

- Least Privilege Principle in DB access

- Use WAF (Web Application Firewall)

What to Document in GitHub

- Your findings from the lab

- Payloads that worked

- Screenshots (if possible)

- What you learned

- How to fix the issue