AUTOMATING SQL INJECTION USING SQLMAP

Project Objective: Learn how to automate SQL Injection using SQLmap.
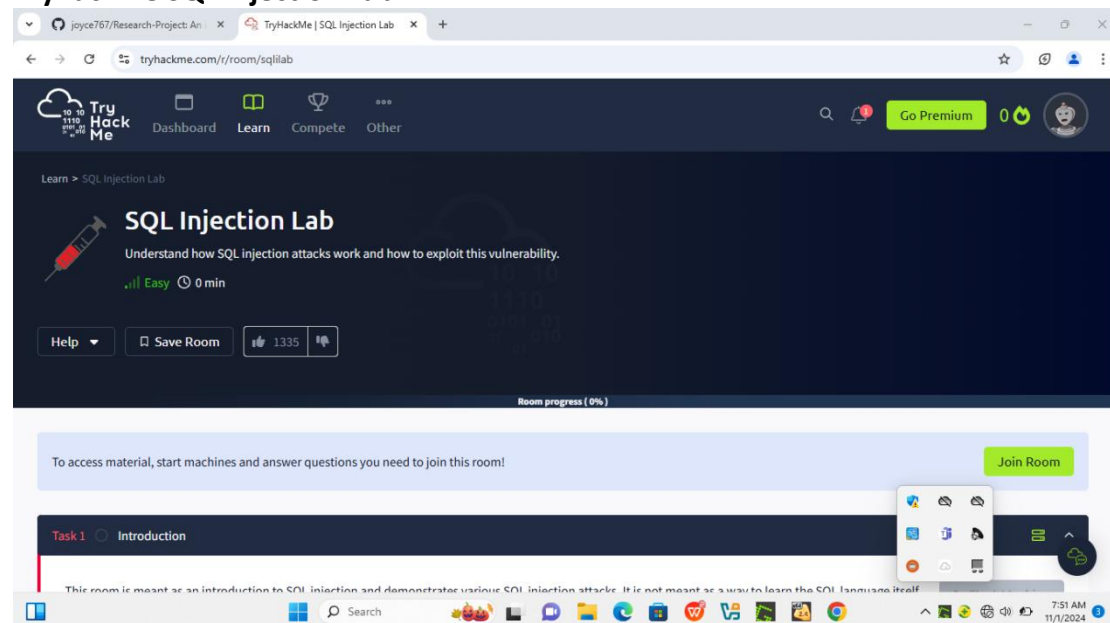**Project site: https://tryhackme.com/room/sqlilab**
Tryhackme.com offers virtual Linux node (AttackBox) to access their target systems.
Also, OPENVPN connection is available. AttackBox contains SQLmap and any other
necessary tools that we will need during this lab project.
SQL Injection consists of insertion or injection of a SQL Query via the input data
from the client to the application.
SQLmap is an open-source tool used as part of a penetration test to detect and
exploit injection flaws.

Tryhackme SQL Injection Lab

Intiating the lab

Starting Machine

Starting ATTACKBOX

Initiating the AttackBox
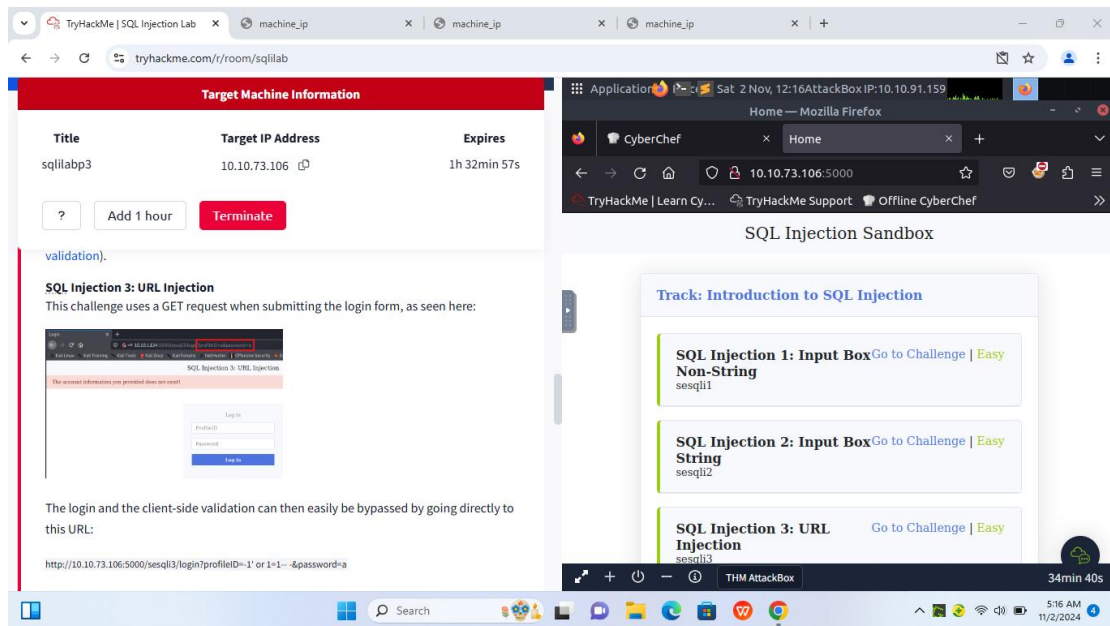
Using the Target IP Address to the website, and port number. The web page consists of labs with different SQL vulnerabilities.
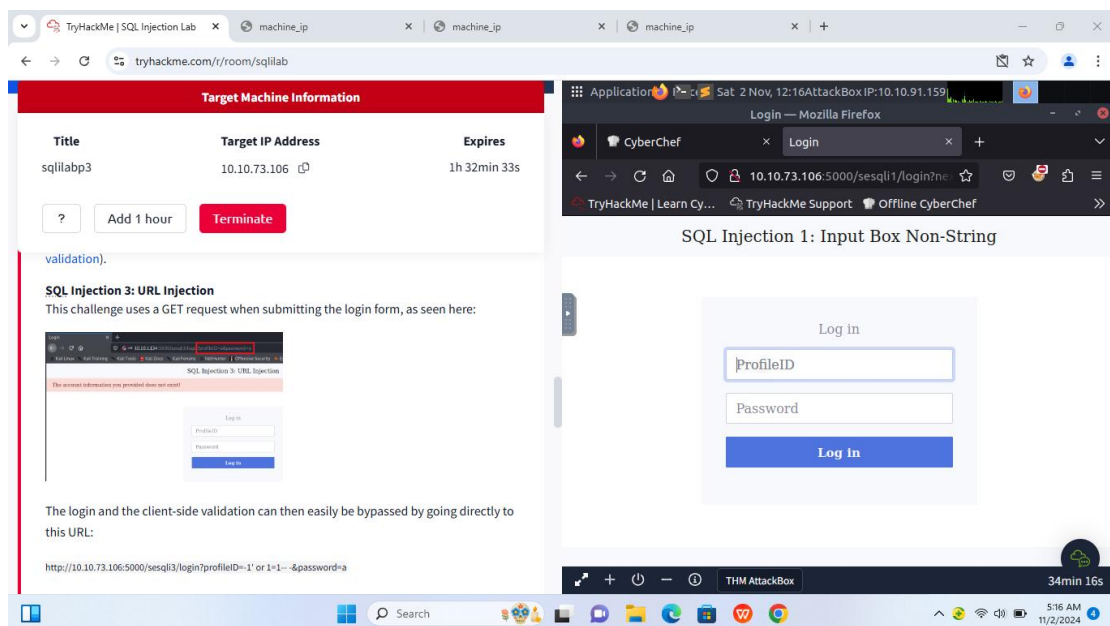
Login in with the profileID and password to test its vulnerability.This login form is vulnerable to SQL Injection.

This presented a profile of the user

Using SQLmap

Target Machine Information

Title	Target IP Address	Expires
sqlilabp3	10.10.73.106	1h 14min 10s

[?] [Add 1 hour] [Terminate]

login form or submit a valid request and intercept it with a proxy tool such as

Burp Suite and modify it:

For information on how Burp Suite works, visit the Burp Suite room.

Answer the questions below

Applications Sat 2 Nov, 12:34 AttackBox IP:10.10.91.159

root@ip-10-10-91-159: ~

File Edit View Search Terminal Help

```
root@ip-10-10-91-159:~# sqlmap -u http://10.10.73.106:5000/sesqli1/login?p
rofileID=1%27%20or%201=1--%20-&password=a
```

THM AttackBox   15min 53s

Search

5:34 AM
11/2/2024