Lab 6 – Automating SQL injection using SQLmap

Lab Objective:

Automate SQL injection using SQLmap.

Lab Purpose:

SQLmap is an open-source tool used as part of a penetration test to detect and exploit injection flaws. SQLmap is particularly useful as it saves time by automating the process of detecting and exploiting SQL injection.

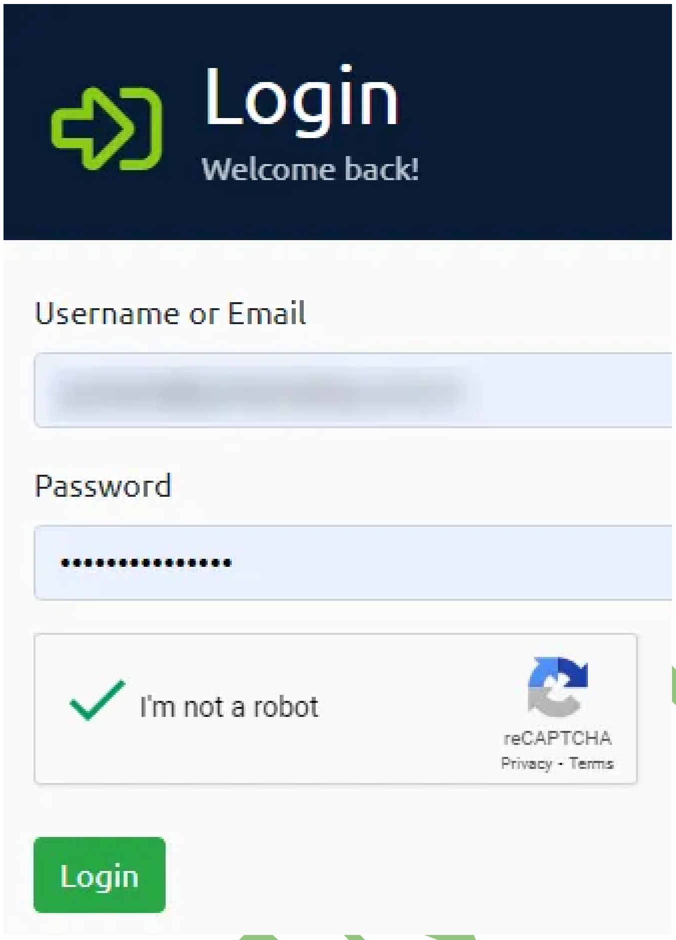
Lab Tool:

Reliable internet connection and a modern browser to connect
https://tryhackme.com/room/sqlilab

Lab Topology:

tryhackme.com offers virtual Linux node (AttackBox) to access their target systems. Also, OpenVPN connection is available. For simplicity in this lab, we will use AttackBox. AttackBox also contains SQLmap and any other necessary tools that we will need during this lab.

STEP ONE:
In order to use AttackBox, tryhackme.com requires membership login. Membership is free and very simple to set up. All that is required is an email address and a password.



Login
Welcome back!

Username or Email

[redacted]

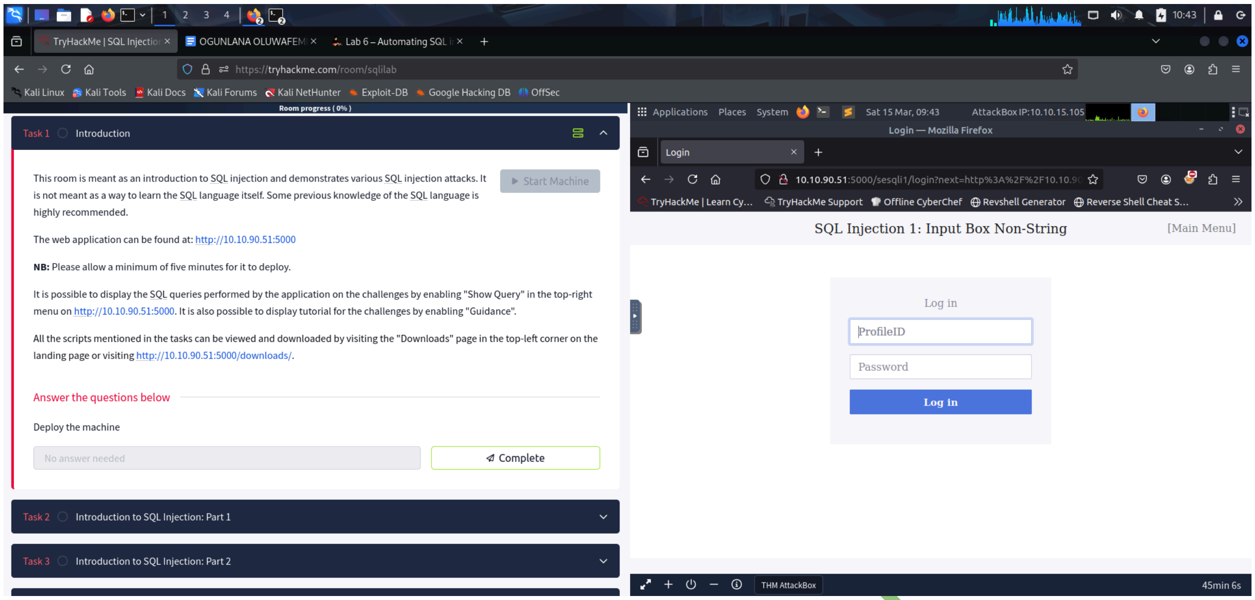
Password

•••••••••••••••

STEP 2:

Once you are on the AttackBox, open the web page with IP address and port number, which is provided on the left panel. In this case, http://10.10.90.51:5000

You will be presented with a webpage containing several labs with different SQL injection vulnerabilities. We will be focusing on the first one for this lab, so click on “go to challenge”.



Task 1 Introduction

This room is meant as an introduction to SQL injection and demonstrates various SQL injection attacks. It is not meant as a way to learn the SQL language itself. Some previous knowledge of the SQL language is highly recommended.

The web application can be found at: http://10.10.90.51:5000

NB: Please allow a minimum of five minutes for it to deploy.

It is possible to display the SQL queries performed by the application on the challenges by enabling "Show Query" in the top-right menu on http://10.10.90.51:5000. It is also possible to display tutorial for the challenges by enabling "Guidance".

All the scripts mentioned in the tasks can be viewed and downloaded by visiting the "Downloads" page in the top-left corner on the landing page or visiting http://10.10.90.51:5000/downloads/.

Answer the questions below

Deploy the machine

No answer needed

Task 2 Introduction to SQL Injection: Part 1

Task 3 Introduction to SQL Injection: Part 2

SQL Injection 1: Input Box Non-String [Main Menu]

Log in

ProfileID

Password

Log in

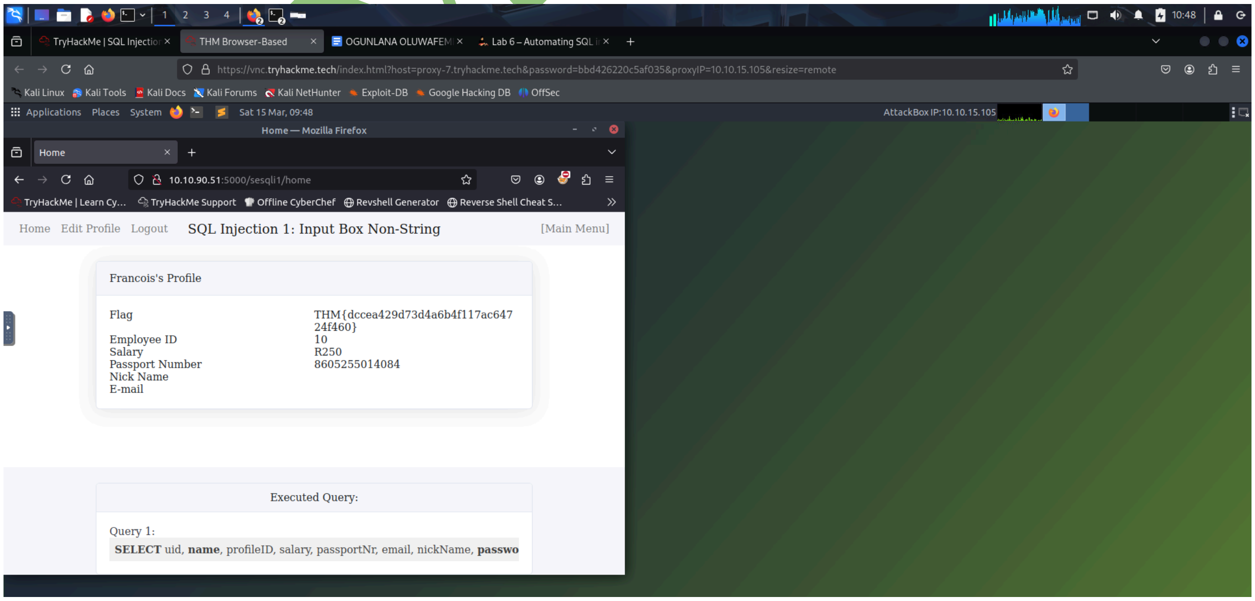
STEP 3:

You will be navigated to a sample login page which is vulnerable to SQL injection. We can test its vulnerability to SQL injection by inputting the following into the Profile ID text box:

“1 or 1=1– -“

Type the above string exactly, but without inverted commas.

Enter any random value into the password field and submit.



Home Edit Profile Logout SQL Injection 1: Input Box Non-String [Main Menu]

Francois's Profile

Flag	THM{dccea429d73d4a6b4f117ac647 24f460}
Employee ID	10
Salary	R250
Passport Number	8605255014084
Nick Name	
E-mail	

Executed Query:

Query 1:

```
SELECT uid, name, profileID, salary, passportNr, email, nickName, passwo
```

STEP 4:

We will then be logged into the application, and you should be able to see the flag for this challenge here.

So, we know this login form is vulnerable to SQL injection, but we want to know how to automatically test this using SQLmap. To do this, copy the link for the login page. Then, open a terminal in AttackBox and type the following:

```
sqlmap -u ‘http://10.10.101.165:5000/sesqli1/login?profileID=q&password=a’ -p ‘profileID’
–level=3 –risk=3
```

-u tells sqlmap the target URL

-p tells the tool which parameter in the URL we want to test for SQL injection

–level=3 will tell the tool to use more detailed and comprehensive SQL injection techniques

–risk=3 will tell the tool not to be subtle about its SQL injection attempt

Once this command is ran, you will notice SQLmap attempting a huge amount of SQL injection techniques against the target.