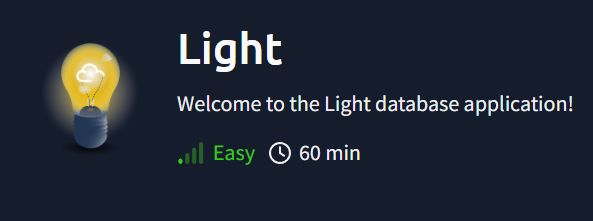
TRYHACKME – LİGHT

<https://tryhackme.com/room/lightroom>



Written by Vusal Isayev

# İntroduction

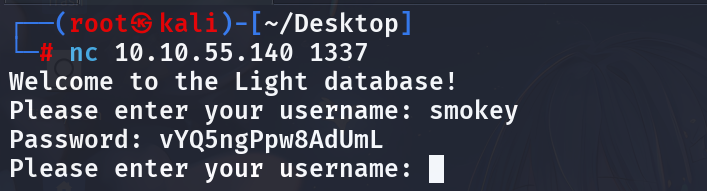
This lab belongs to the easy level SLQi. It asks us for 3 things as a task. These are the admin username, its password, and the flag in the system.

It tells us to connect to port 1337 to start. It also gives the username "smokey" to use.

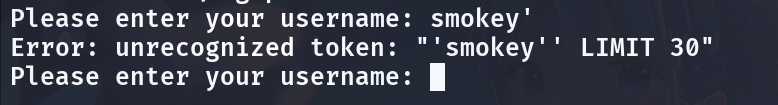
# Exploitation

We understand that the database used on name of CTF is sqlite.

Let's connect first:



It takes a username from us and returns a password accordingly.

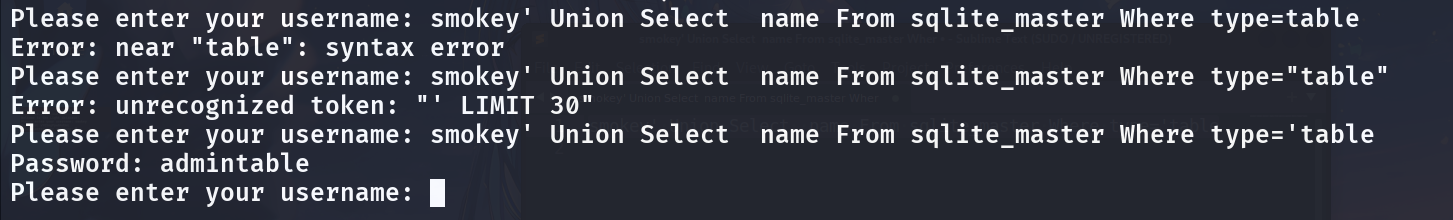


It gave us an error message when we used single quotes. So it could be Union-based SQLi here.

First, let's try to find out the table name. For this, let's prepare our payload:

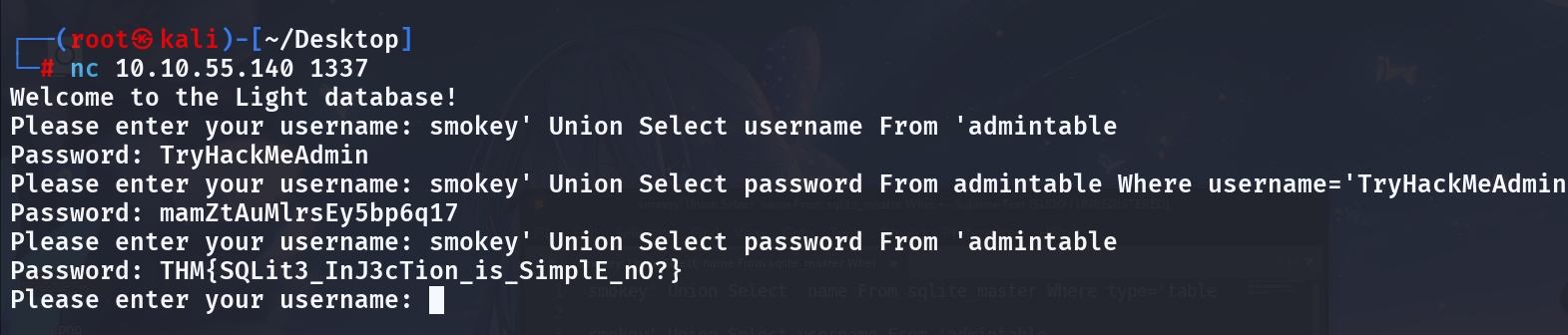


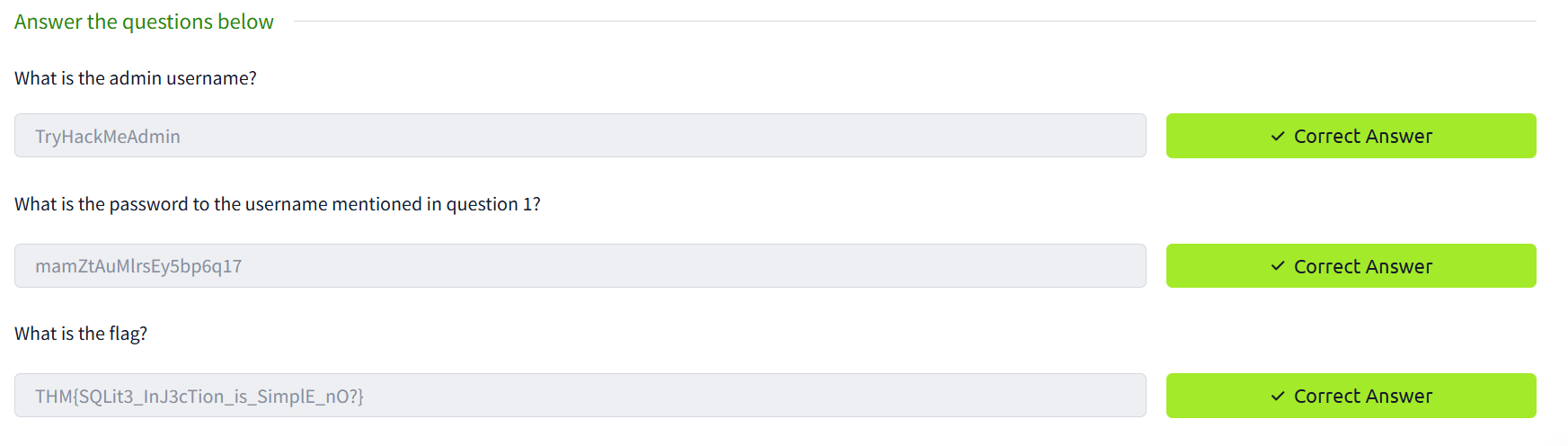
Oopss. They have implemented a filter to prevent SQLi. Let's try to bypass this:



And finally we got the answer.

Let's find the answers to the questions:





And we’re done.