RECOVERY [WEB]

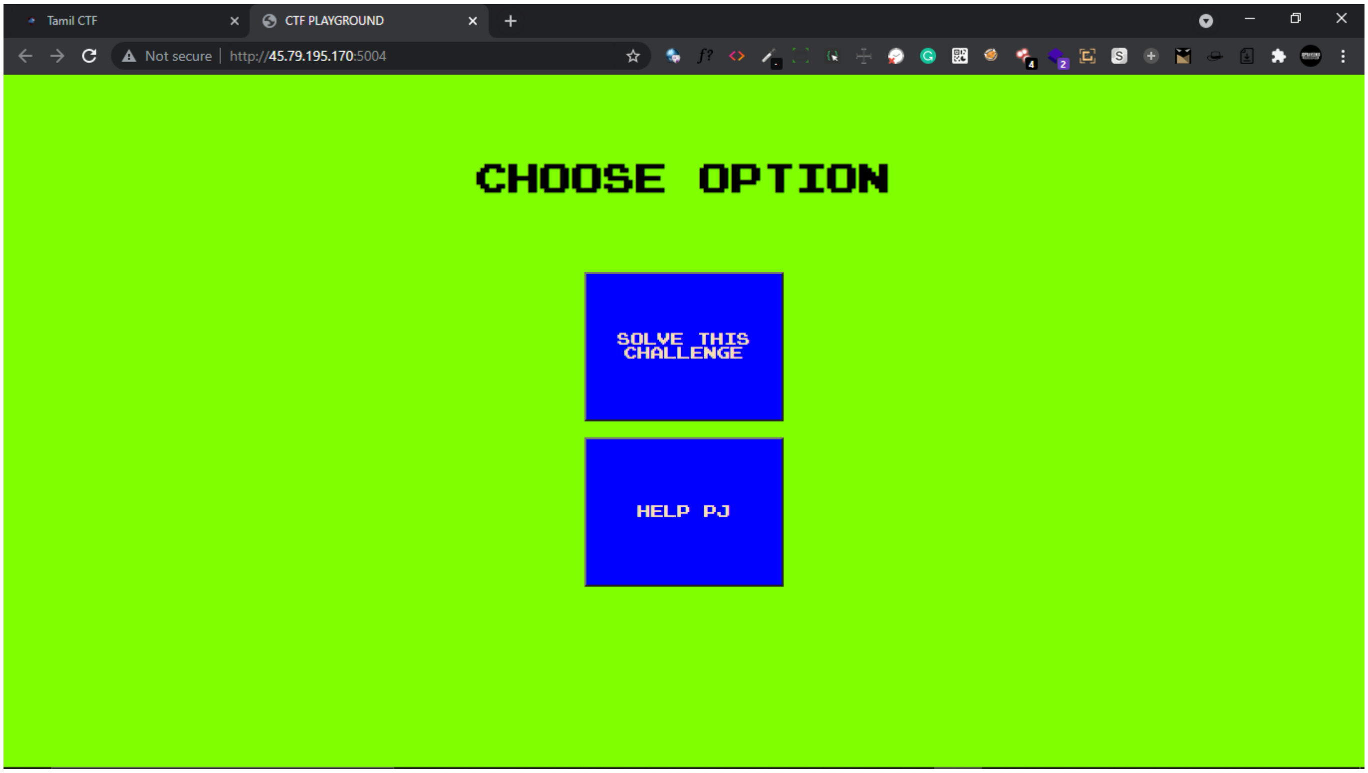
description:

Help PJ pls, he is a memory loss patient who forgot his password

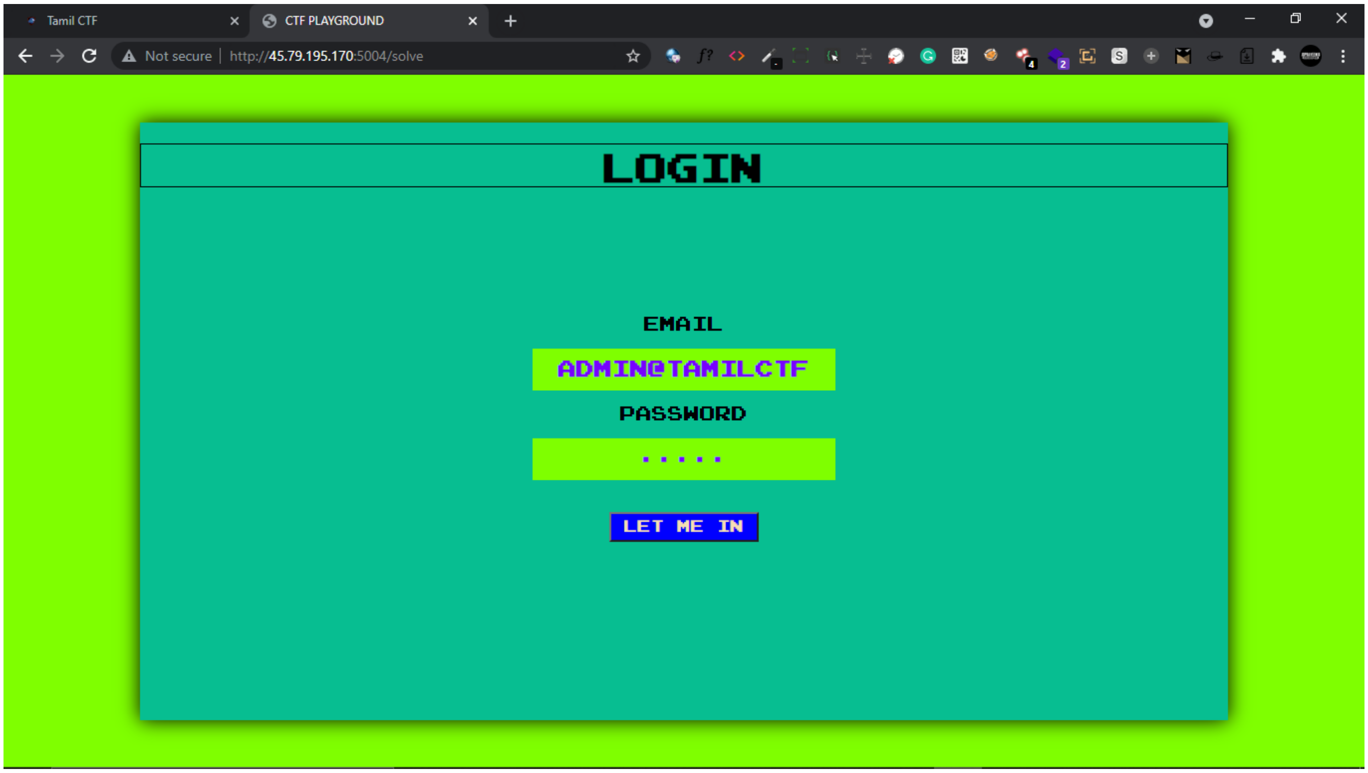
Try your hacking skills to help him

CHALLENGE WRITEUP

Starting page:



There are two options, first let's select option-1



Tamil CTF

CTF PLAYGROUND

Not secure | http://45.79.195.170:5004/solve

LOGIN

EMAIL

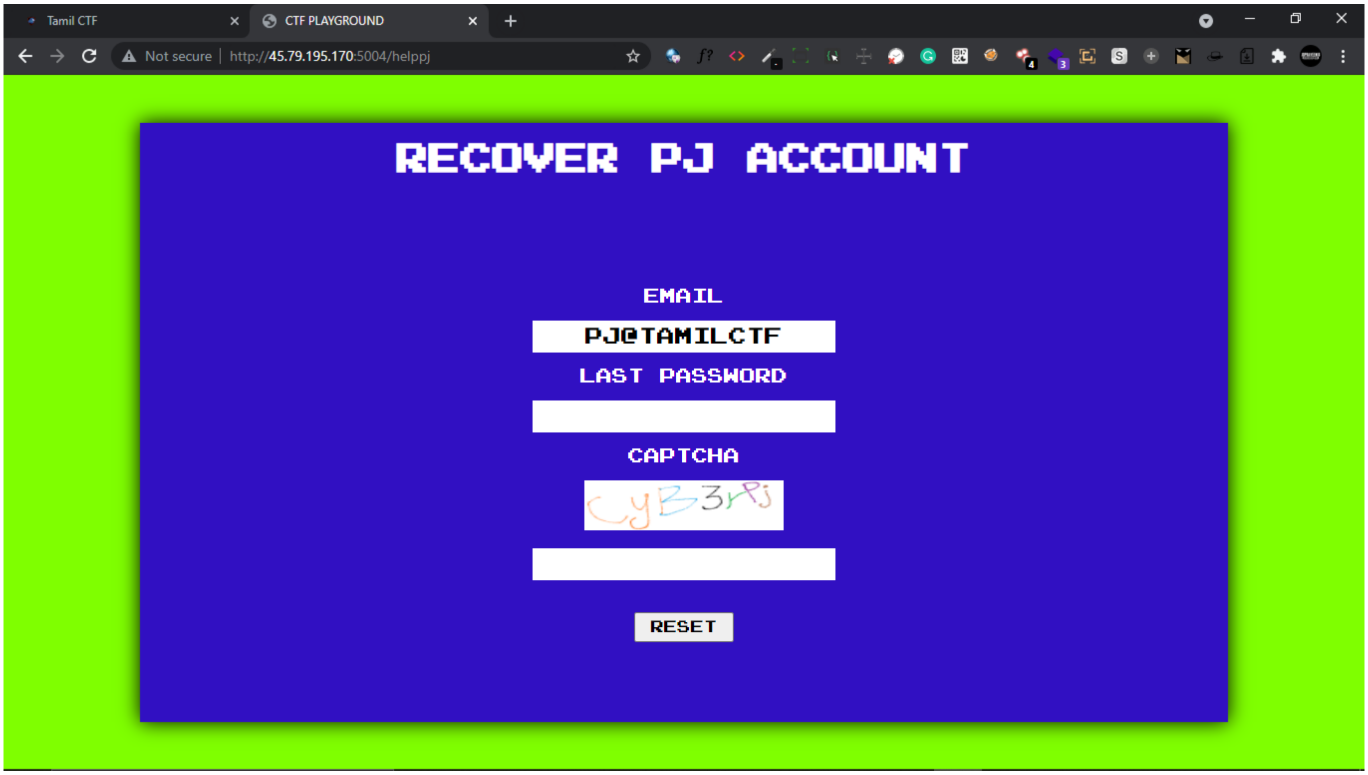
ADMIN@TAMILCTF

PASSWORD

.....

Looks like a login page, let's login with these default values.
when I click it, It returned to the starting page :(

Now let's select the option two **(help PJ)**



Tamil CTF

CTF PLAYGROUND

Not secure | http://45.79.195.170:5004/helppj

RECOVER PJ ACCOUNT

EMAIL

PJ@TAMILCTF

LAST PASSWORD

CAPTCHA

CyB3rPJ

Looks like PJ forgeted his password, let's try to help him.

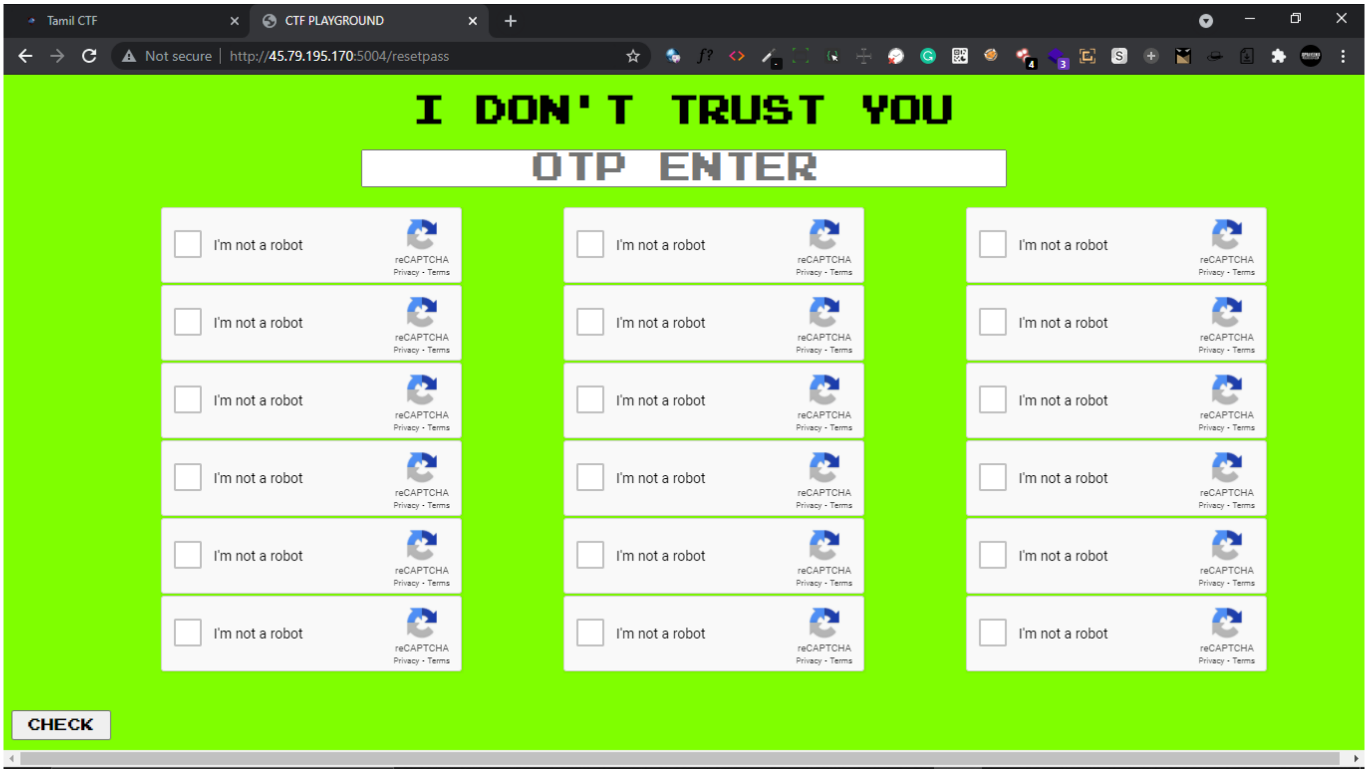
view source code of the form:

```html
<form action="/resetpass" method="POST">
<p>email</p>
<input style="font-family: 'Nintendoid1';" type="text" name="email"
value="pj@tamilctf">
<p>last password</p>
<!-- i think it's tamilctf123 -->
<input style="font-family: 'Nintendoid1';" type="text"
name="lastpass">
<p>captcha</p>
<img style="height: 50px;width: 200px;" src="[/static/captcha.png]
(http://127.0.0.1:5000/static/captcha.png)" alt="captcha"><br><br>
<input style="font-family: monospace;font-size:xx-large;" type="text"
name="captcha"><br><br><br>
<button style="font-family: 'Nintendoid1';height: 30px;width: 100px;"
type="submit">RESET</button>
</form>
```

Ok here we got everything

email: pj@tamilctf
last password: tamilctf123
captcha: cyB3rpj

Now let's click **RESET**

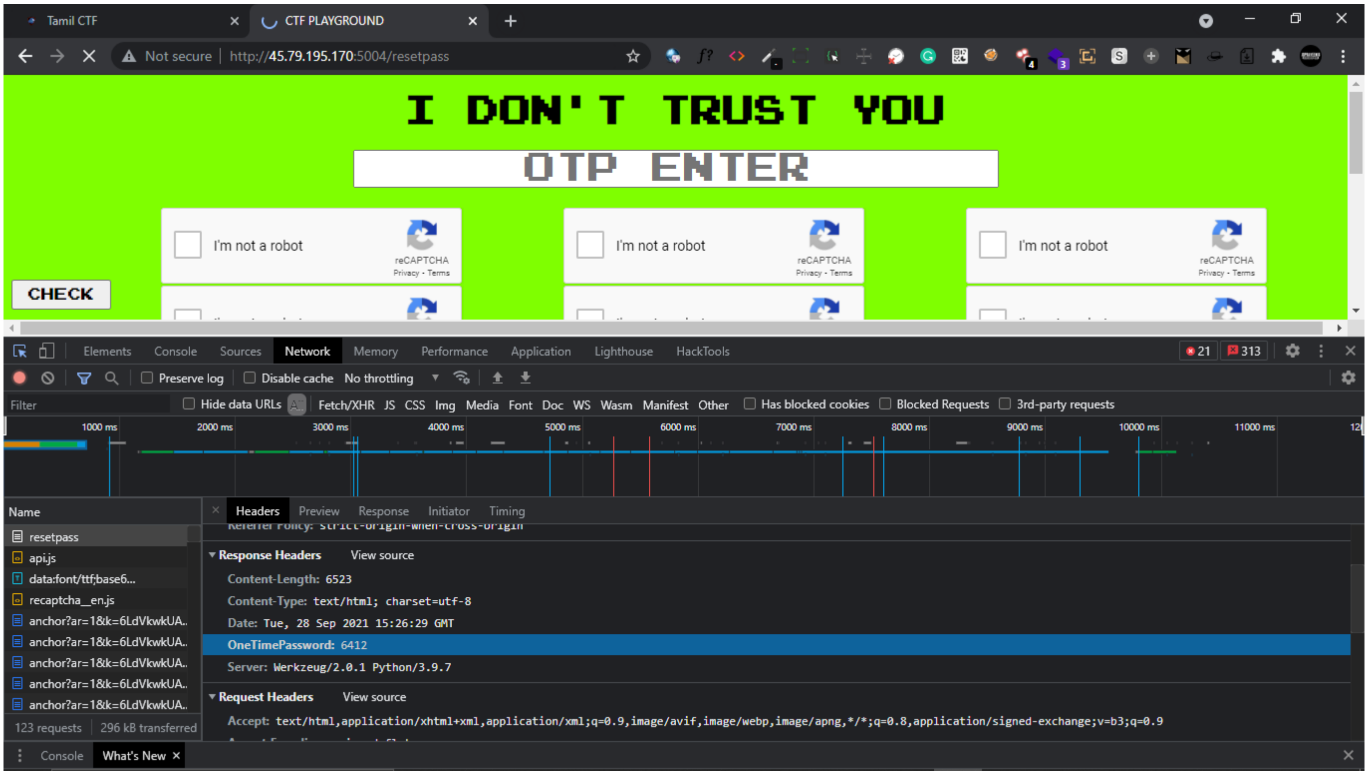


oh no so many checks, but all are rabbit holes..

Read the text in input field **OTP ENTER**

so looks like we need to type the otp and press enter to submit

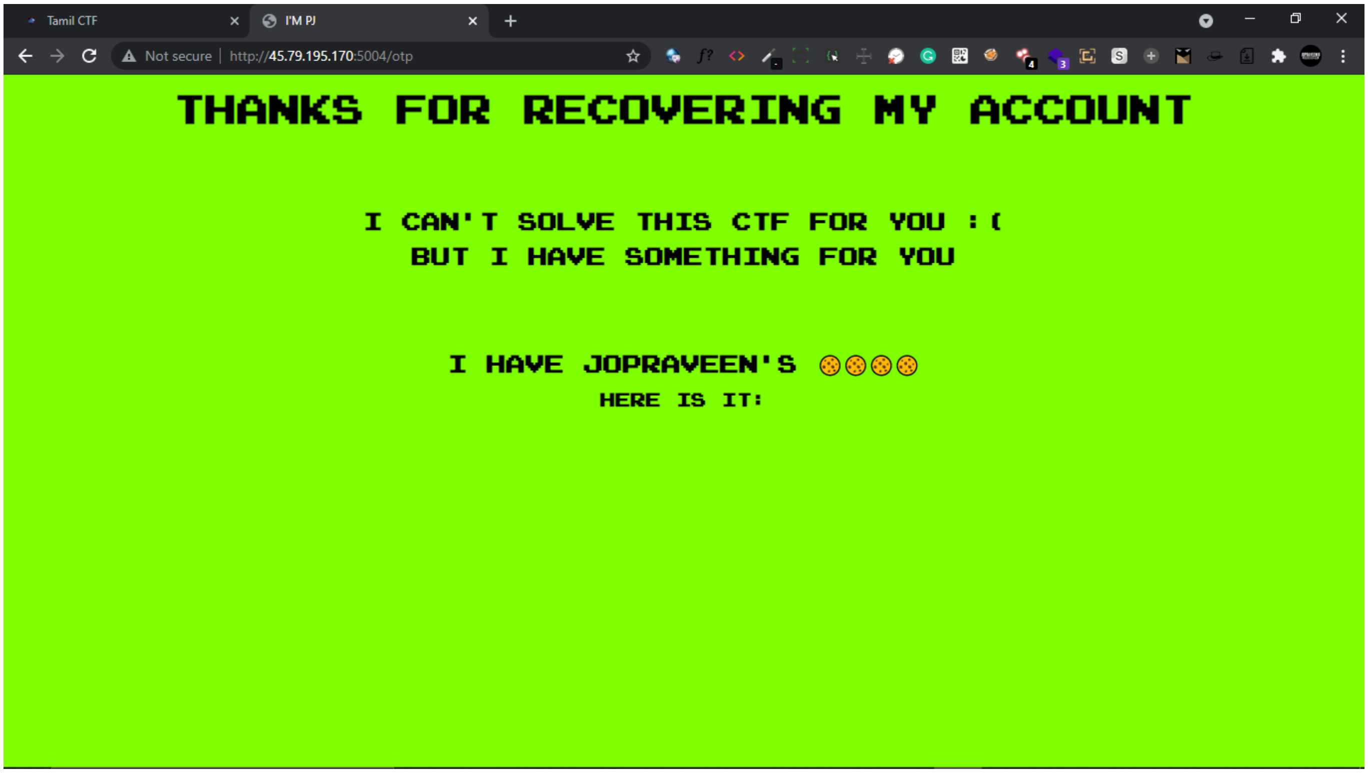
But where is the otp?



```
resetpass
api.js
data:font/ttf;base6...
recaptcha__en.js
anchor?ar=1&k=6LdVkwkUA..
anchor?ar=1&k=6LdVkwkUA..
anchor?ar=1&k=6LdVkwkUA..
anchor?ar=1&k=6LdVkwkUA..
anchor?ar=1&k=6LdVkwkUA..
```

```
Referrer Policy: strict-origin-when-cross-origin
▼ Response Headers    View source
  Content-Length: 6523
  Content-Type: text/html; charset=utf-8
  Date: Tue, 28 Sep 2021 15:26:29 GMT
  OneTimePassword: 6412
  Server: Werkzeug/2.0.1 Python/3.9.7
▼ Request Headers    View source
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
```

Here you can see the otp, it's in the headers
Now let's type this otp and press enter



THANKS FOR RECOVERING MY ACCOUNT

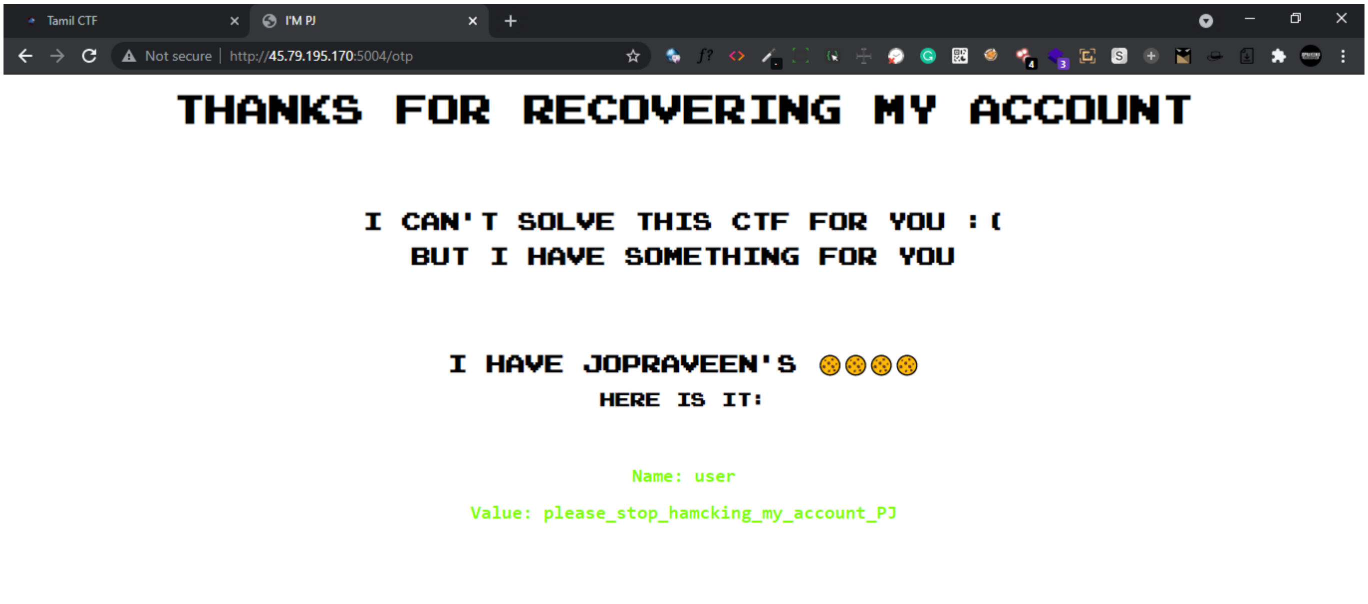
I CAN'T SOLVE THIS CTF FOR YOU :(
BUT I HAVE SOMETHING FOR YOU

I HAVE JOPRAVEEN'S 🍪🍪🍪🍪
HERE IS IT:

Great finally we got PJ's account, There's no flag but there's something PJ want's to give us

`I have jopraveen's 🍪🍪🍪🍪` ???

Let's change the background color of this website



THANKS FOR RECOVERING MY ACCOUNT

I CAN'T SOLVE THIS CTF FOR YOU :(
BUT I HAVE SOMETHING FOR YOU

I HAVE JOPRAVEEN'S 🍪🍪🍪🍪
HERE IS IT:

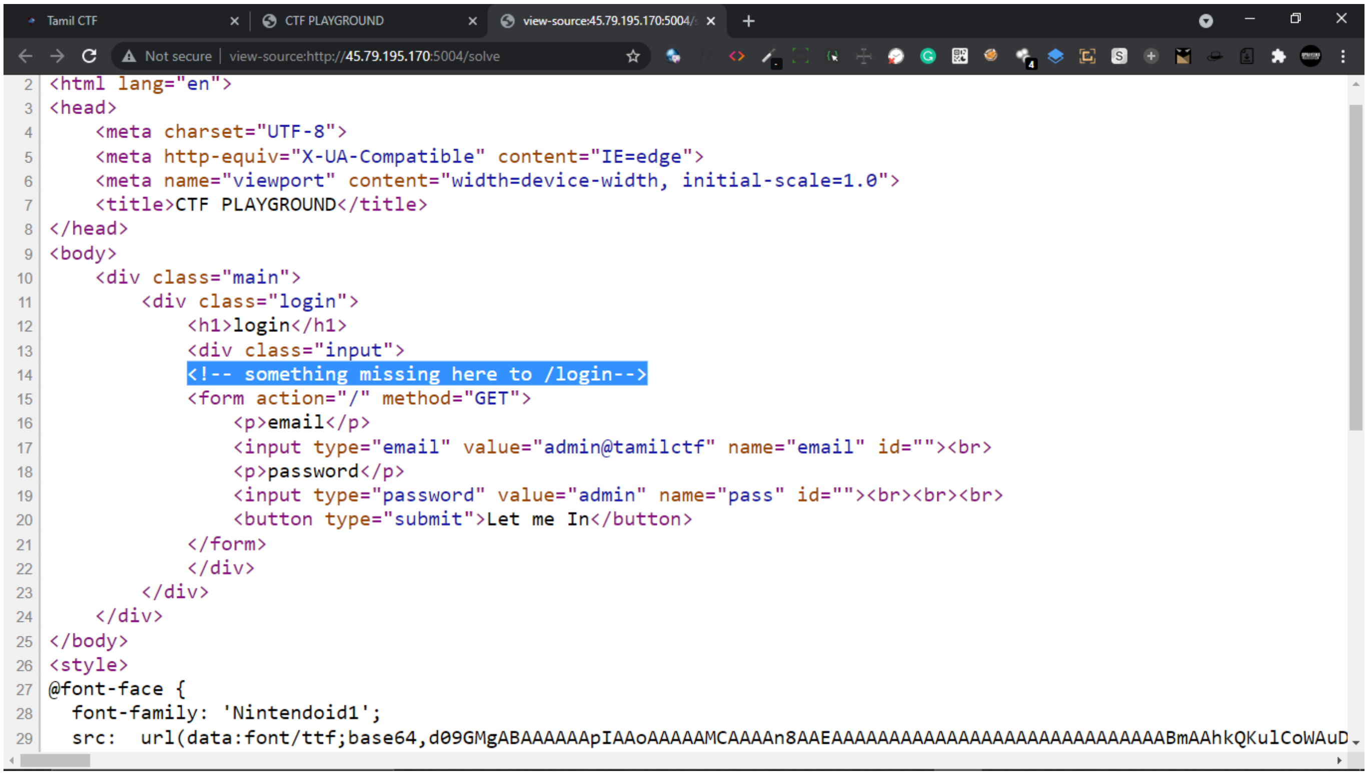
Name: user

Value: please_stop_hamcking_my_account_PJ

Cool we got the cookies

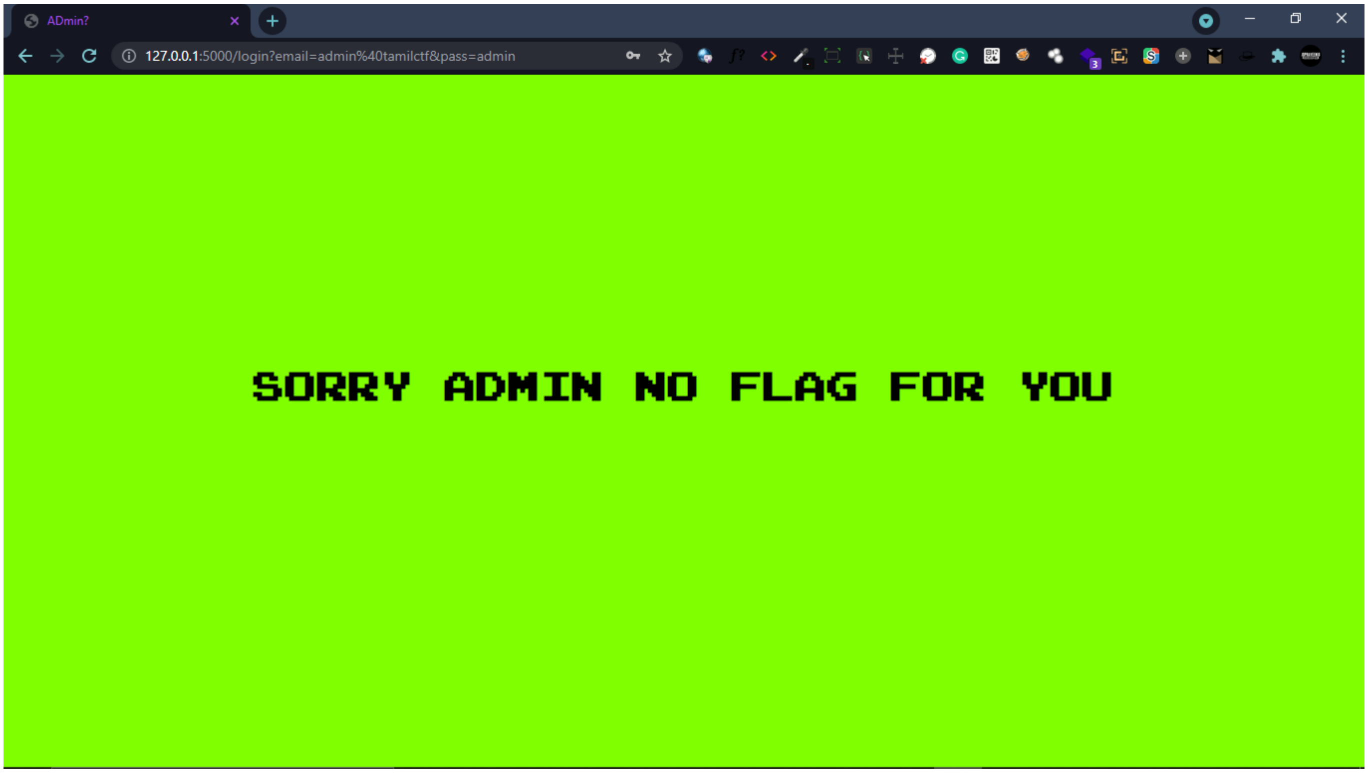
```
Name: user
Value: please_stop_hamcking_my_account_PJ
```

Now let's go to the starting page and click (solve this challenge)


Tamil CTF
CTF PLAYGROUND
view-source:45.79.195.170:5004/
Not secure
view-source:http://45.79.195.170:5004/solve

```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>CTF PLAYGROUND</title>
</head>
<body>
    <div class="main">
        <div class="login">
            <h1>login</h1>
            <div class="input">
            <!-- something missing here to /login-->
            <form action="/" method="GET">
                <p>email</p>
                <input type="email" value="admin@tamilctf" name="email" id=""><br>
                <p>password</p>
                <input type="password" value="admin" name="pass" id=""><br><br><br>
                <button type="submit">Let me In</button>
            </form>
            </div>
        </div>
    </div>
</body>
<style>
@font-face {
  font-family: 'Nintendoid1';
  src:  url(data:font/ttf;base64,d09GMgABAAAAAApIAAoAAAAAMCAAAAn8AAEAAAAAAAAAAAAAAAAAAAAAAAAAAAAABmAAhkQKulCoWAuD
```

By viewing the source code of it you can understand that the action is `/` so we need to change it to `/login` to login
Let's edit that with inspect element and login



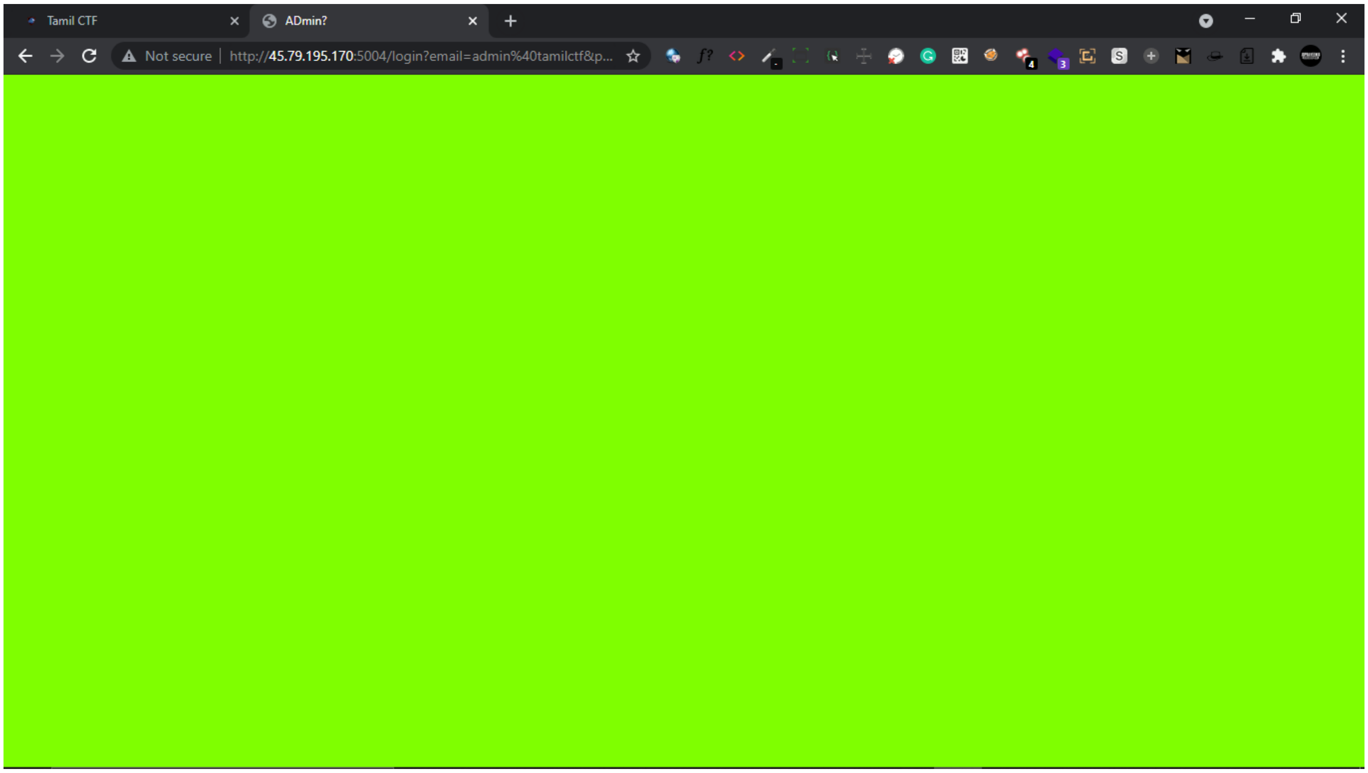
127.0.0.1:5000/login?email=admin%40tamilctf&pass=admin

SORRY ADMIN NO FLAG FOR YOU

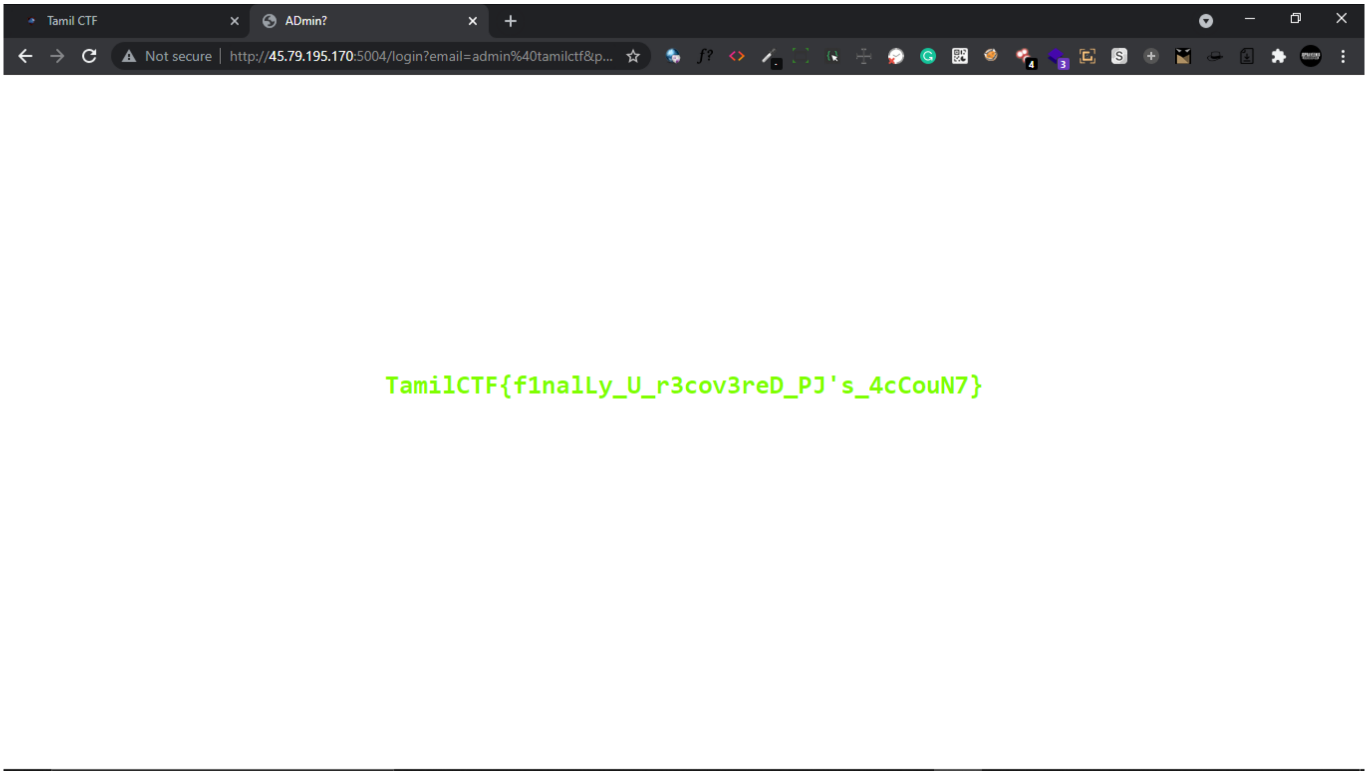
Sad there's no flag here, now let's try to use the cookies that we got from PJ

```
Name: user
Value: please_stop_hamcking_my_account_PJ
```

Add these things to the cookies



After adding the cookies still we can't see anything, let's try the old method, changing the background



TamilCTF{f1nalLy_U_r3cov3reD_PJ's_4cCouN7}

Cool we got the flag

`TamilCTF{f1nalLy_U_r3cov3reD_PJ's_4cCouN7}`