

Tan Ton

CS373 Final

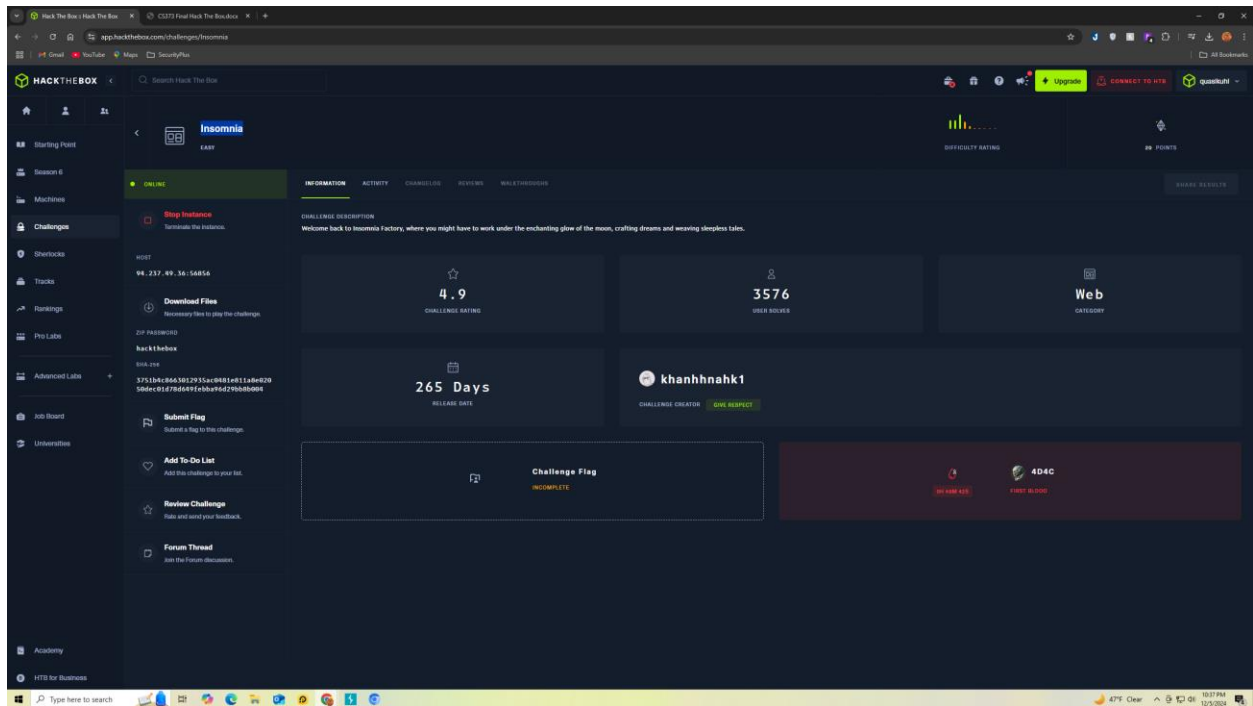
Challenge Points: 20 Pts

Challenge Name: Insomnia

Discussion Forum : <https://forum.hackthebox.com/t/official-insomnia-discussion/309741>

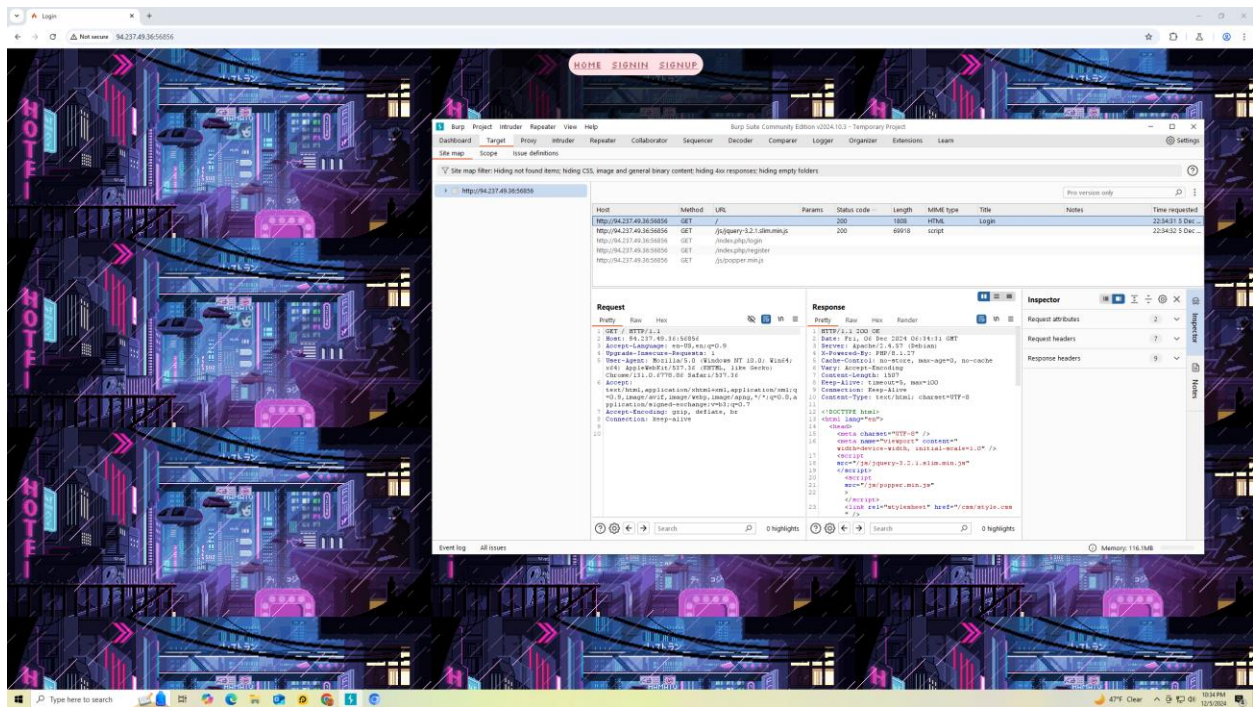
Tool Used: Chrome and Burp

First, I start the Instance from challenge page:



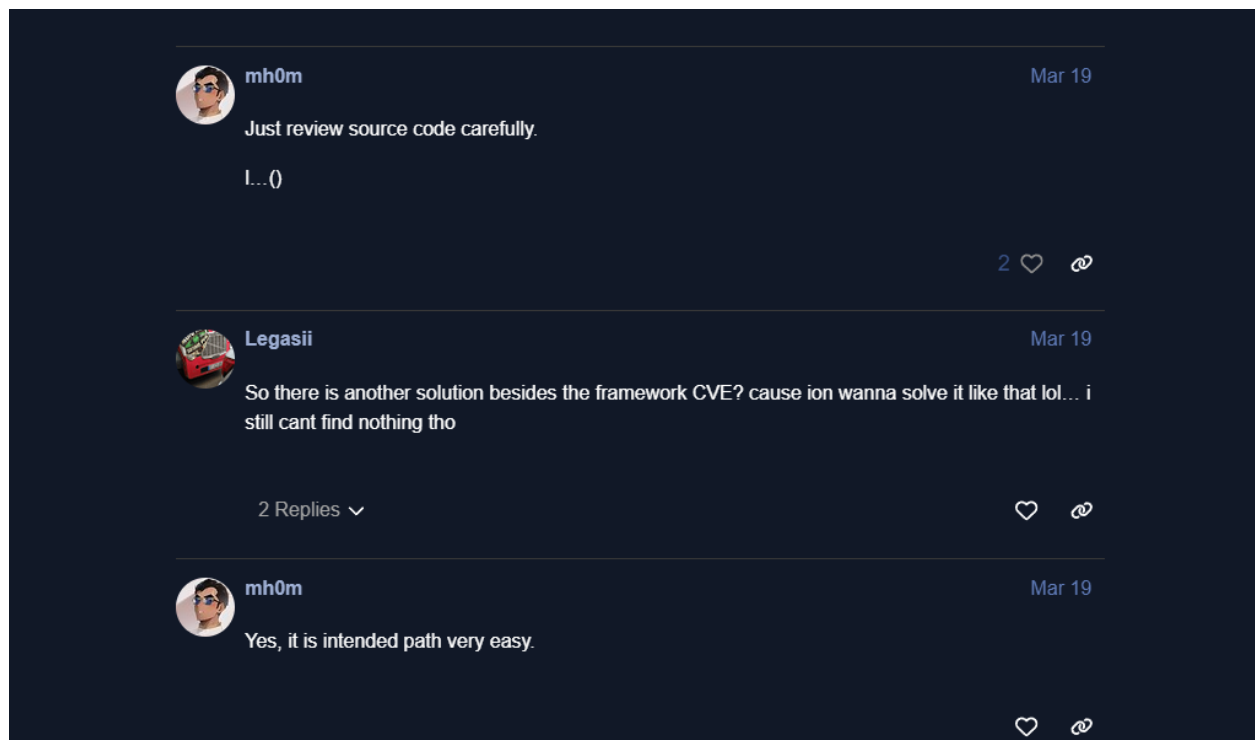
Copy the instance and paste it into my burp, I get the following:

Copy the instance and paste it into my burp, I get the following:

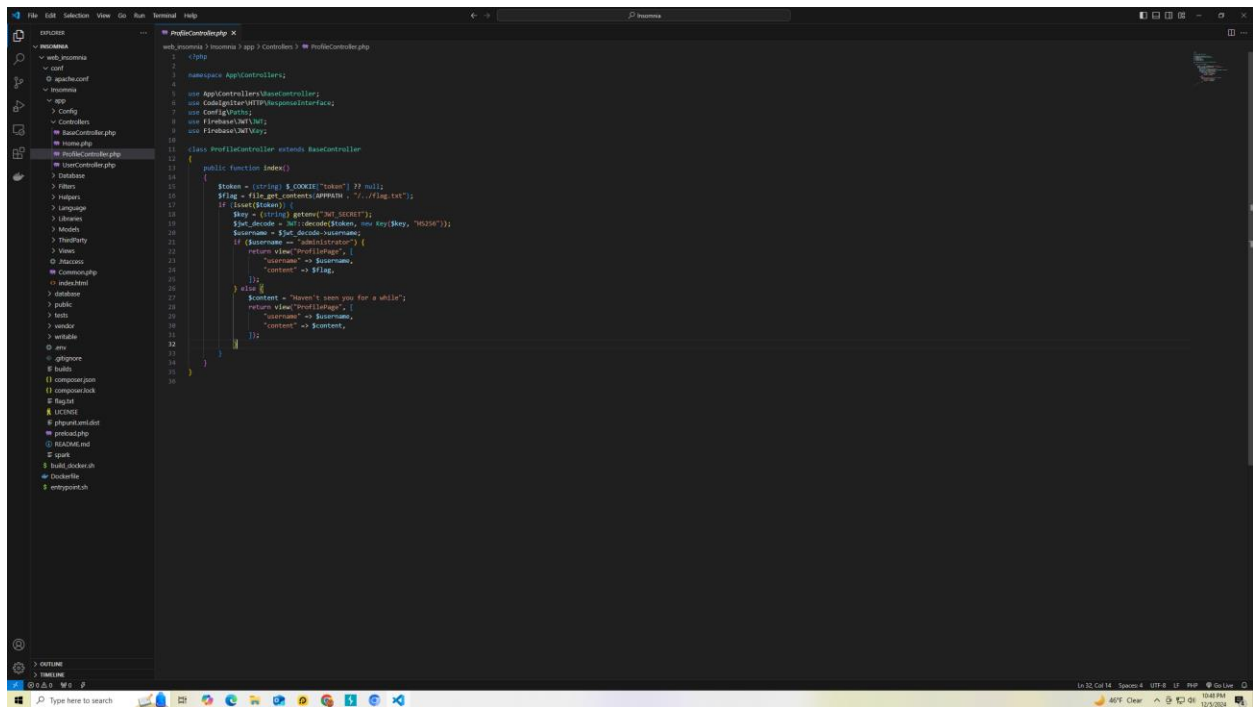


Messing around the site, I could not find anything related to the flag. I did signup and signin but nothing appear that related to. I then take a hint and look at the discussion forum with the link provided.

This helps me take a look at the source code, which is also provided on the site.



There was nothing much to look that related to the exploit, except for a the word Flag.



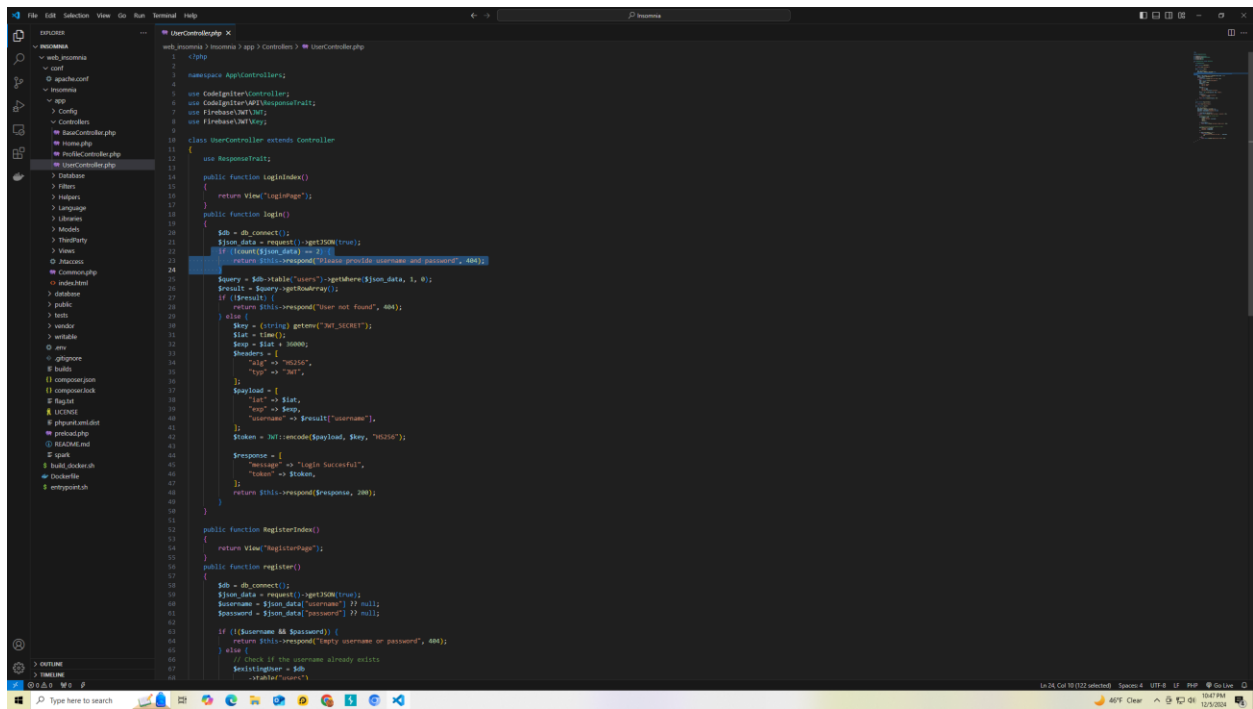
```
1 <?php
2
3 namespace App\Controllers;
4
5 use App\Controllers\BaseController;
6 use CodeIgniter\HTTP\RequestInterface;
7 use Config\Config;
8 use Firebase\JWT\JWT;
9 use Firebase\JWT\Key;
10
11 class HomeController extends BaseController
12 {
13     public function index()
14     {
15         $token = (string) $_COOKIE['token']; // null;
16         $flag = file_get_contents('flag.txt');
17         if (isset($token)) {
18             $key = (string) getenv('JWT_SECRET');
19             $jwt_decode = JWT::decode($token, new Key($key, 'HS256'));
20             $username = $jwt_decode->username;
21             if ($username == 'administrator') {
22                 return view('profilepage', [
23                     'username' => $username,
24                     'content' => $flag,
25                 ]);
26             }
27             $content = "You're not seen you for a while";
28             return view('profilepage', [
29                 'username' => $username,
30                 'content' => $content,
31             ]);
32         }
33     }
34 }
```

This mean i have to access the page with admin privilege to get the flag, and to do so, I have to get the token.

Preview the next code, I see some weird logic,

- `count($json_data)` gives the number of items in the `$json_data` array.
- The `!` (negation) in front of `count($json_data)` turns the result into its opposite. So if `count($json_data)` is 2, then `!2` becomes false because it's a non-zero number.
- The expression `!count($json_data) == 2` checks if false is equal to 2. Since false is not the same as 2, this condition will always be false.

So, the code is saying that this check will never pass if `$json_data` has 2 elements. The idea about "logging in as admin" may refer to a specific part of the code where this logic is used to control access, but this condition alone is always false.

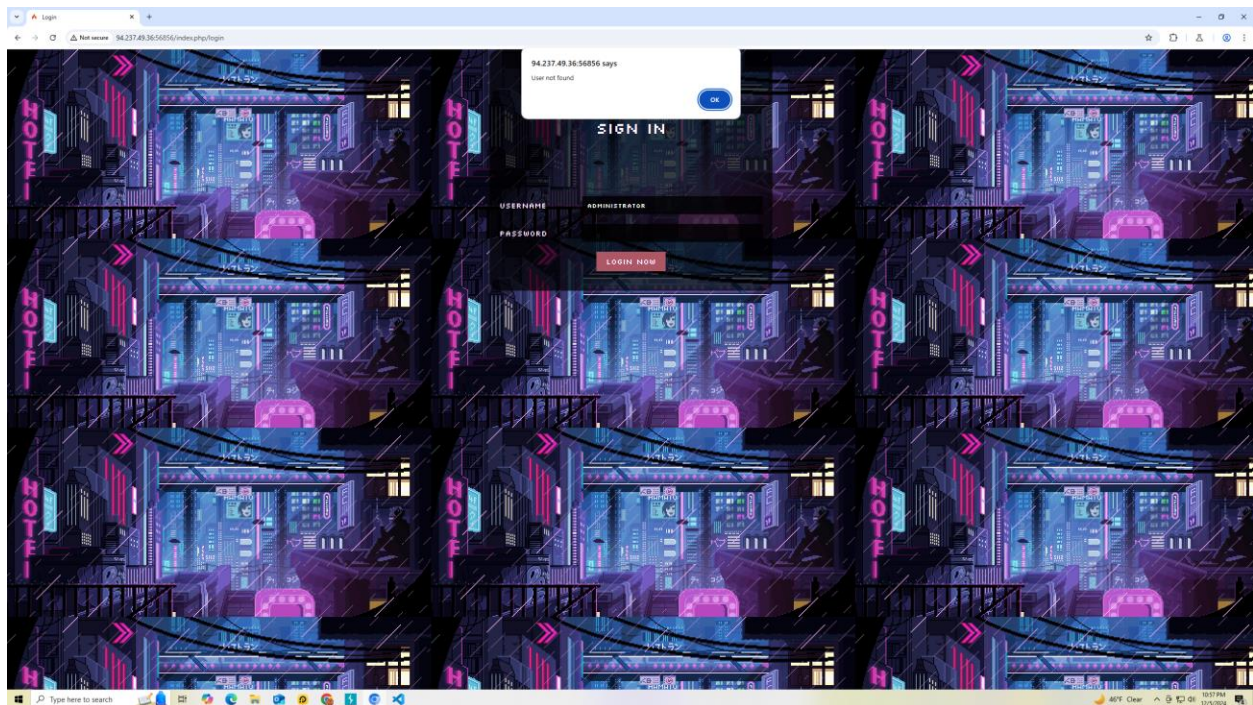


Coming back to the previous code,

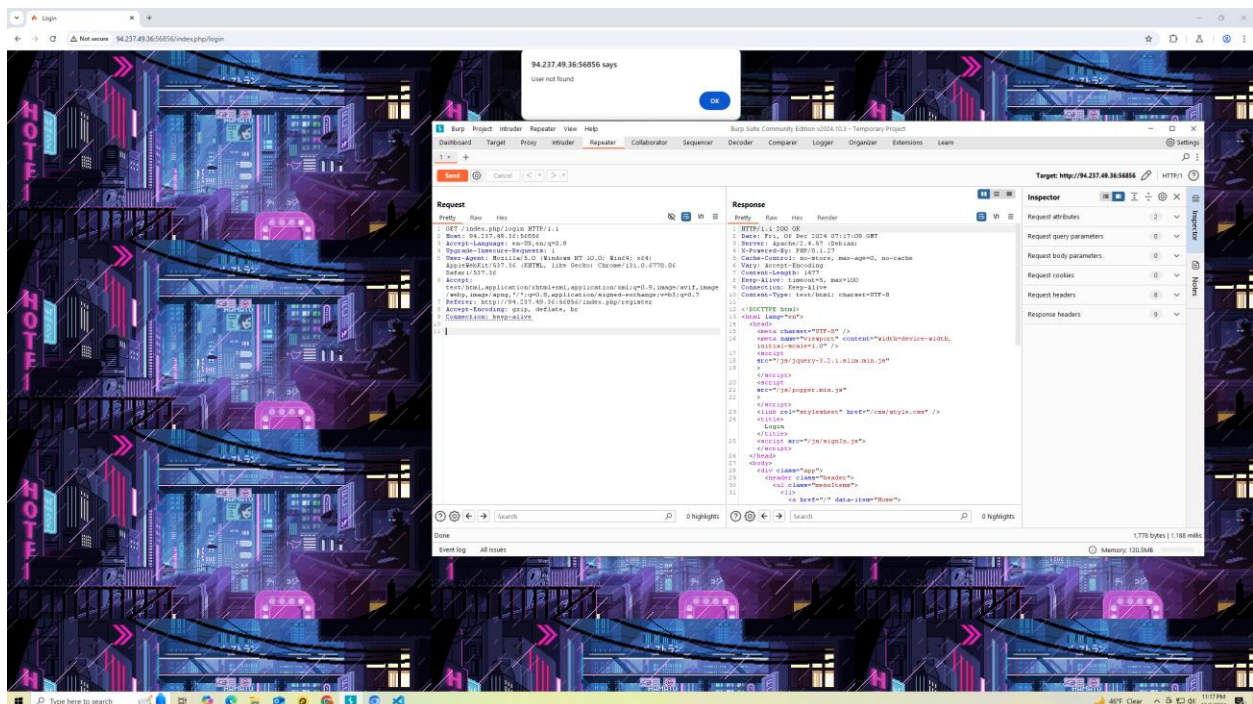
```
if ($username == "administrator") {
    return view("ProfilePage", [
        "username" => $username,
        "content" => $flag,
```

I tried to login through the website first, but then I realized, the admin login can be accessed through token.



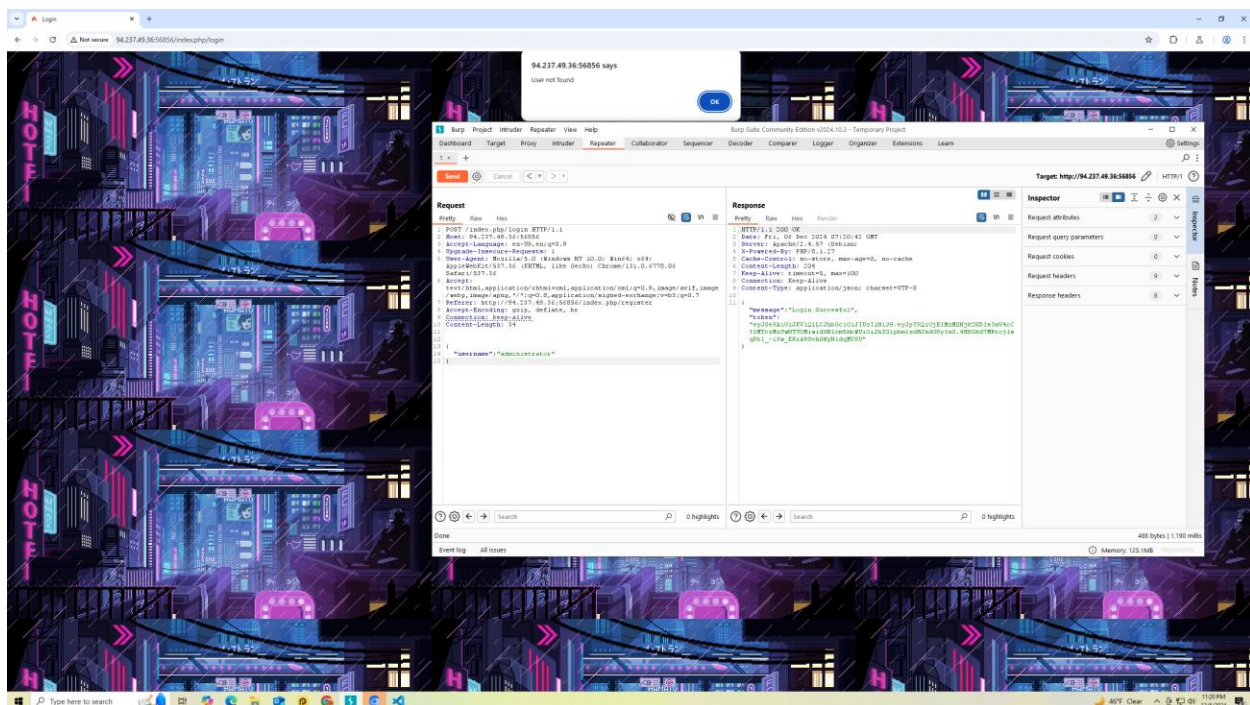


I then use Burp, send the login page to the repeater as follows:



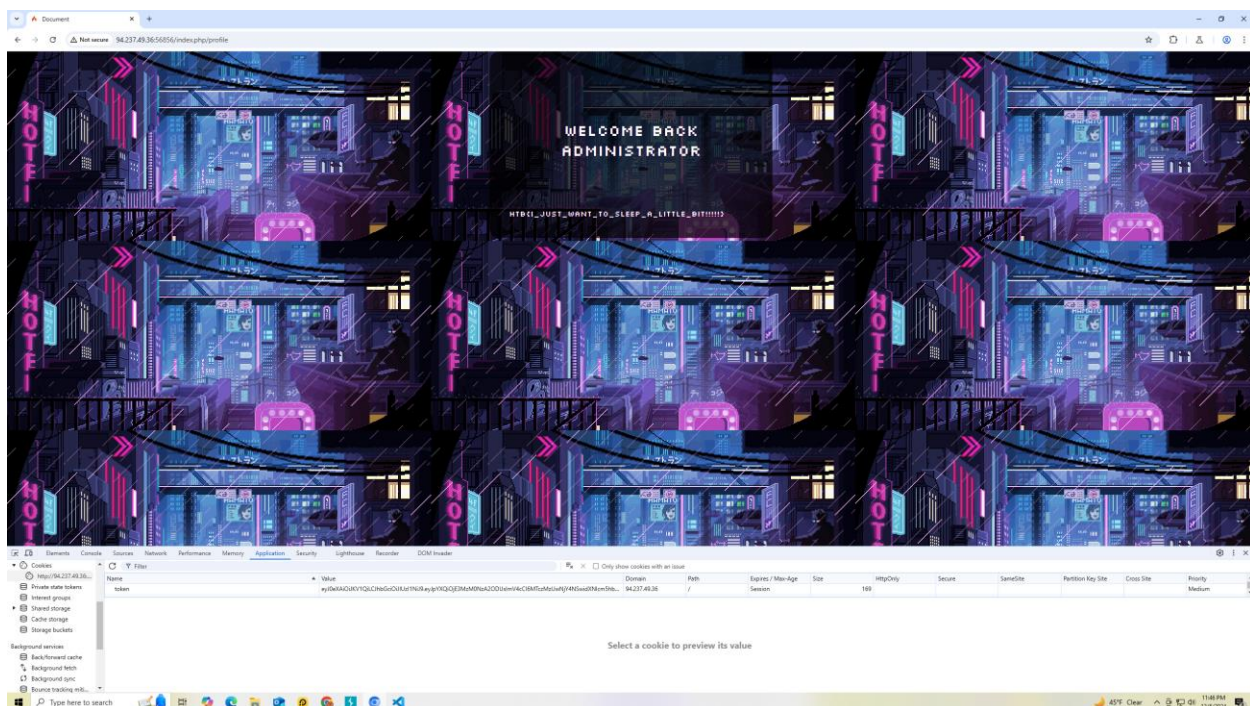
Since the request is GET (retrieving data), I will change to POST to update/add the username to the server and try to find the token. I added username as “administrator”



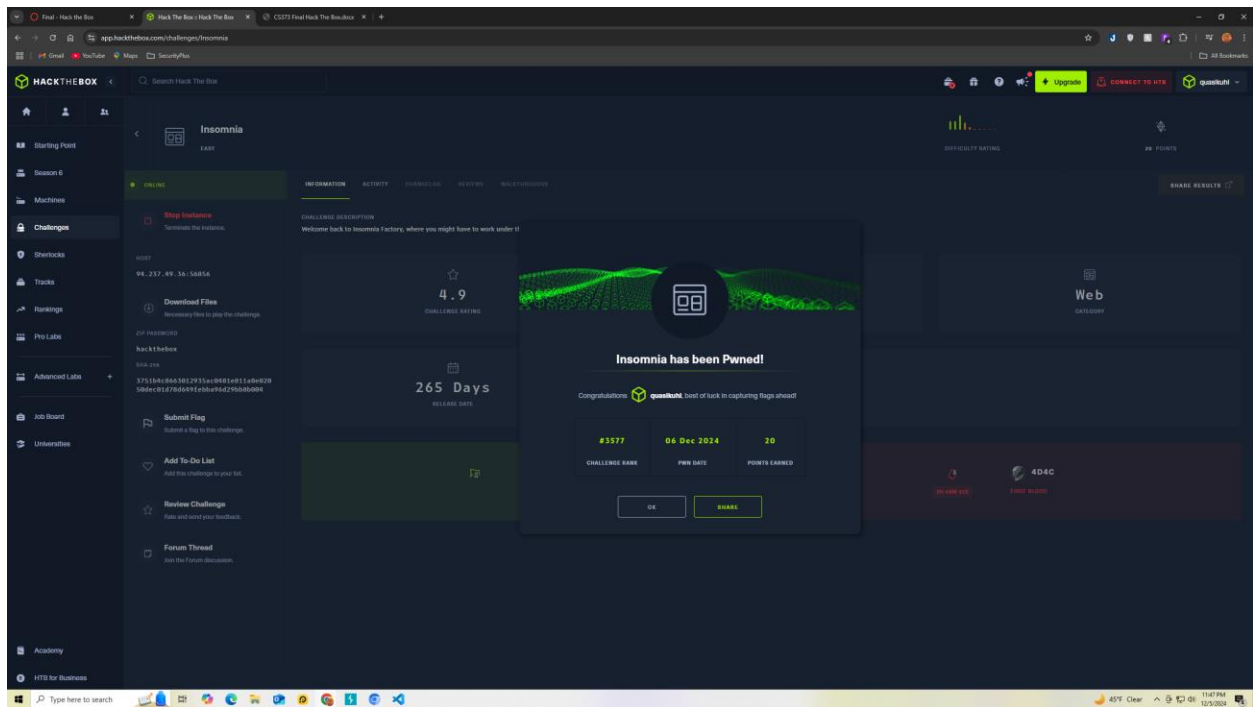


The login was successful, and the token appeared.

The last step I needed was input the token into the cookies and reload the site with /profile.



The flag finally appeared and submitted it to HackTheBox.



Overall, this challenge took me 2 days to finish, and I have to take a lot of research around the Discussion forum to get to the final answer. Really great class and I really love it.