h0t

A Happy pwner

OSCTF 2024 web writeup

Posted **Jul 13, 2024** • Updated **Jul 13, 2024**

By **Obaidah Salameh**

2 min read

Introspection

Web

Welcome to the Secret Agents Portal. Find the flag hidden in the secrets of the Universe!!!

Author: @5h1kh4r

```
Web Instance: http://34.16.207.52:5134
```

we are presented with a page with a box to check if the flag is right or not.

if we view the page source we will find a javascript file “script.js”.

```html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Web CTF Challenge</title>
    <link rel="stylesheet" href="styles.css">
</head>
<body>
    <div class="container">
        <h1>Welcome to the Secret Agents portal</h1>
        <p>Find the hidden flag in the secrets of the Universe</p>
        <input type="text" id="flagInput" placeholder="Enter flag here">
        <button onclick="checkFlag()">Submit</button>
        <p id="result"></p>
    </div>
    <script src="script.js"></script>
</body>
</html>

```

we open it and we get the flag!!!!

h0t

A Happy pwner


```
function checkFlag() {
    const flagInput = document.getElementById('flagInput').value;
    const result = document.getElementById('result');
    const flag = "OSCTF{Cr4zY_In5P3c71On}";

    if (flagInput === flag) {
        result.textContent = "Congratulations! You found the flag!";
        result.style.color = "green";
    } else {
        result.textContent = "Incorrect flag. Try again.";
        result.style.color = "red";
    }
}
```

Flag: `OSCTF{Cr4zY_In5P3c71On}`

Style Query Listing...?

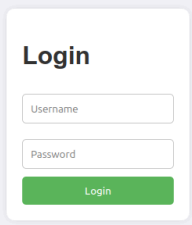
Web

pfft.. Listen, I've gained access to this login portal but I'm not able to log in. The admins are surely hiding something from the public, but… I don't understand what. Here take the link and be quiet, don't share it with anyone

Author: @5h1kh4r

```
Web instance: http://34.16.207.52:3635/
```

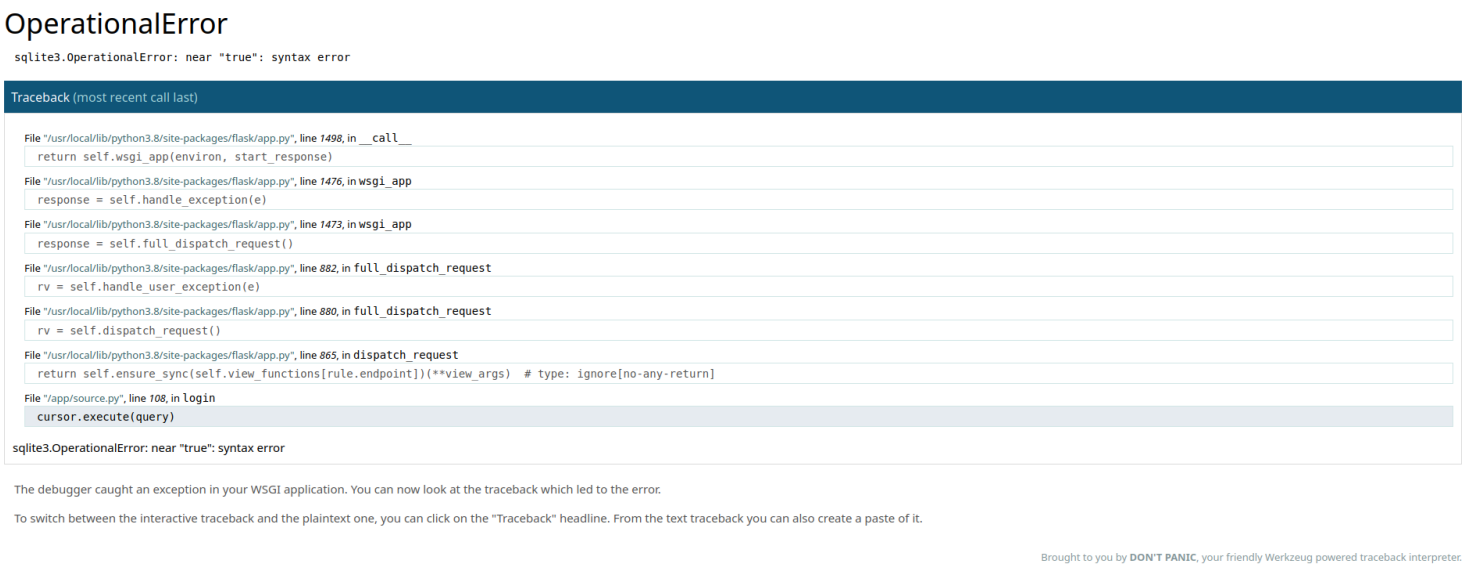
we are presented with a login page, if you try to login with default credentials nothing will work, so as the name suggests its SQL injection.



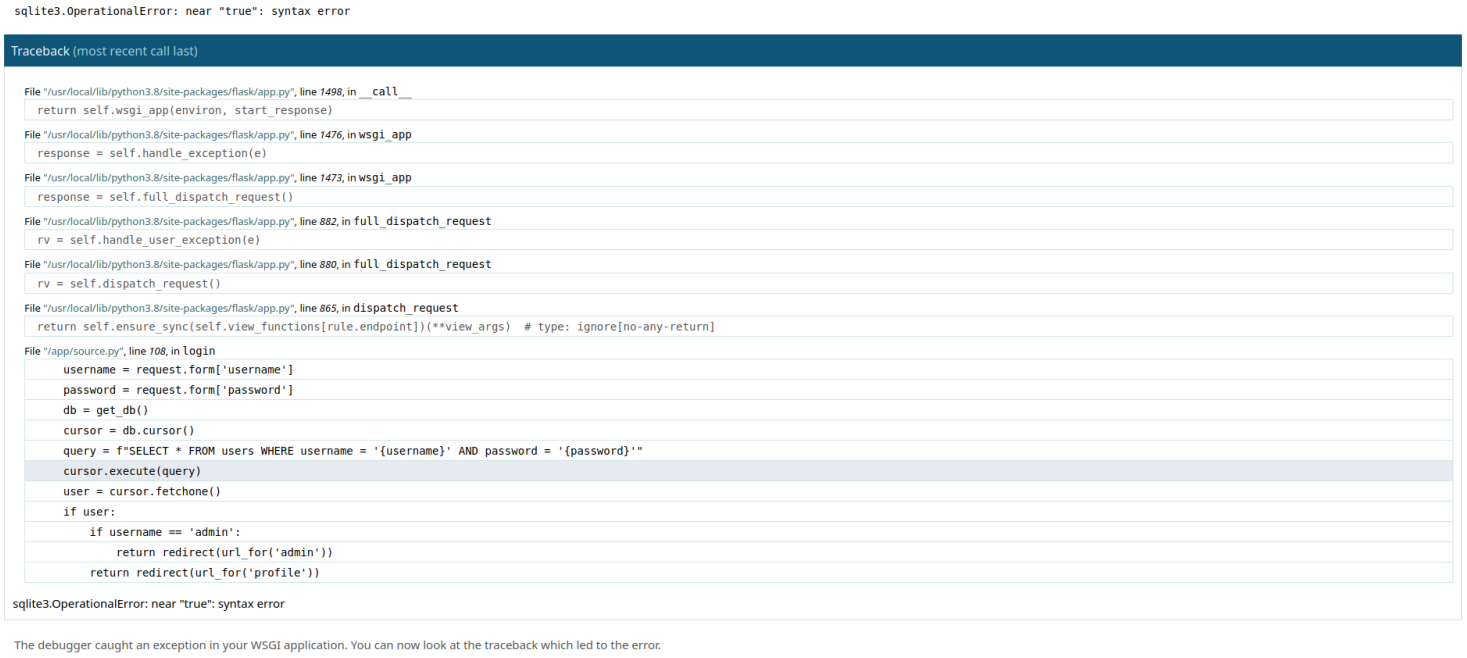
h0t

A Happy pwner

the first payload i tried is `admin' or true-- -`



and we get an exception from the Werkzug server, the good thing about these messages is that it shows 5 lines above and bottom of the line that got the error.

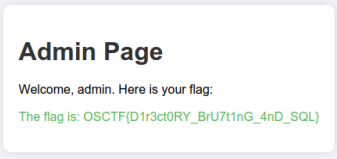


Python

```python
if username == 'admin':
        return redirect(url_for('admin'))
```

so if the user is admin in the input it will redirect the user to the admin page, which is /admin.

if we go to `http://34.16.207.52:3635/admin` we will find the flag!!!



Flag: `OSCTF{D1r3ct0RY_BrU7t1nG_4nD_SQL}`

Indoor WebApp

Web

The production of this application has been completely indoor so that no corona virus spreads, but that's an old talk right?

Author: @5h1kh4r

```
Web Instance: http://34.16.207.52:2546
```

We see the Vulnerability name in the main page, with a button to view a profile.

the button will take us to `http://34.16.207.52:2546/profile?user_id=1` we see a username and an email. but in the link the query parameter `?user_id=1` indicates that we can change the number to view other profiles, for sanity check i like to try 2.

and we got the flag!!!

Flag: `OSCTF{1nd00r_M4dE_n0_5enS3}`

Action Notes

Web

I have created this notes taking app so that I don't forget what I've studied

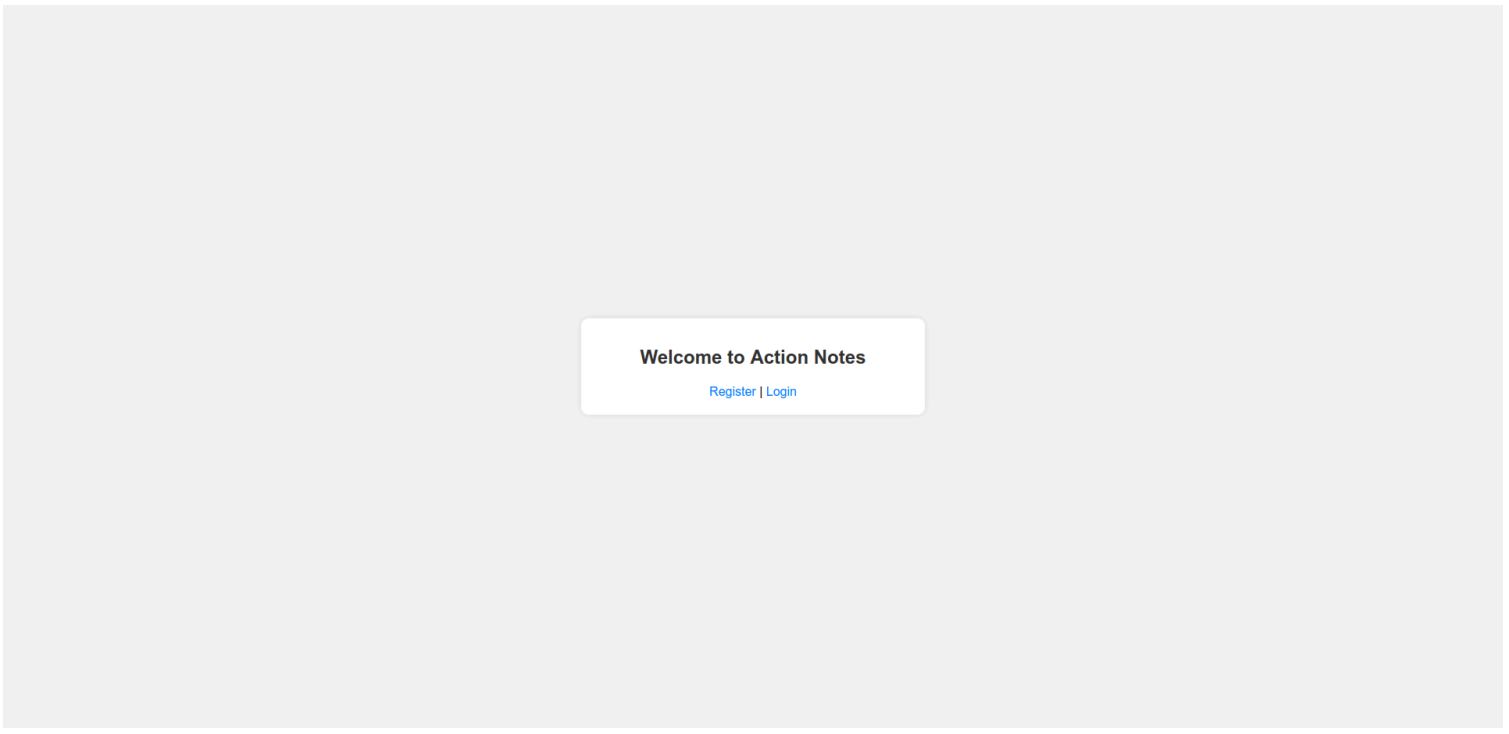
Author: @5h1kh4r

```
Web Instance: http://34.16.207.52:8965
```

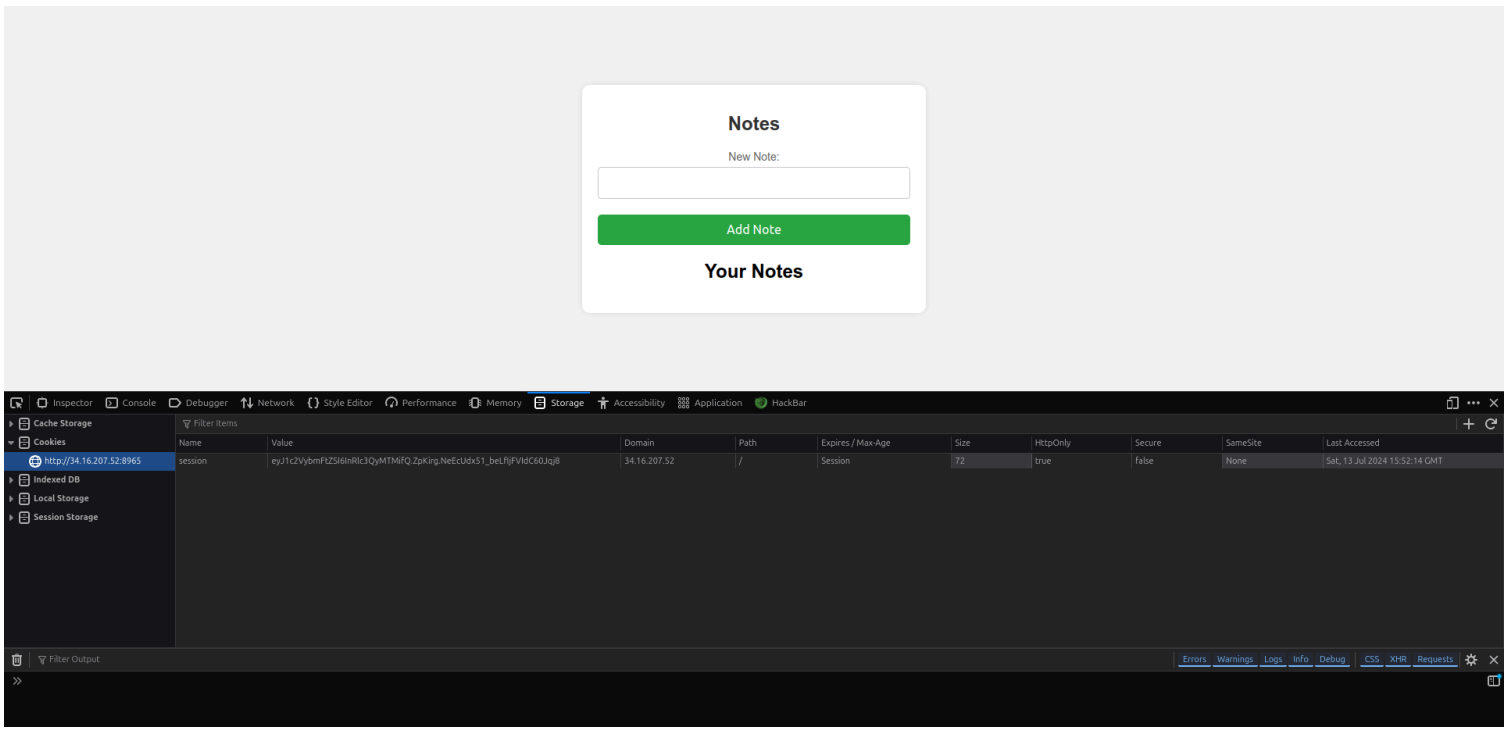
h0t

A Happy pwner

In the main page we can either login or register, so i register an account and login with it.



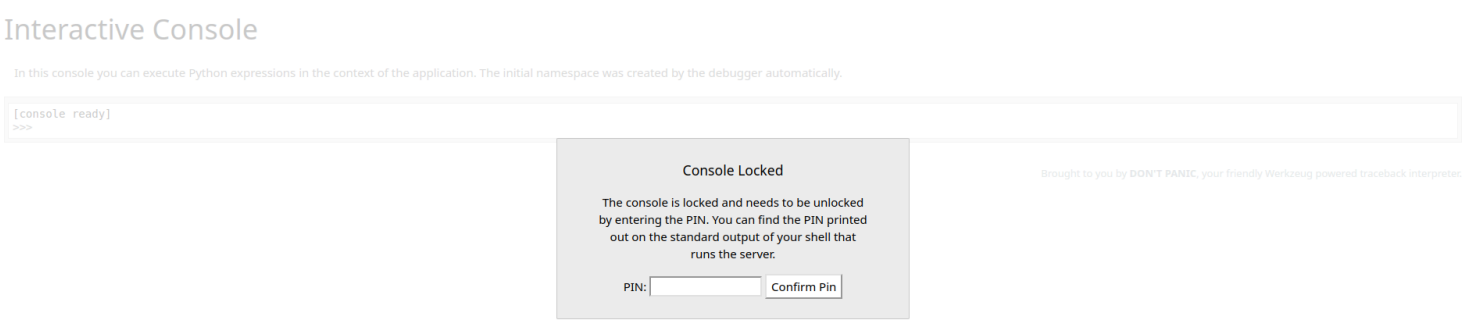
We can add notes to our profile, but i first looked to the cookies.



`session:eyJ1c2VybmFtZSI6InRlc3QyMTMifQ.ZpKirg.NeEcUdx51_beLfIjFVIdC60Jqj8`

the session cookie looks like a JWT but if you try to decode it with jwt.io you will get an error.

but we know this is a flask server because if you go to /console you will get:

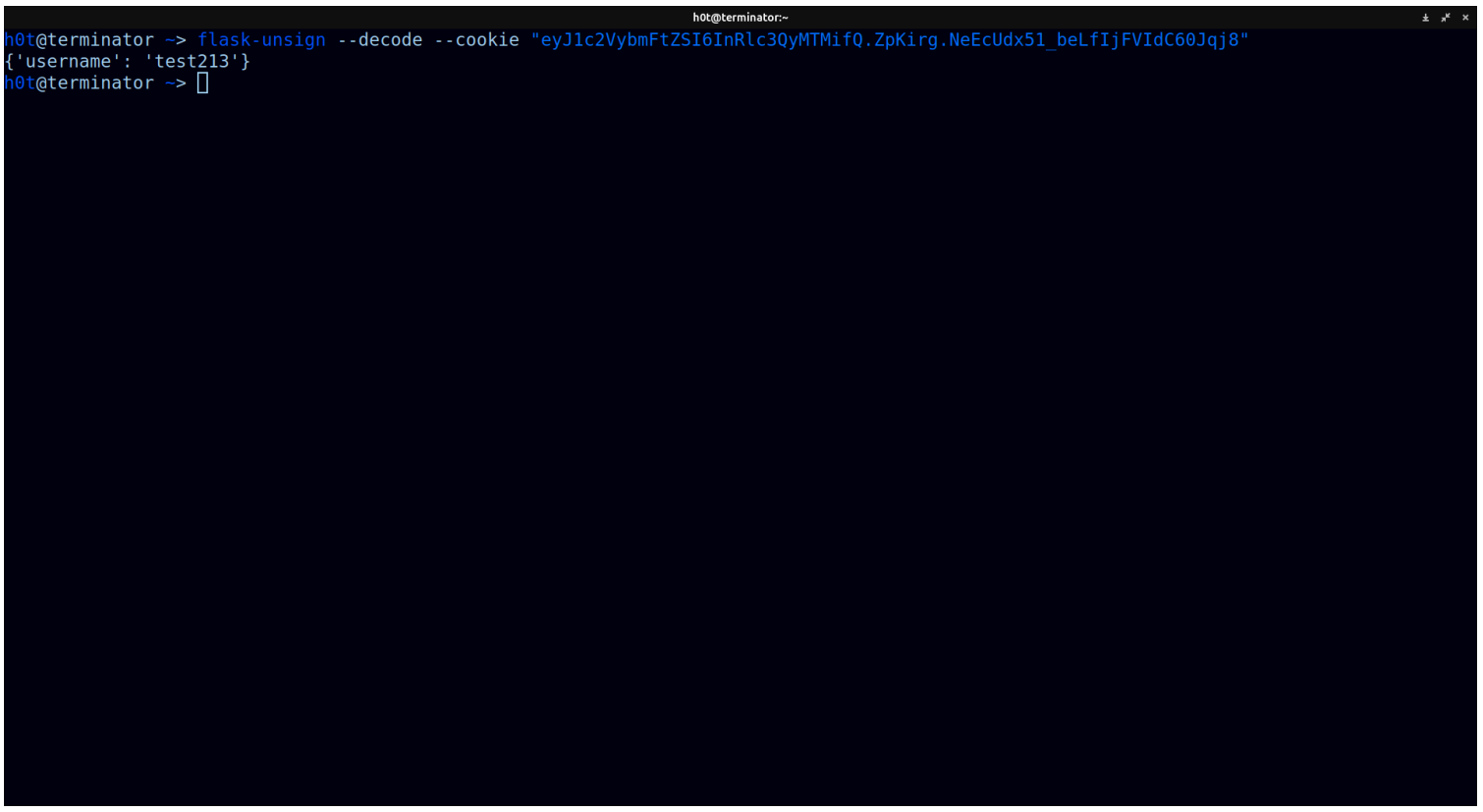


in HackTricks we can see there is a tool called `flask-unsign` , if we put the cookie in it and try to decode it we will get:

```shell
flask-unsign --decode --cookie "eyJ1c2VybmFtZSI6InRlc3QyMTMifQ.ZpKirg.NeEcUdx51_beLfIjFVIdC60
```

h0t

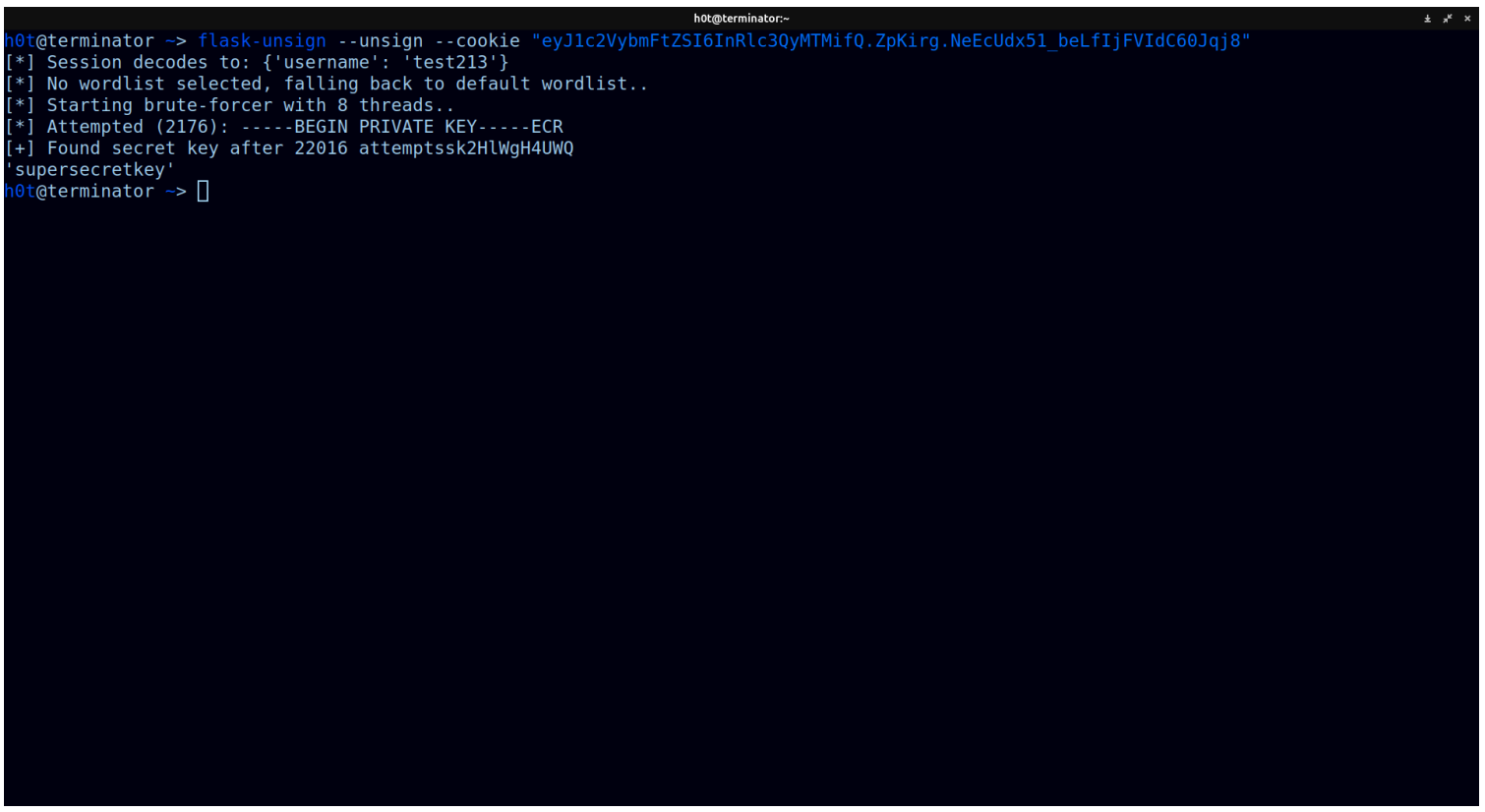
A Happy pwner



using the tool we can try to crack the secret code using the same tool with this command:

```shell
flask-unsign --unsign --cookie "eyJ1c2VybmFtZSI6InRlc3QyMTMifQ.ZpKirg.NeEcUdx51_beLfIjFVIdC60
```

and we got the secret key!!!



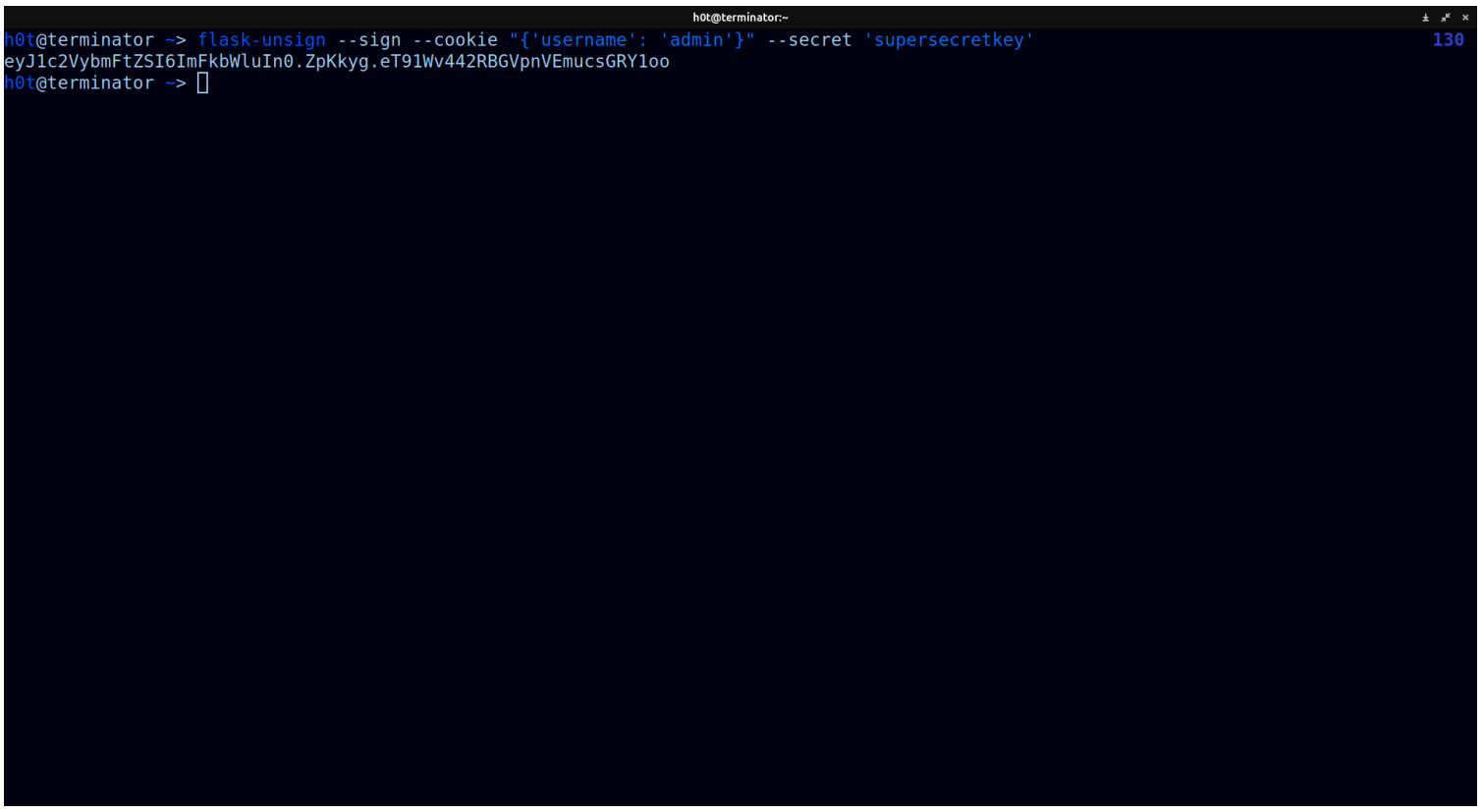
Secret Key: `supersecretkey`

so know we can sign our own cookies and change the username to admin.

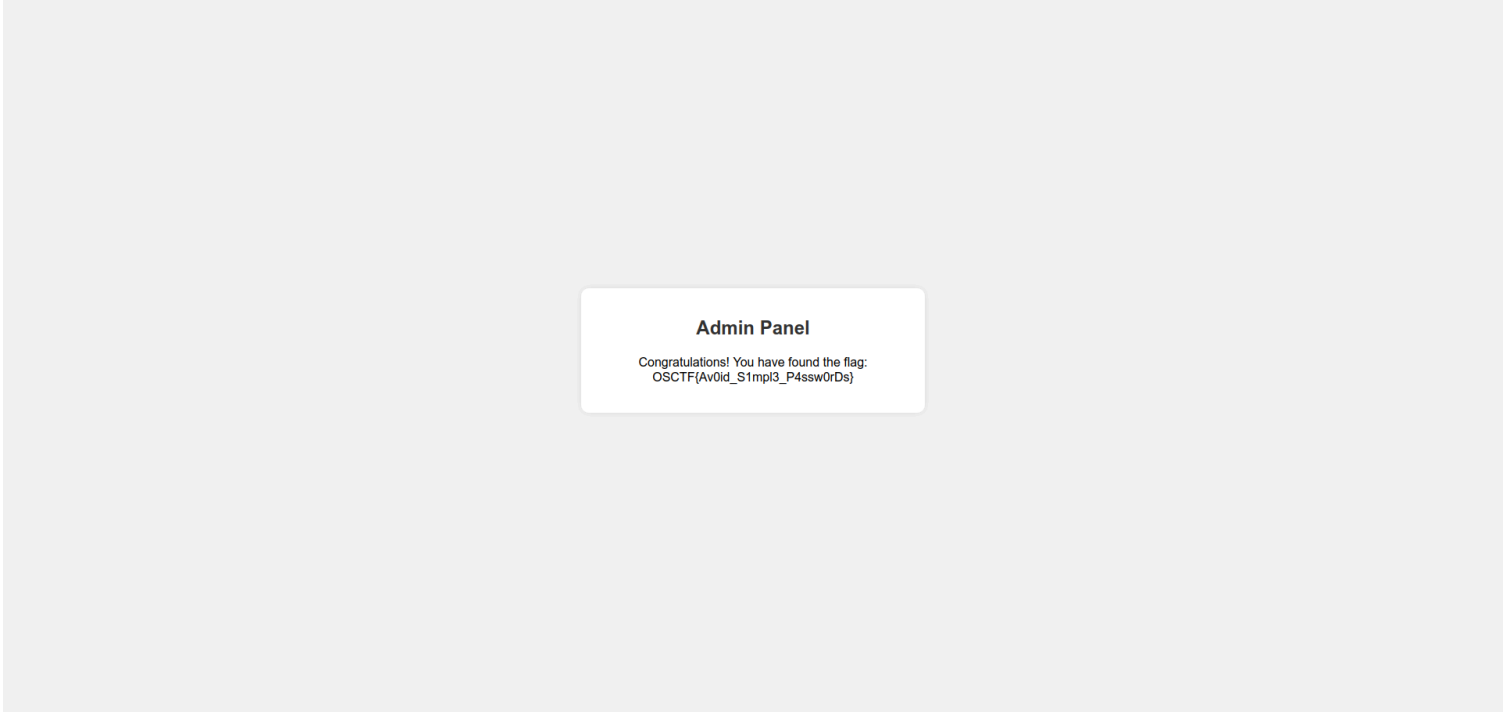
```shell
flask-unsign --sign --cookie "{'username': 'admin'}" --secret 'supersecretkey'
```

h0t

A Happy pwner



and we got our new cookie, if we change it with the new one in our browser, we will see some players trolling, but if we go to /admin we will find the flag.



We got the flag!!!

Flag: `OSCTF{Av0id_S1mpl3_P4ssw0rDs}`

writeups

ctf web flask

Share:

Further Reading

Mar 23, 2024

TuxCTF 2024

TuxCTF 2024 web Writeups Hello, This is the Intended solutions for TuxCTF 2024 web Challenges Level1 San…

Feb 28, 2024

TryHackMe Chocolate Factory WriteUp

TryHackMe Chocolate Factory WriteUp Hello and Welcome to my first writeup! Reconnaissance and…

Mar 1, 2024

TryHackMe Blog WriteUp

Tryhackme Blog Writeup Hello Again :) Reconnaissance and Enumeration as usual, we start with scanning the…

h0t

A Happy pwner

HOME

CATEGORIES

TAGS

ARCHIVES

ABOUT

OLDER

TuxCTF 2024

NEWER

-