The Hunt

This is some of the web challenges for hackers teaching hackers CTF 2022. The theme was from the movie “The Goonies”

Nmap reveals port 7504 open

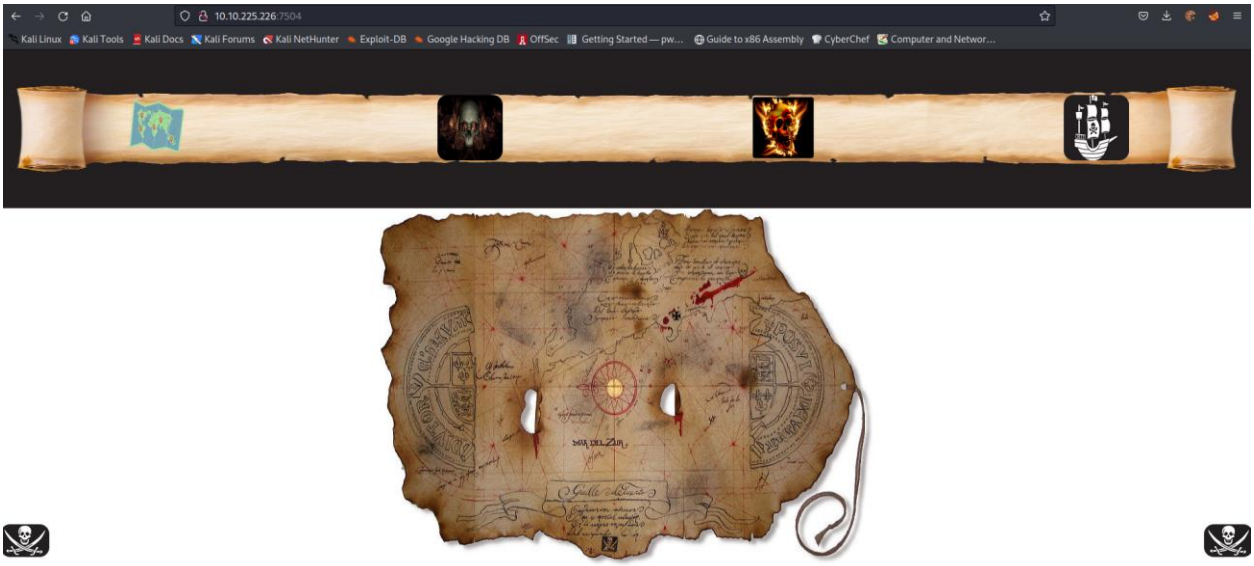
```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.225.226
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-20 17:53 EST
Nmap scan report for 10.10.225.226
Host is up (0.12s latency).
All 1000 scanned ports on 10.10.225.226 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 12.67 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.225.226 -p- --min-rate 3000
Starting Nmap 7.93 ( https://nmap.org ) at 2022-1
1-20 17:58 EST
Nmap scan report for 10.10.225.226
Host is up (0.12s latency).
Not shown: 65534 closed tcp ports (conn-refused)
PORT     STATE SERVICE
7504/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 27
.93 seconds
```

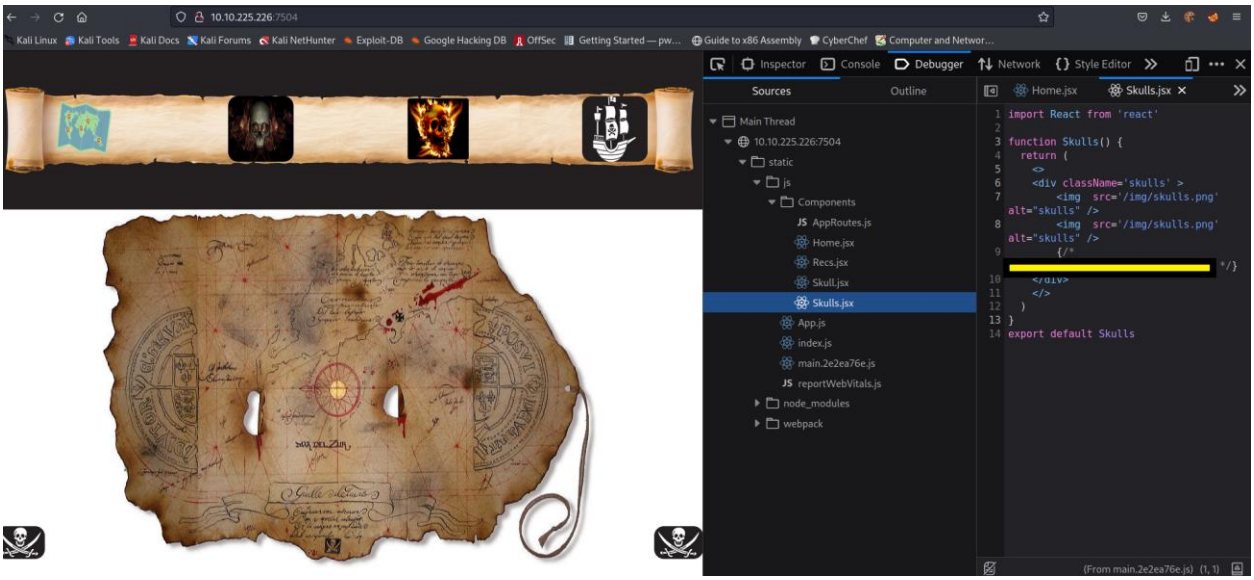
dirsearch quickly gives us some end points,

```
┌──(kali㉿kali)-[~]
└─$ dirsearch -f -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://10.10.225.226:7504

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 220545

Output File: /home/kali/.dirsearch/reports/10.10.225.226-7504/_22-11-20_18-05-52.txt

Error Log: /home/kali/.dirsearch/logs/errors-22-11-20_18-05-52.log

Target: http://10.10.225.226:7504/

[18:05:52] Starting:
[18:05:53] 200 -    1KB - /1
[18:05:53] 301 -  173B  - /img  →  /img/     (Added to queue)
[18:05:53] 200 -    1KB - /login
[18:05:54] 200 -  637B  - /0
[18:05:54] 302 -   32B  - /directory  →  /something
[18:05:54] 200 -  952B  - /welcome
[18:05:54] 301 -  179B  - /static  →  /static/     (Added to queue)
[18:05:57] 200 -    1KB - /Login
[18:05:59] 302 -   28B  - /logout  →  /login
[18:06:02] 200 -  952B  - /Welcome
CTRL+C detected: Pausing threads, please wait...
[q]uit / [c]ontinue / [n]ext:
```

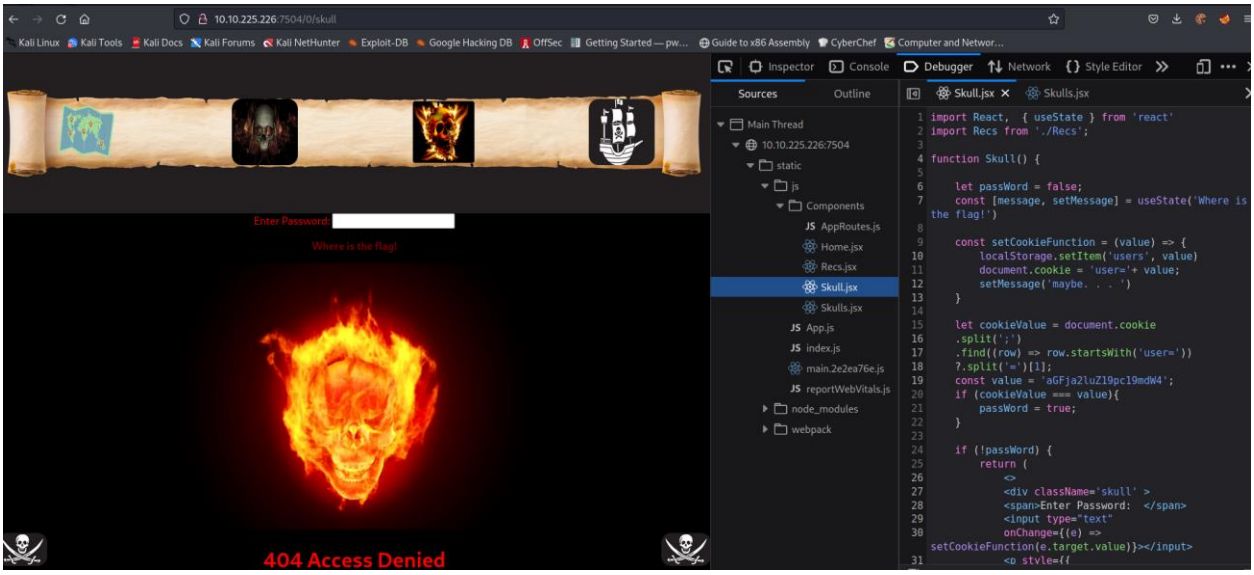
We navigate to port 7504 on browser to find code that looks like a react app.



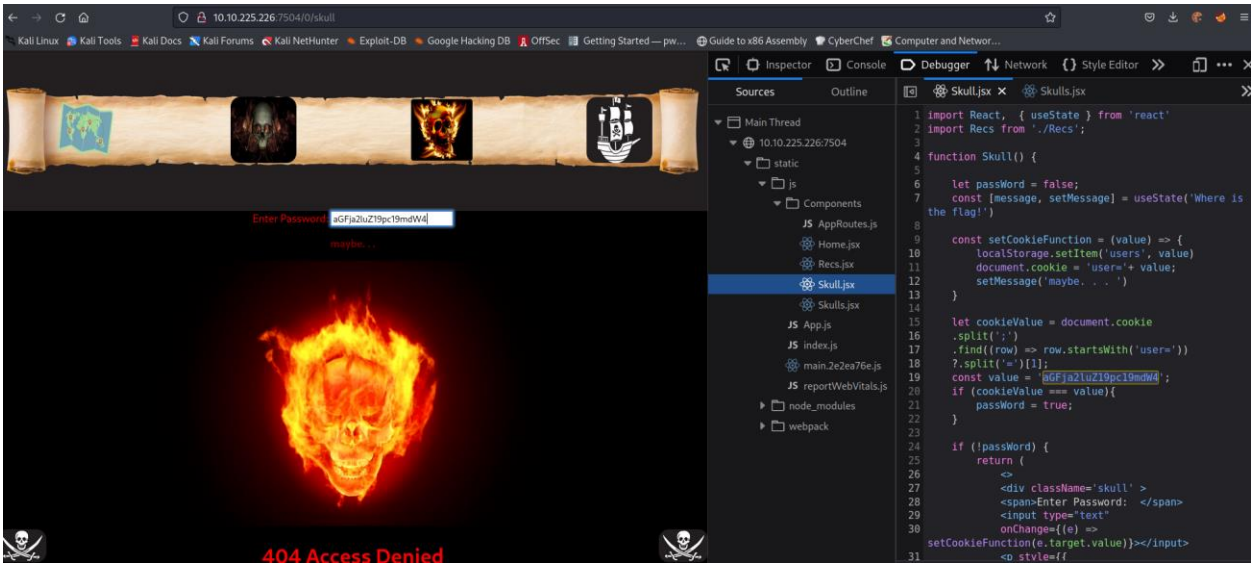
After looking around at the code, we find the first flag



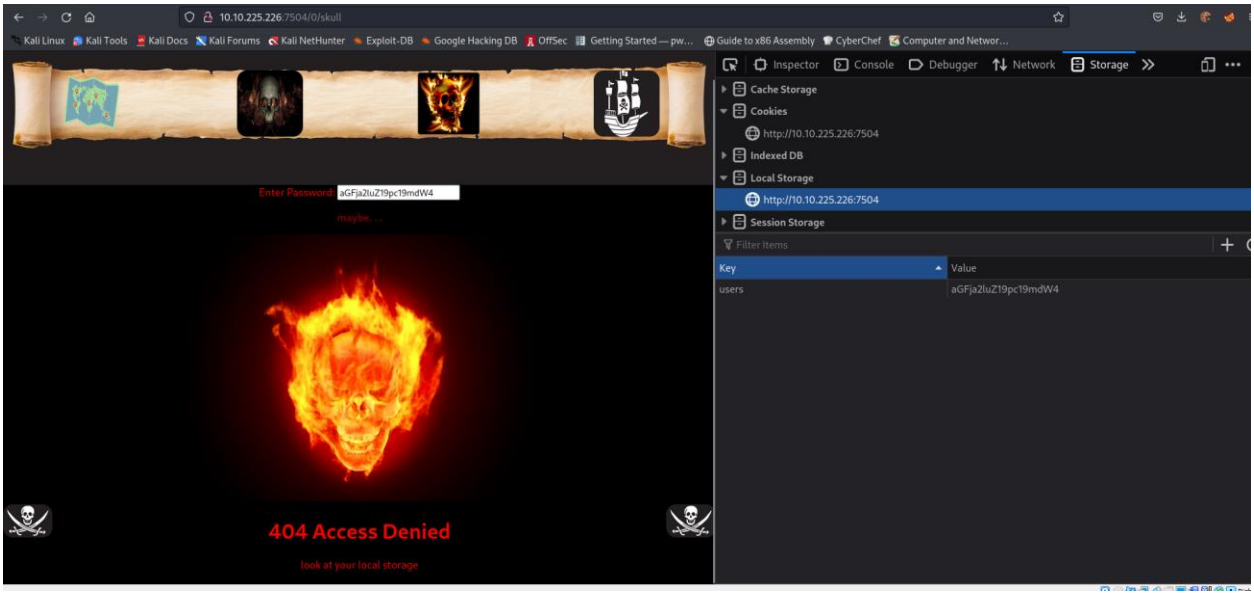
Let go to the second image in the navbar



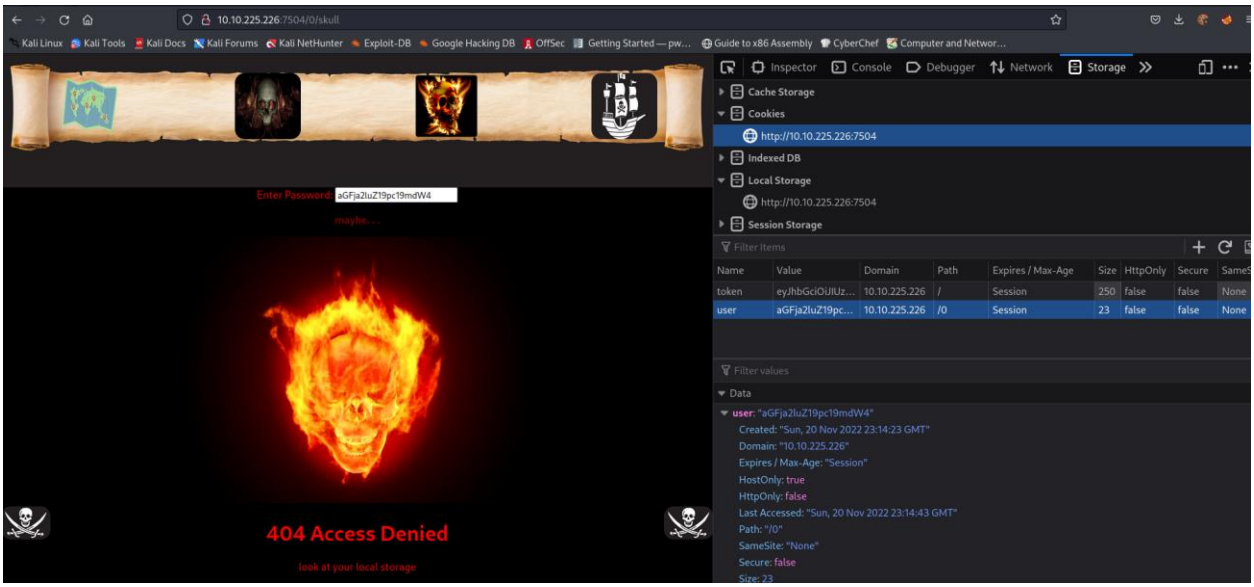
The code says if I put that value, then it will set the cookie,



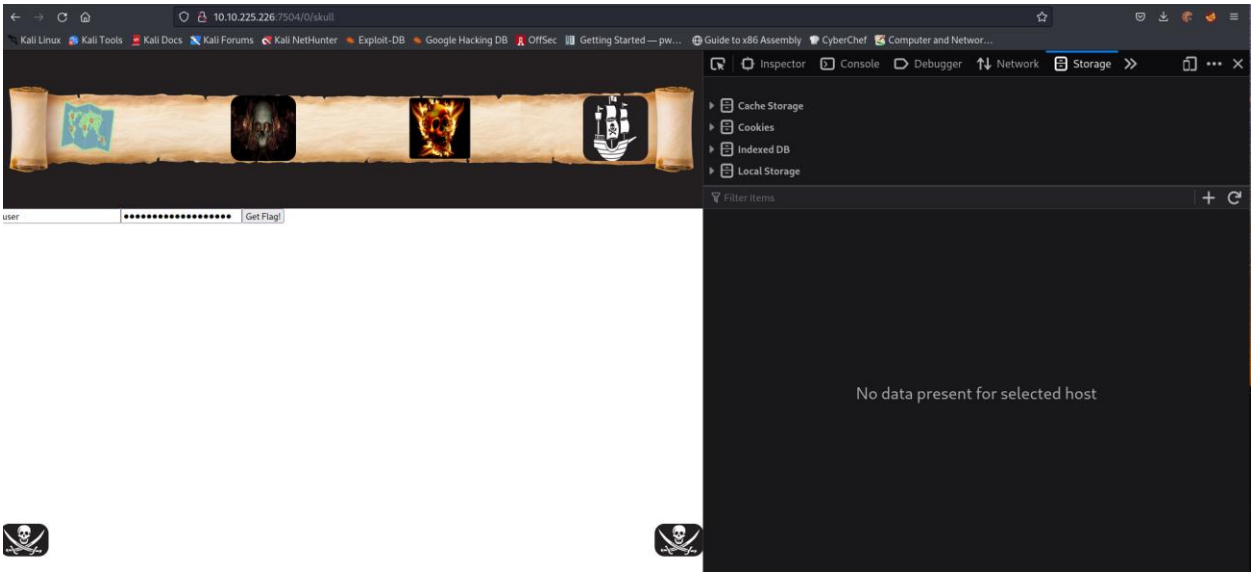
Nothing happens, it says to look at local storage, lets see what's going on over there,



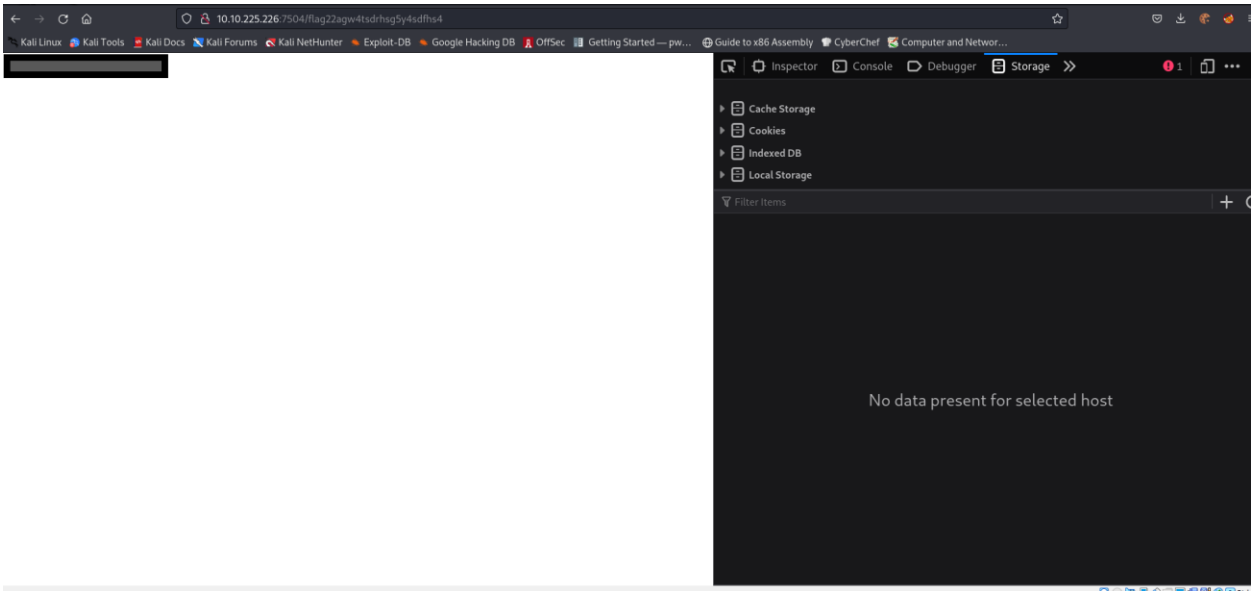
And let's look at the cookies, there are two cookies, one looks like a JWT and the other looks like a normal cookie, let's looks at the normal cookie,



Everything looks good, let's try refreshing the page, and whoa!

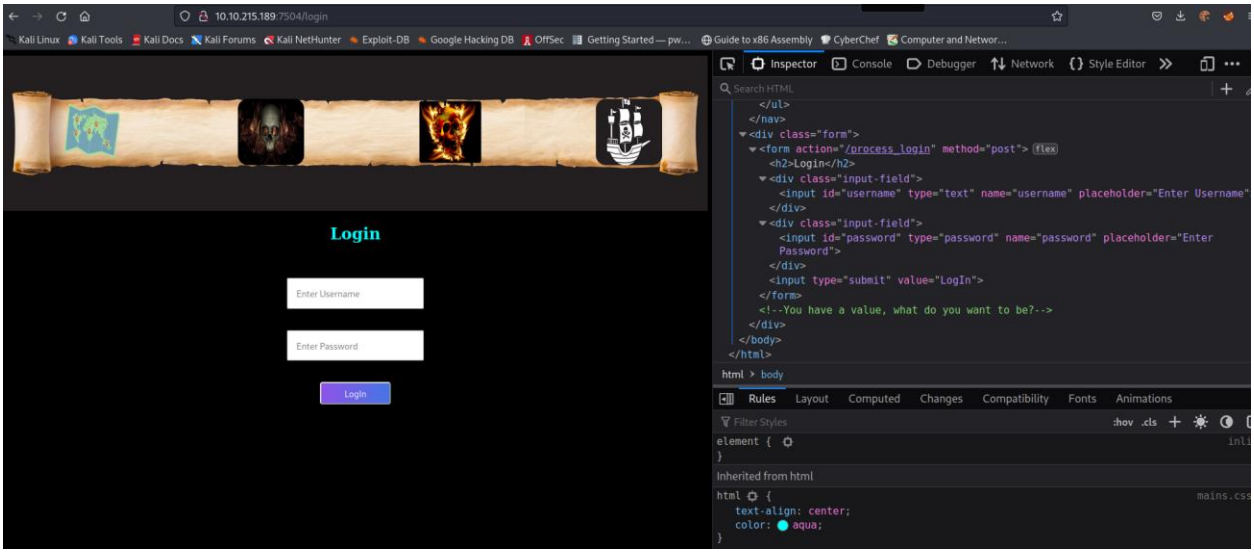


We get redirected and see a form already filled out for us, let's submit that form to get our flag!

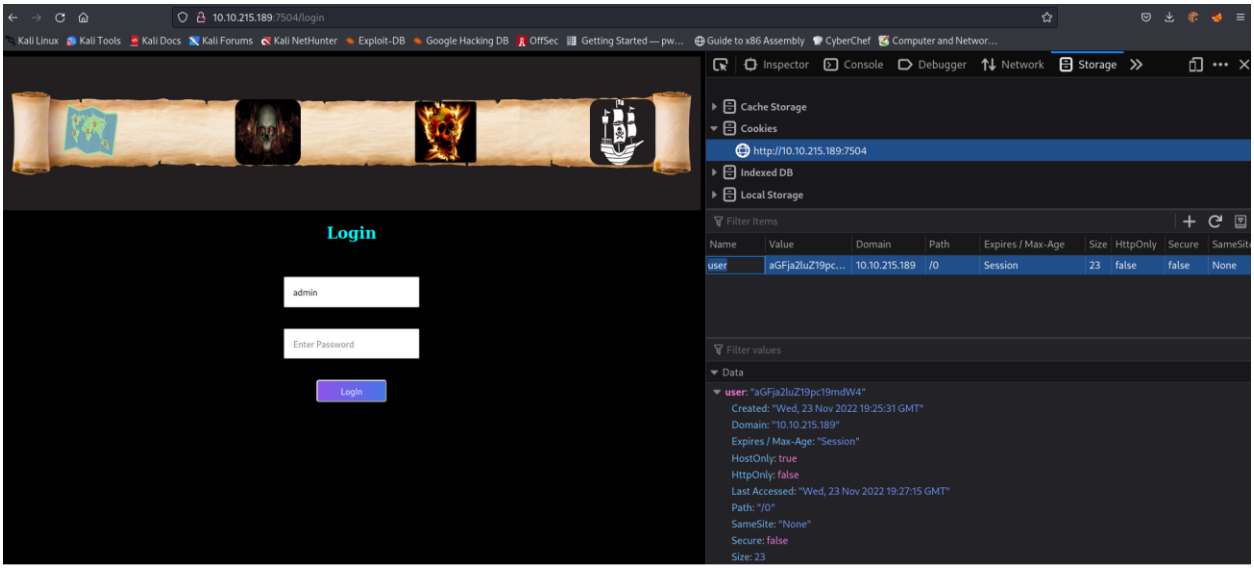


We move on to the third navlink, the flaming skull and we are presented with a login page.

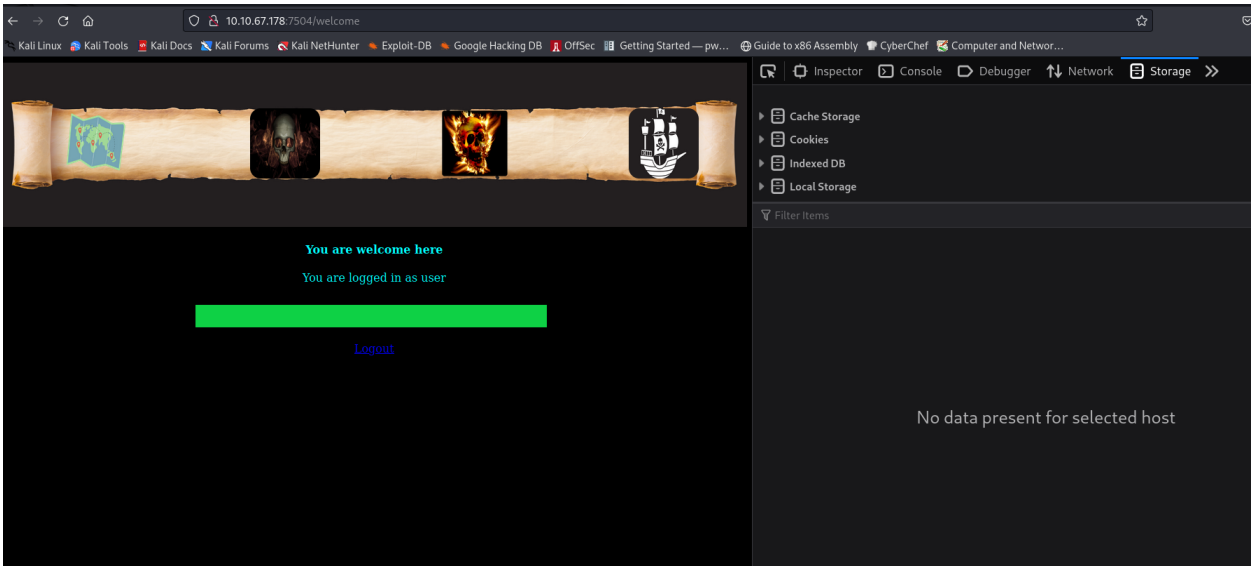
There is a hint,



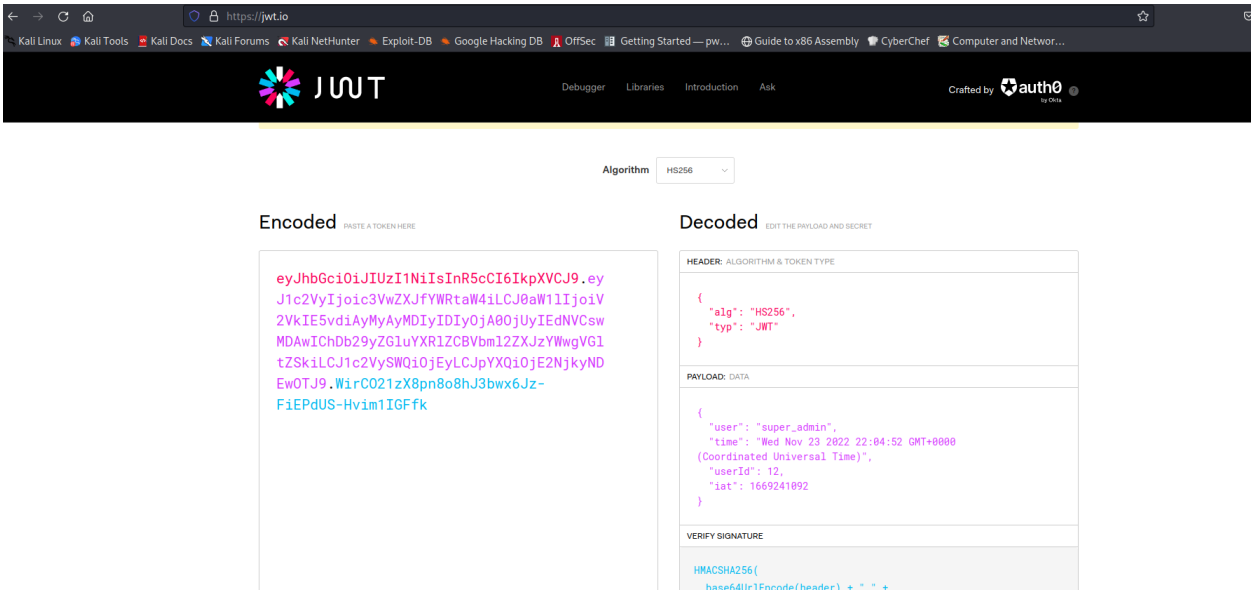
Let's sign in the the values from the cookie,



And we are redirected to the welcome page, and find the welcome flag.

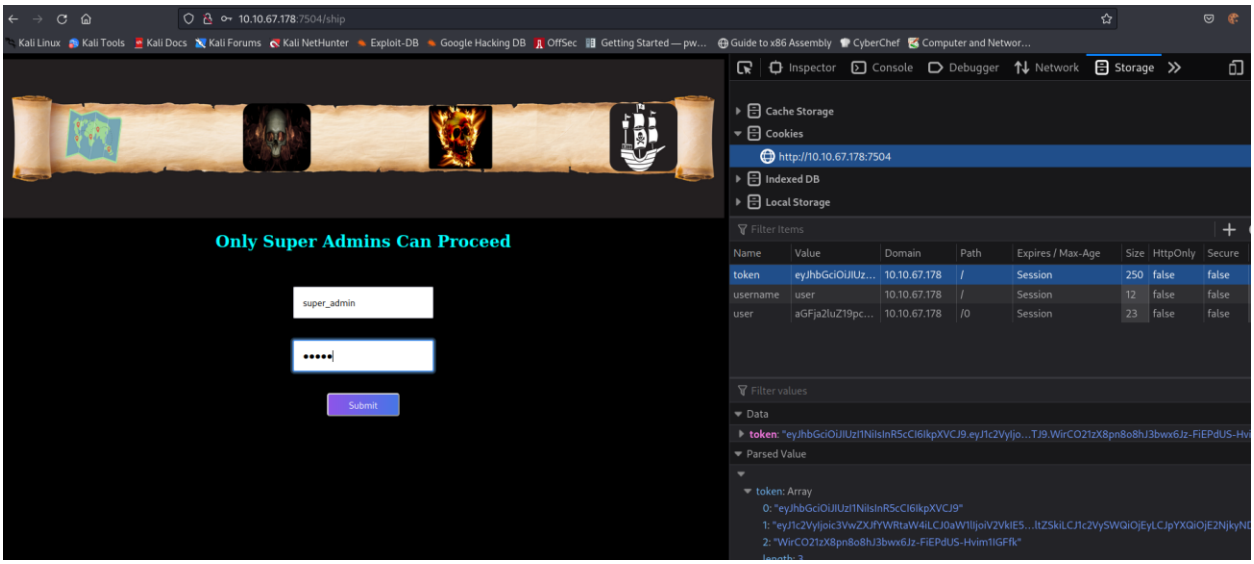


When we navigate to the fourth navlink we can see it saved another cookie with a name of token,

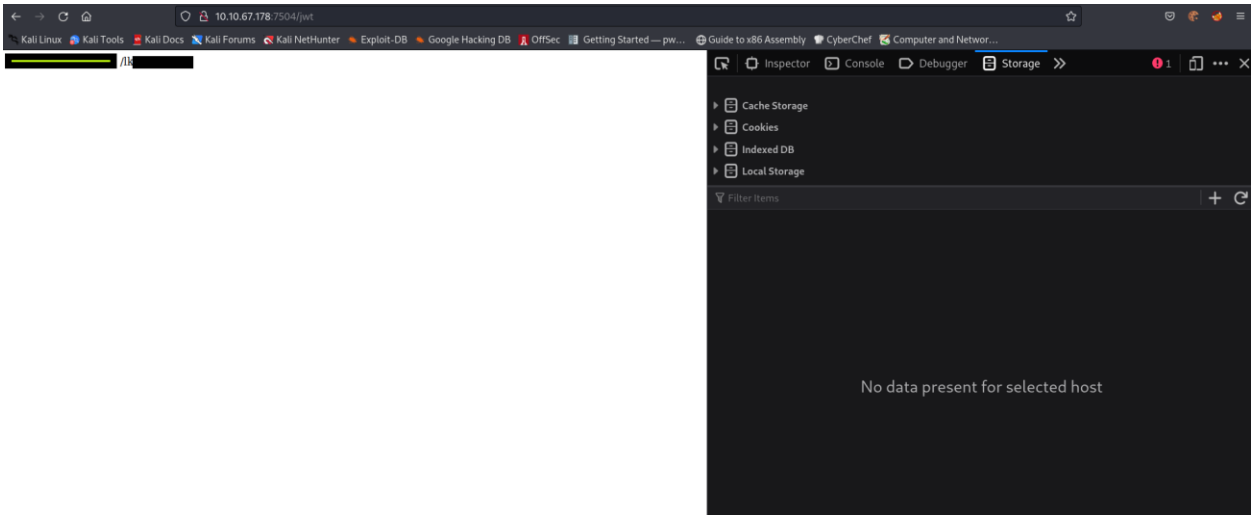


We use hashcat to decode secret

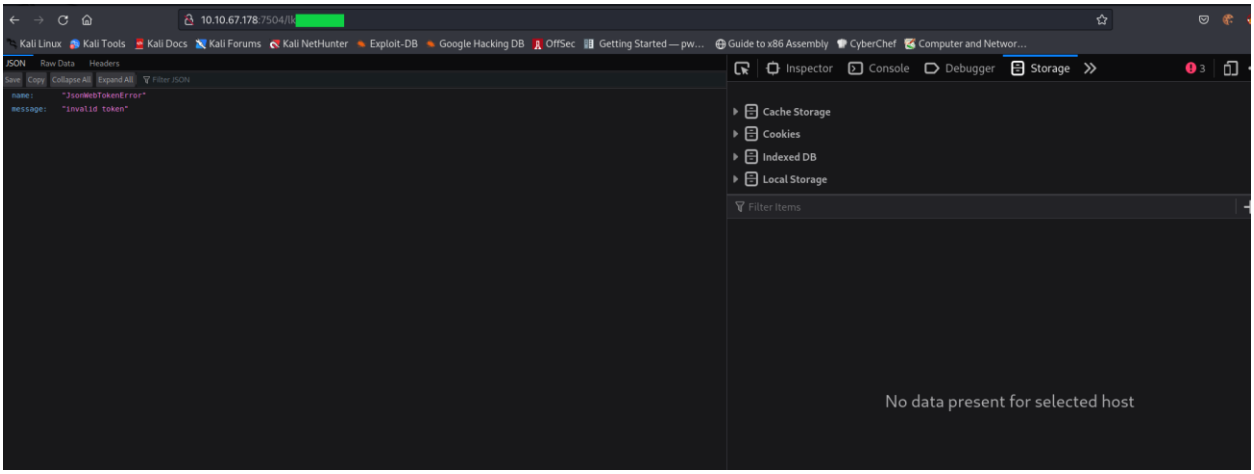
Let try login in



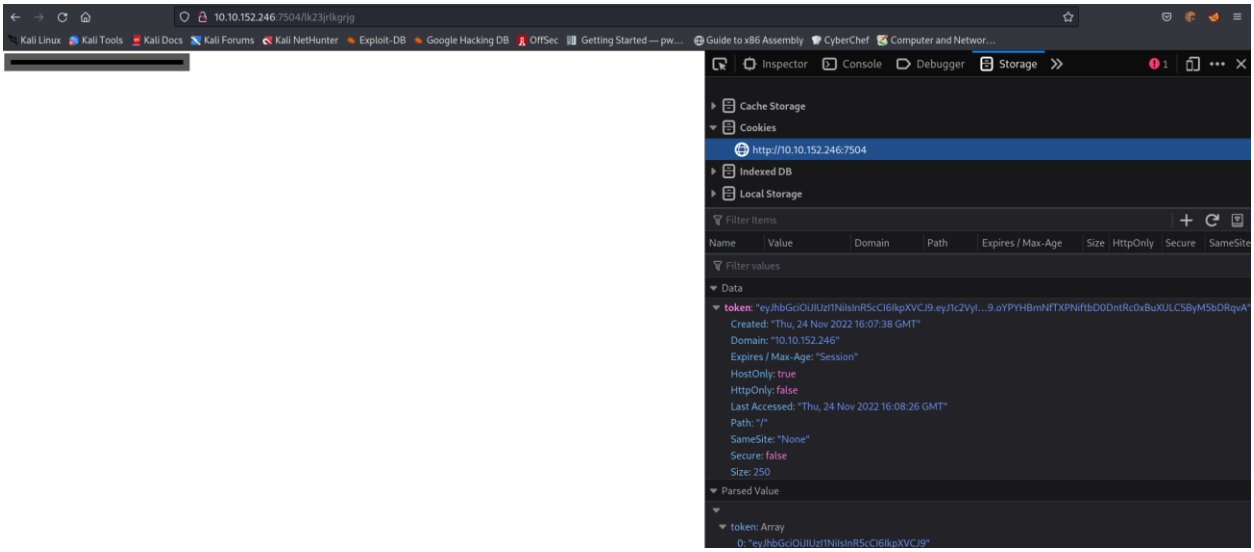
We get our flag and what looks like an endpoint



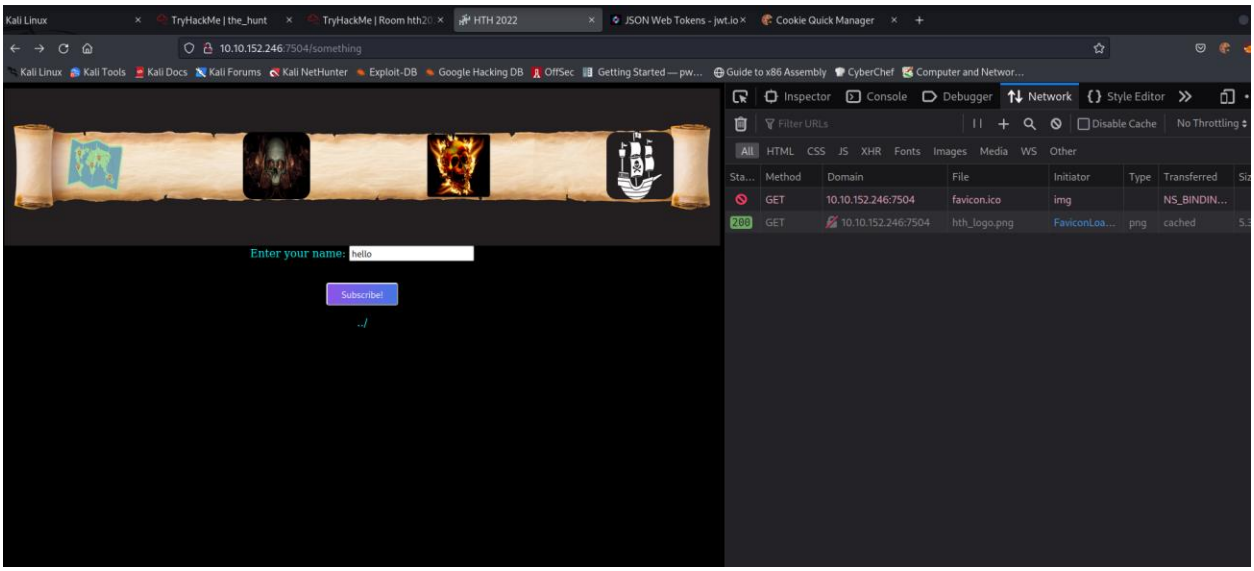
Let’s navigate to that end point,



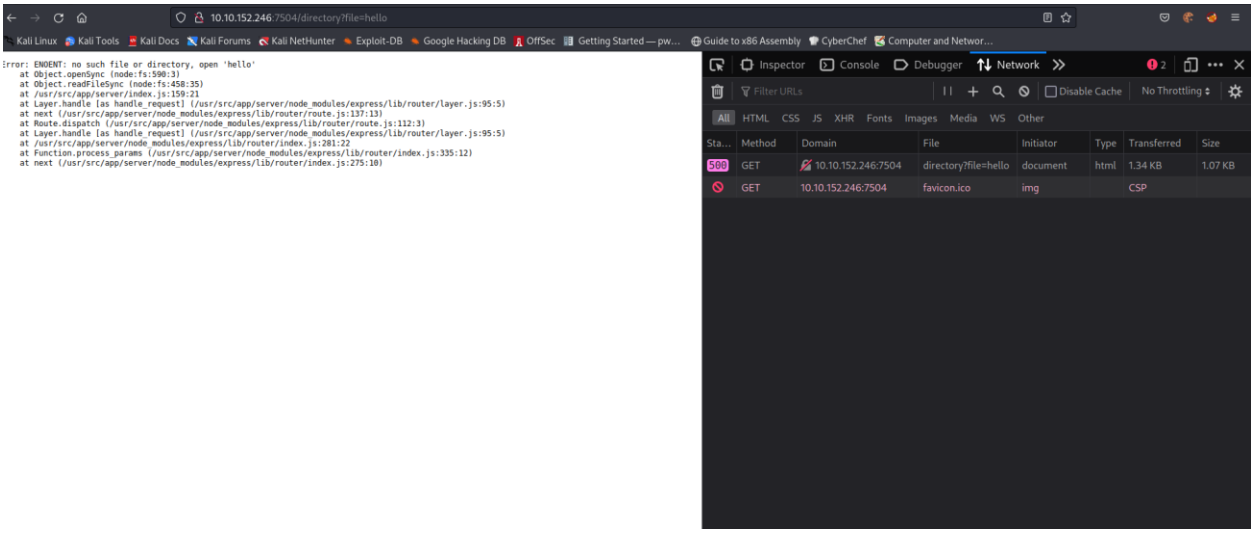
We get an error message, maybe if we use that endpoint as the secret in the JWT,,,



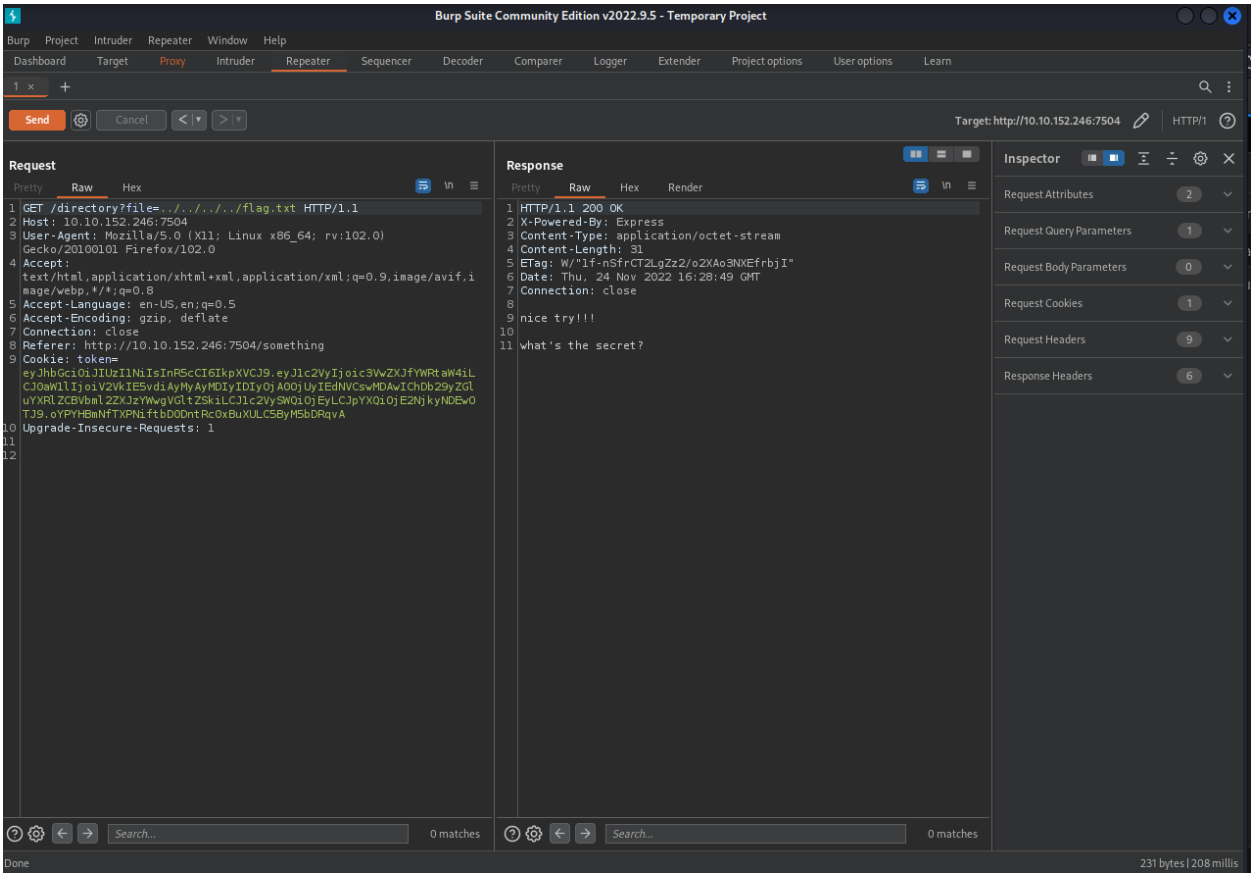
For the last flag, remember that /directory endpoint that dirsearch found,



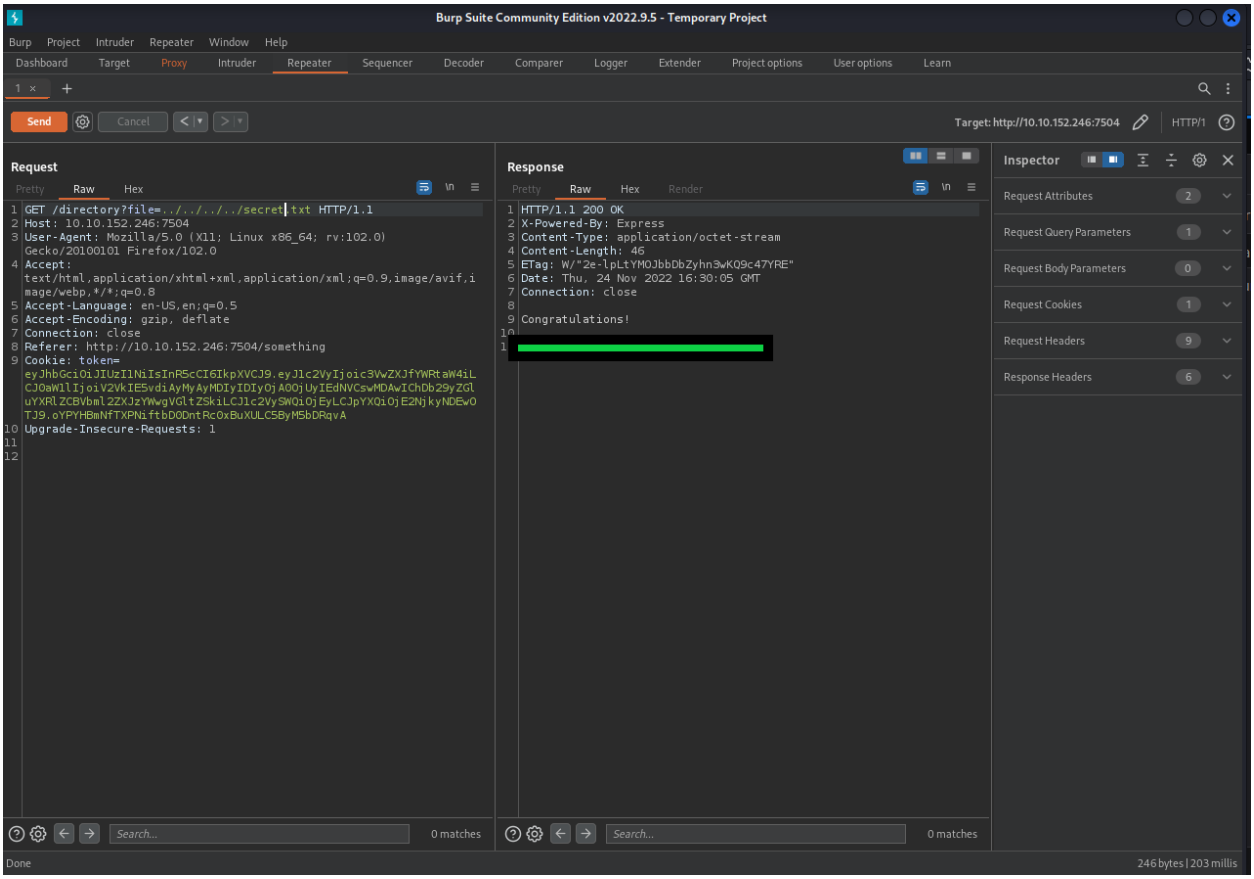
It immediately redirects us to /something, let's type hello and see what happens,



Let's send that to burpsuite,



Cool, we have directory traversal, the hint says secret a few times,



And we get our last flag!

Thank you for playing.