

UJ CyberClub CTF

- **Challenge name** Levi
- **Challenge category** Reverse

There was a file attached so I ran the command file to check for the type

```
(kali㉿kali)-[~/Downloads/Levi]
$ file Levi
Levi: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=c8bf1bd70c53551f78c33b0c01f97898586dd9a6, for GNU/Linux 3.2.0, not stripped
```

It's an executable file so I ran it then used the command ltrace to check how the program works

```
(kali㉿kali)-[~/Downloads/Levi]
$ ltrace ./Levi
puts("[+] Levi: Kenny ...what is the pa" ... [+] Levi: Kenny ...what is the password you goddamn monster?!:
) = 62
__isoc99_scanf(0x55bff70387b6, 0x7ffd6e00d2fe, 1, 0x7f5dea9c9190
1
) = 1
strcmp("1", "FZMUV90Q") = -21
+++ exited (status 0) +++
```

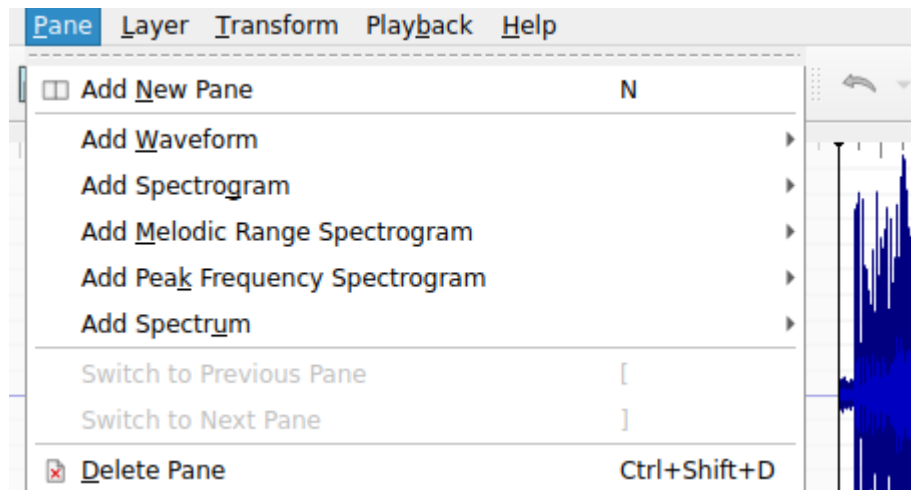
We can see that there is a function that takes the input and compares it with the value FZMUV90Q using strcmp function

```
(kali㉿kali)-[~/Downloads/Levi]
$ ./Levi
[+] Levi: Kenny ...what is the password you goddamn monster?!:
FZMUV90Q
UJCyberClub{KEeEeEeEeEeEeEny!}
```

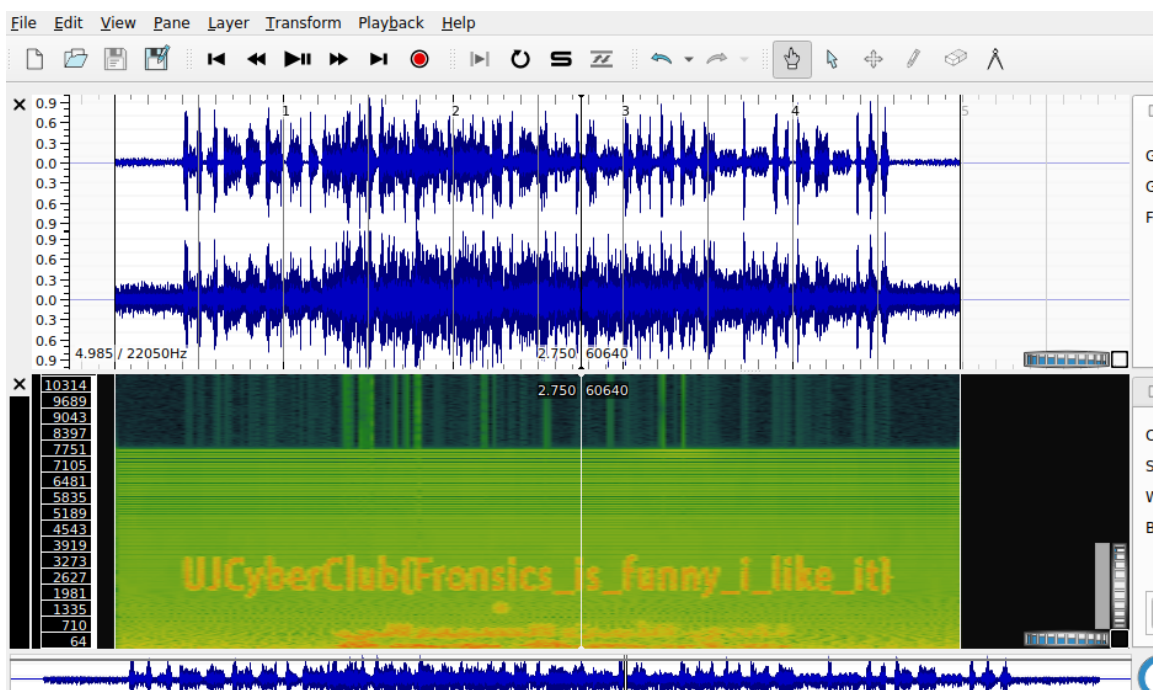
I put the value FZMUV90Q as a password and got the flag

- **Challenge name** CAN U HEAR ME??
- **Challenge category** Stenography

There was an audio file attached and challenge category is stenography I used sonic visualiser



Added spectrogram from the pane menu



And then flag was visible

- **Challenge name** LetsWarmUp
- **Challenge category** Reverse

```
kali@kali: ~/Downloads/CyberClubCTF/LetsWarmUp
File Actions Edit View Help

(kali@kali)~-[~/Downloads/CyberClubCTF/LetsWarmUp]
$ ls
pewpew.flag.py

(kali@kali)~-[~/Downloads/CyberClubCTF/LetsWarmUp]
$ python pewpew.flag.py
Please enter correct password for flag:
That password is incorrect

(kali@kali)~-[~/Downloads/CyberClubCTF/LetsWarmUp]
$
```

There was a python code attached so I ran it then it asked me for a password

```
pewpew.flag.py - VSCodium
File Edit Selection View Go Run Terminal Help

pewpew.flag.py X
home > kali > Downloads > CyberClubCTF > LetsWarmUp > pewpew.flag.py
1 import sys
2 a = "!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNPQRSTUVWXYZ" + \
3   "[\]^_`abcdefghijklmnopqrstuvwxyz{|}~"
4 def arg133(arg432):
5     if arg432 == a[71]+a[64]+a[79]+a[79]+a[88]+a[66]+a[71]+a[64]+a[77]+a[66]+a[68]:
6         return True
7     else:
8         print(a[51]+a[71]+a[64]+a[83]+a[94]+a[79]+a[64]+a[82]+a[82]+a[86]+a[78]+a[
9 a[81]+a[67]+a[94]+a[72]+a[82]+a[94]+a[72]+a[77]+a[66]+a[78]+a[81]+a[
10 a[81]+a[68]+a[66]+a[83])
11     sys.exit(0)
12     return False
13 def arg232():
14     return input(a[47]+a[75]+a[68]+a[64]+a[82]+a[68]+a[94]+a[68]+a[77]+a[83]+a[
15 a[68]+a[81]+a[94]+a[66]+a[78]+a[81]+a[81]+a[68]+a[66]+a[83]+a[
16 a[94]+a[79]+a[64]+a[82]+a[82]+a[86]+a[78]+a[81]+a[67]+a[94]+a[
17 a[69]+a[78]+a[81]+a[94]+a[69]+a[75]+a[64]+a[70]+a[25]+a[94])
18 def arg112():
19     print(a[54]+a[68]+a[75]+a[66]+a[78]+a[76]+a[68]+a[94]+a[65]+a[64]+a[66]+a[
20 a[74]+a[13]+a[13]+a[13]+a[94]+a[88]+a[78]+a[84]+a[81]+a[94]+a[69]+a[
21 a[75]+a[64]+a[70]+a[11]+a[94]+a[84]+a[82]+a[68]+a[81]+a[25])
22 def arg122():
23     print(a[52]+a[41]+a[34]+a[88]+a[65]+a[68]+a[81]+a[34]+a[75]+a[84]+a[65]+a[90]+a[81]+a[18]+a[
24 arg432 = arg232()
25 if arg133(arg432):
26     arg122()
27 sys.exit(0)
28
```

In line 5 we can see that the password might be the value of arg432 so I printed the value before the if condition

```
4 print(a[71]+a[64]+a[79]+a[79]+a[88]+a[66]+a[71]+a[64]+a[77]+a[66]+a[68])
```

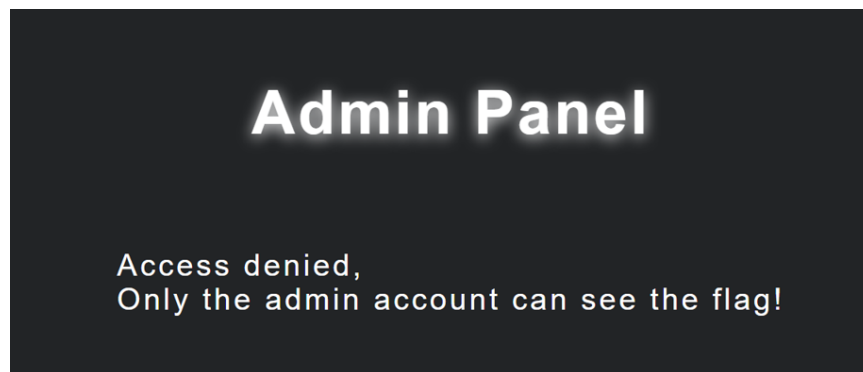
I ran the code again and got the password

```
(kali@kali)~-[~/Downloads/CyberClubCTF/LetsWarmUp]
$ python pewpew.flag.py
happyhance
Please enter correct password for flag:
```

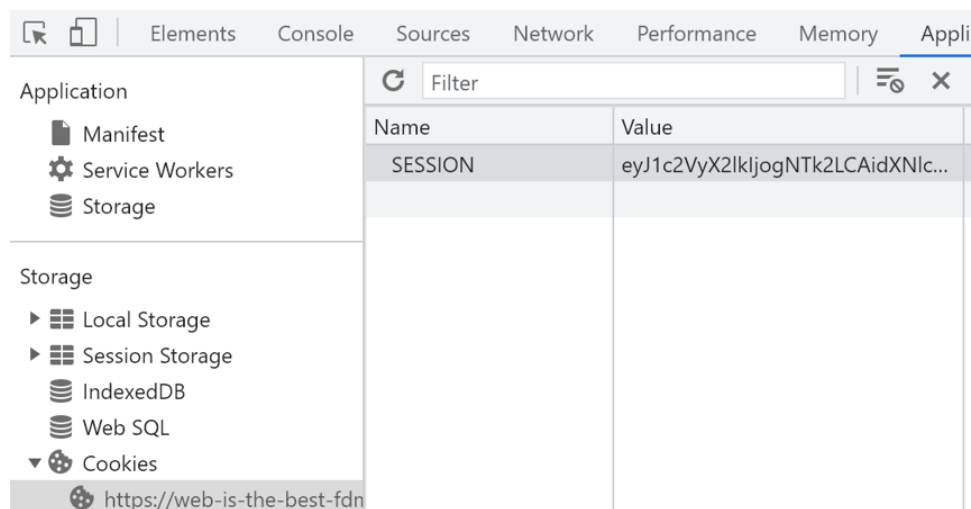
I entered the password and got the flag

- **Challenge name** Cookie
- **Challenge category** Web

The challenge made you go to a link that displayed this panel



From the challenge's name we can see that it has something to do with cookies so we will check the cookies of the website



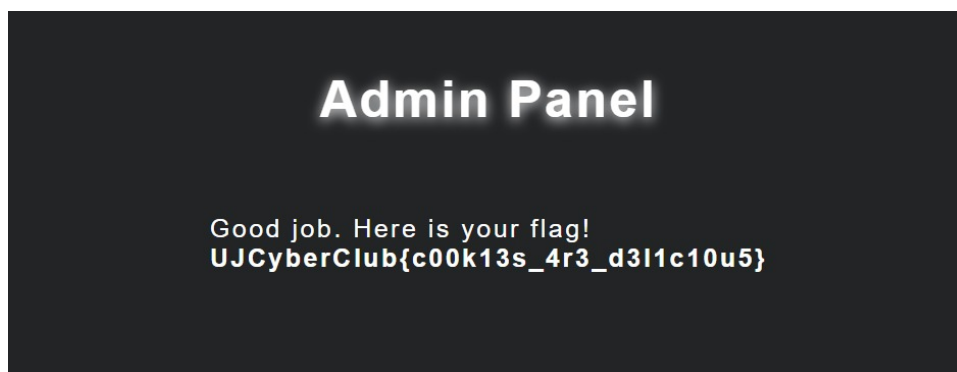
As we can see the value of the cookies is encoded using base64 so we will copy the value and decode it

```
{"user_id": 596, "username": "guest", "admin": false}
```

This is the value after decoding it so i'll try to change "guest" into "admin", set the user_id to 1 and change false to true

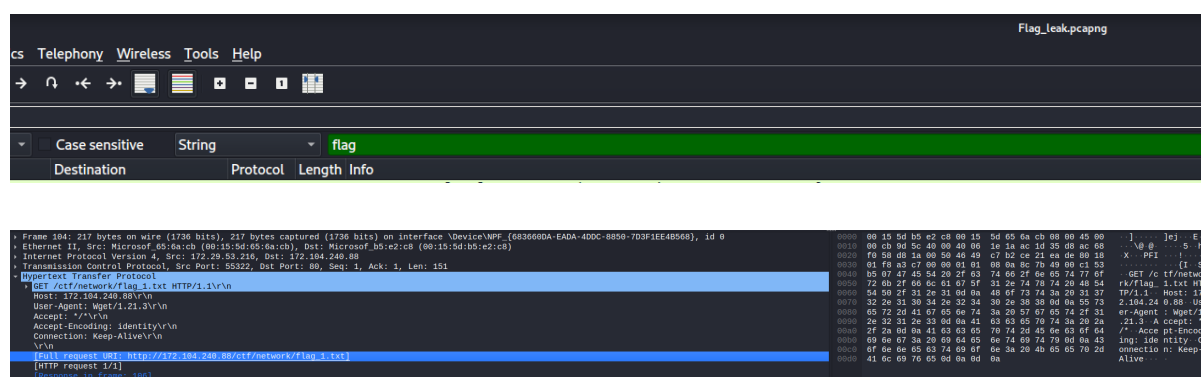
So the value will be `{"user_id": 1, "username": "guest", "admin": true}`

After encoding it to base64 and changing the cookie value the flag appeared

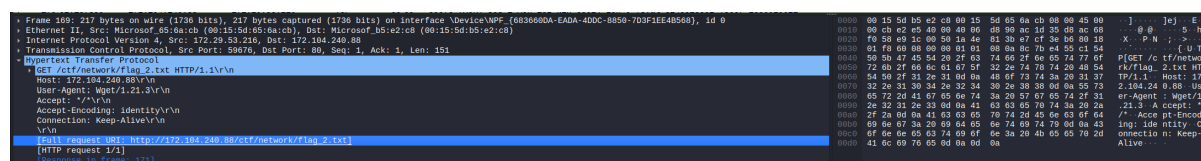


- Challenge name Flag leak
- Challenge category Network

There was a pcap file attached so I opened it using wireshark and searched for the word flag



When I opened the txt file it had a text encoded using base64 but wasn't the correct flag so I kept looking and found another txt file



After decoding the text in the file I got the correct flag

```
svat=2356929551 TSecr=0 WS=128  
(kali㉿kali)-[~] 43528283 TSecr=2356929551 WS=128  
$ echo VUpDeWJlckNsdWJ7eTB1XzRyM19nMDBkX3cxdGhfdzFyMzVoNHJrfQ== | base64 -d  
UJCyberClub{y0u_4r3_g00d_w1th_w1r35h4rk}
```