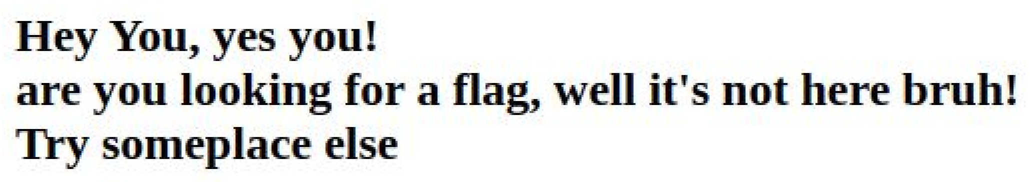
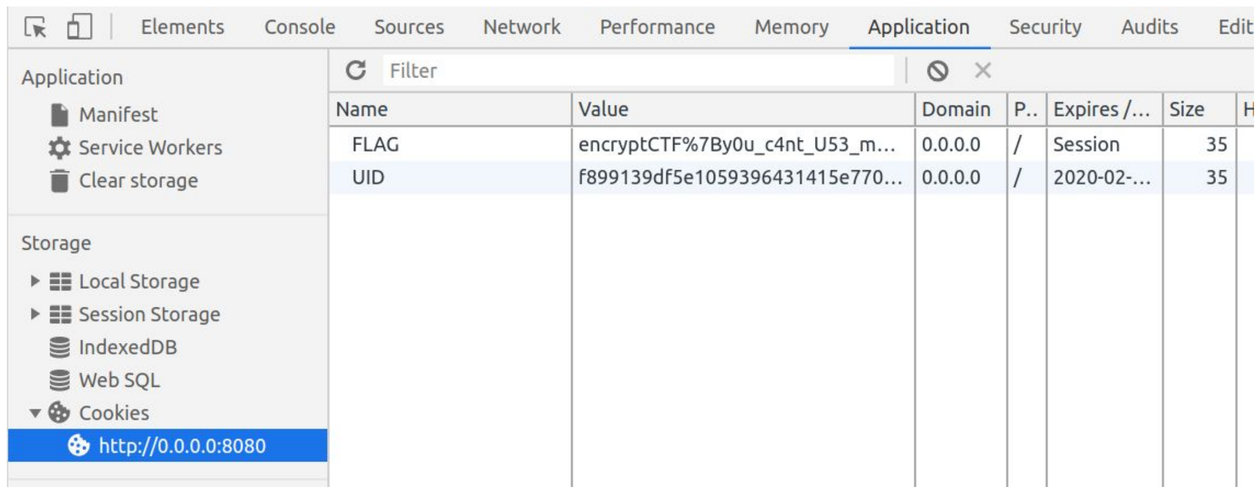
WEB: Sweeeeeet

We are given the following web page:



Hey You, yes you!
are you looking for a flag, well it's not here bruh!
Try someplace else

Nothing much to look around here. By inspecting the cookies we can see something interesting:



Name	Value	Domain	P..	Expires /...	Size	H
FLAG	encryptCTF%7By0u_c4nt_U53_m...	0.0.0.0	/	Session	35	
UID	f899139df5e1059396431415e770...	0.0.0.0	/	2020-02-...	35	

There are two cookies:

1. FLAG: which contains an incomplete flag;
2. UID: user ID

What we can think is that by giving the correct user-ID, the page will return the flag.

The value contained in UID “f899139df5e1059396431415e770c6dd” seems a hashed value.
By using a password cracker we can see that the value is an MD5 hash, where the ciphertext is 100.

This means that the UID= MD5(100) is a wrong UID (since we don’t have a correct flag). UID seems the MD5 of an integer: what if we bruteforce them? We can start from 1 to 100.
In order to do it, we suggest using Python code.

The flag can be found at iteration 0:

encryptCTF%7B4lwa4y5_Ch3ck_7h3_c00ki3s%7D%0A

This is url-formatted. We obtain the flag:

encryptCTF{4lwa4y5_Ch3ck_7h3_c00ki3s}