FLERT [MISC]

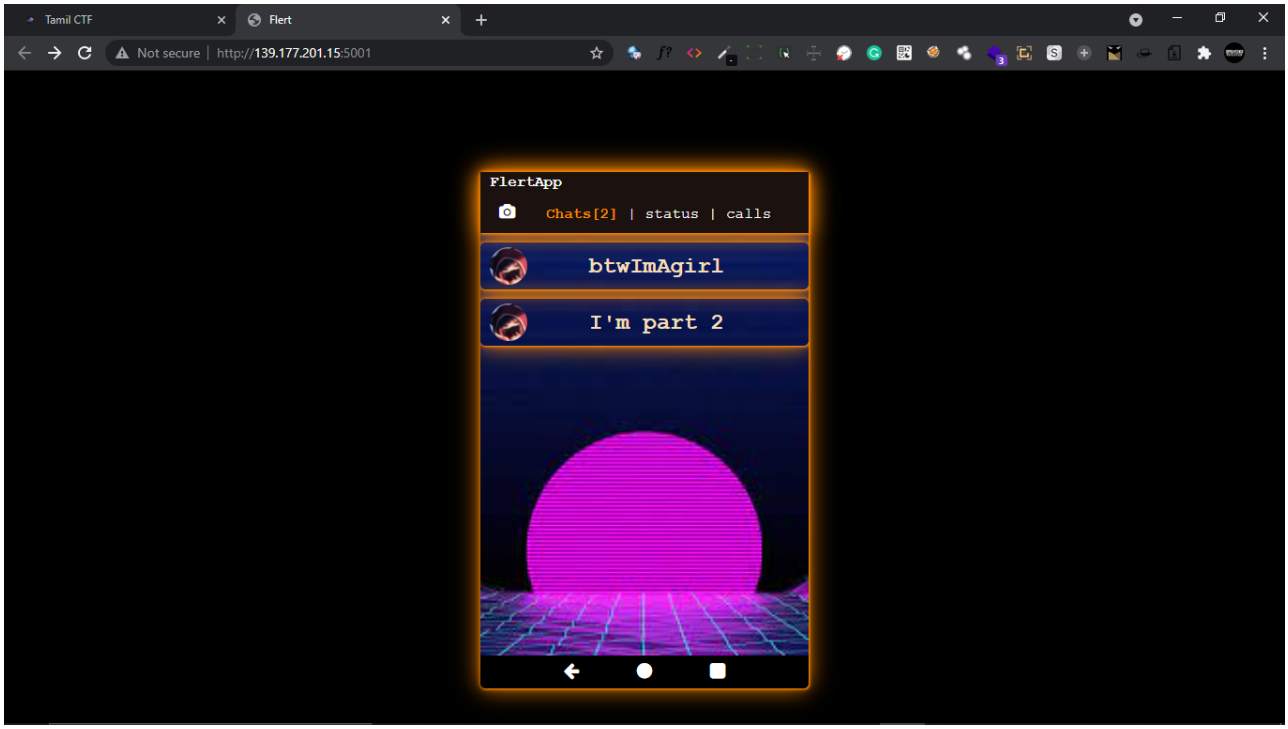
Description

- This website has cool colours 😉
- Get first part of flag by chatting with **btwImAgirl**
- Get second part of the flag by chatting with **I'm part 2**

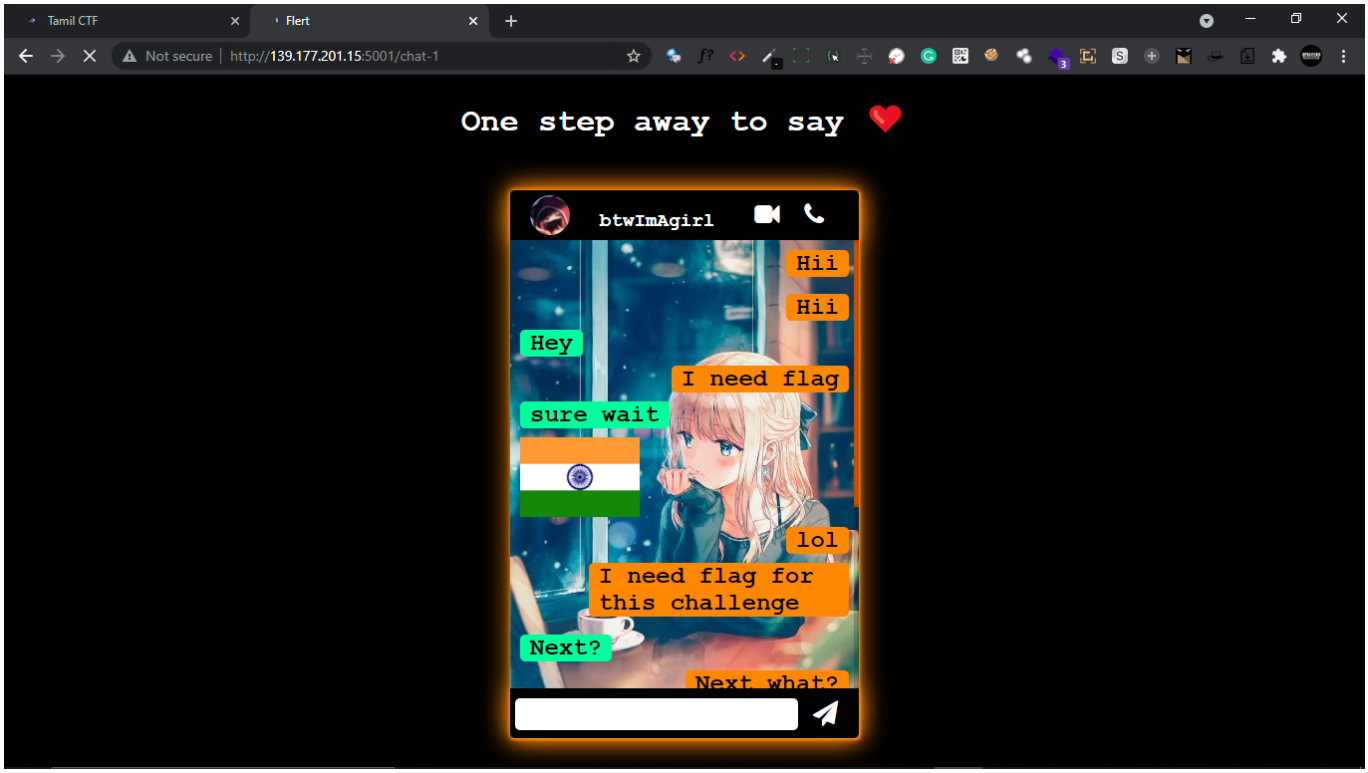
Writeup

First part

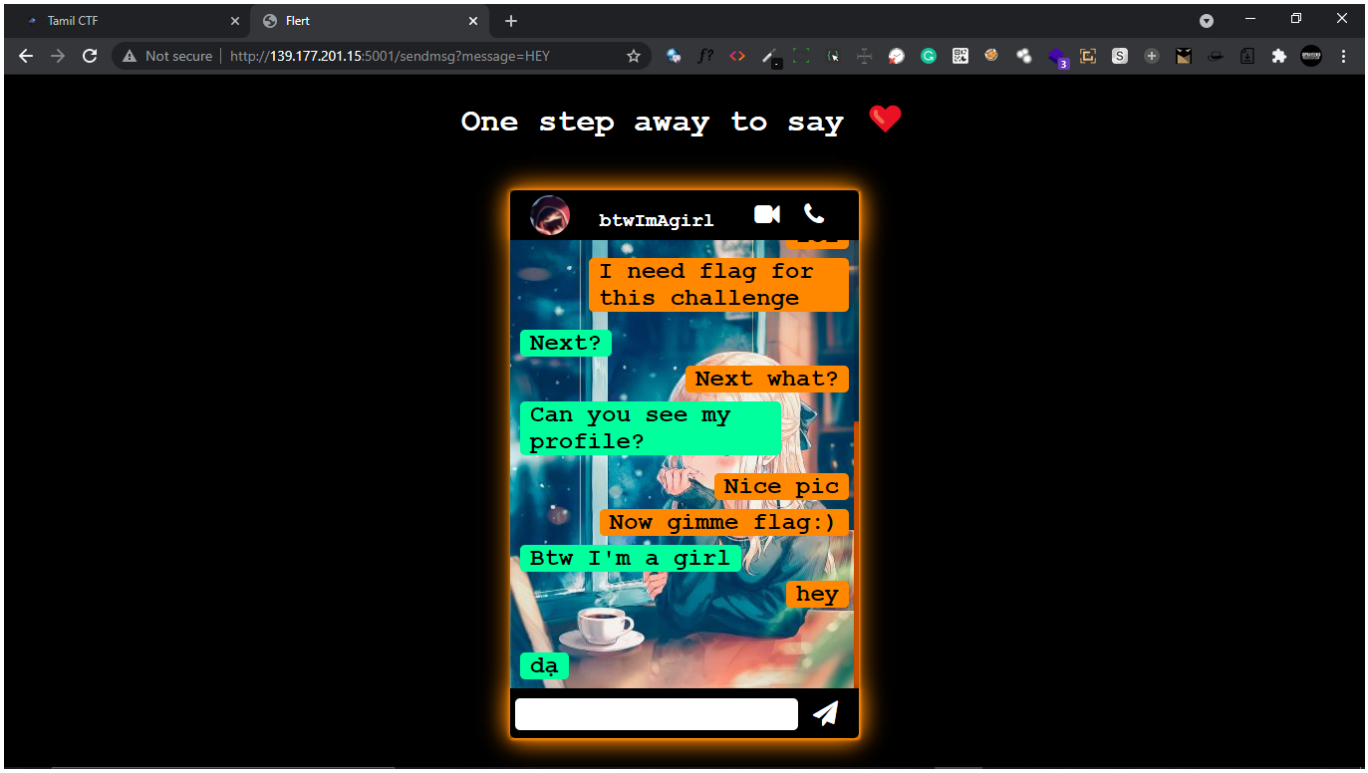
- First let's see the website
- Let's click the first chat



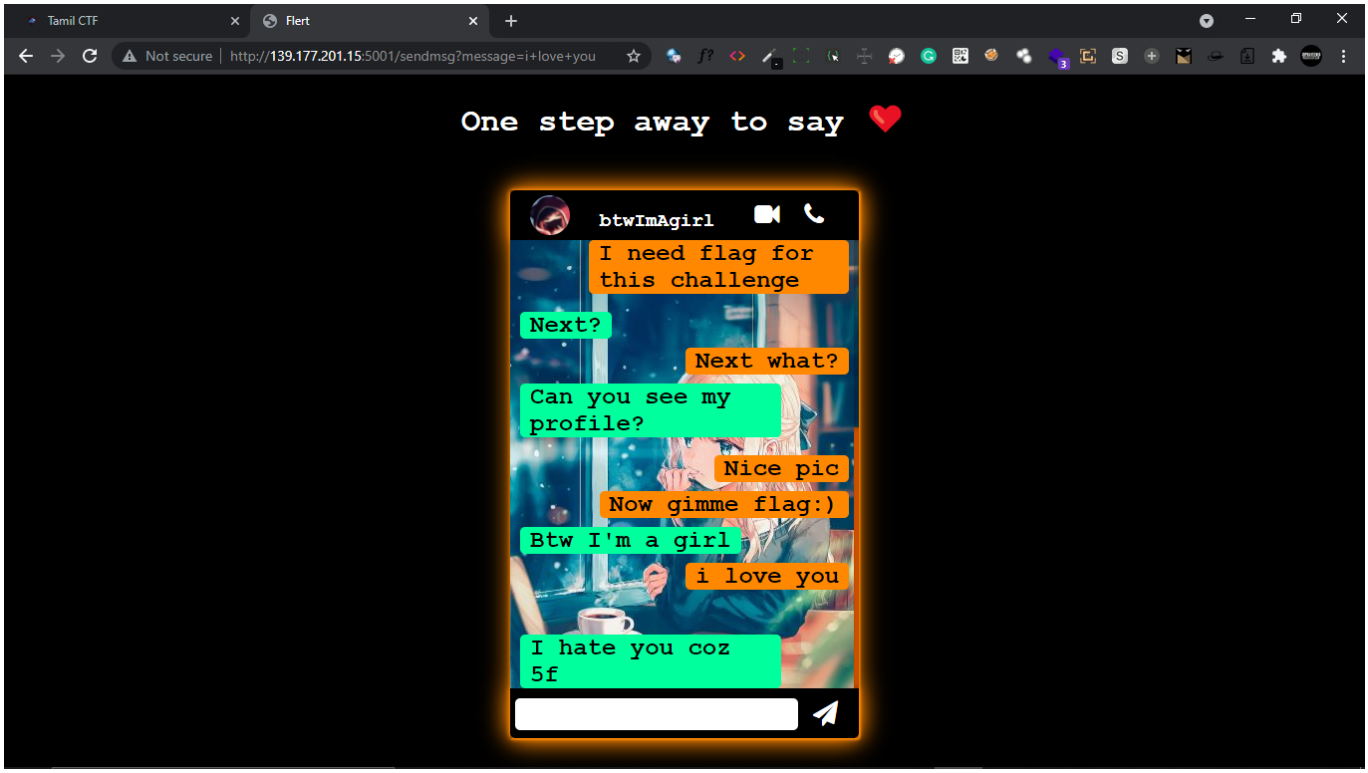
First chat



- Some chats are here
- He's asking for flag
- But she doesn't gave it
- Now let's send a message



- Fine it replying us, it looks like a chat bot :)
- But it doesn't giving us flag :(
- Look at the title `One step away to say ❤`
- Fine let's send `i love you`



- `I hate you coz 5f`
- Ok what means 5f?
- Let's send `i love you` again
- Now it replied `I hate you coz 61`
- Looks like these are hex values
- Sending `i love you` again, she replied `I hate you coz 6c`
- Fine now let's try to collect these values by sending `i love you` multiple times

```
❯ for i in {1..100}; do curl "http://139.177.201.15:5001/sendmsg?message=i+love+you" | grep "hate" >> out.txt; done
```

- I'm greping it like this and storing the output in out.txt

interesting things in every output

```
color: #4;">I hate you coz 6c
color: #17;">I hate you coz 53
```

- description says `this website has cool colours 😉`
- and we getting randome hex values in every output
- So looks like value of the colour is the index
- ex `color: #4;">I hate you coz 6c`
- so `6c` is in `4` th index
- by using this we can arrange the output

Arranging together

- We don't know how many characters are there
- So let's put it in a for loop and sort the unique output
- I'm gonna run this command 1000 times using for loop

```
for i in {1..1000}; do curl "http://139.177.201.15:5001/sendmsg?
message=i+love+you" | grep "hate" >> out.txt; done
```

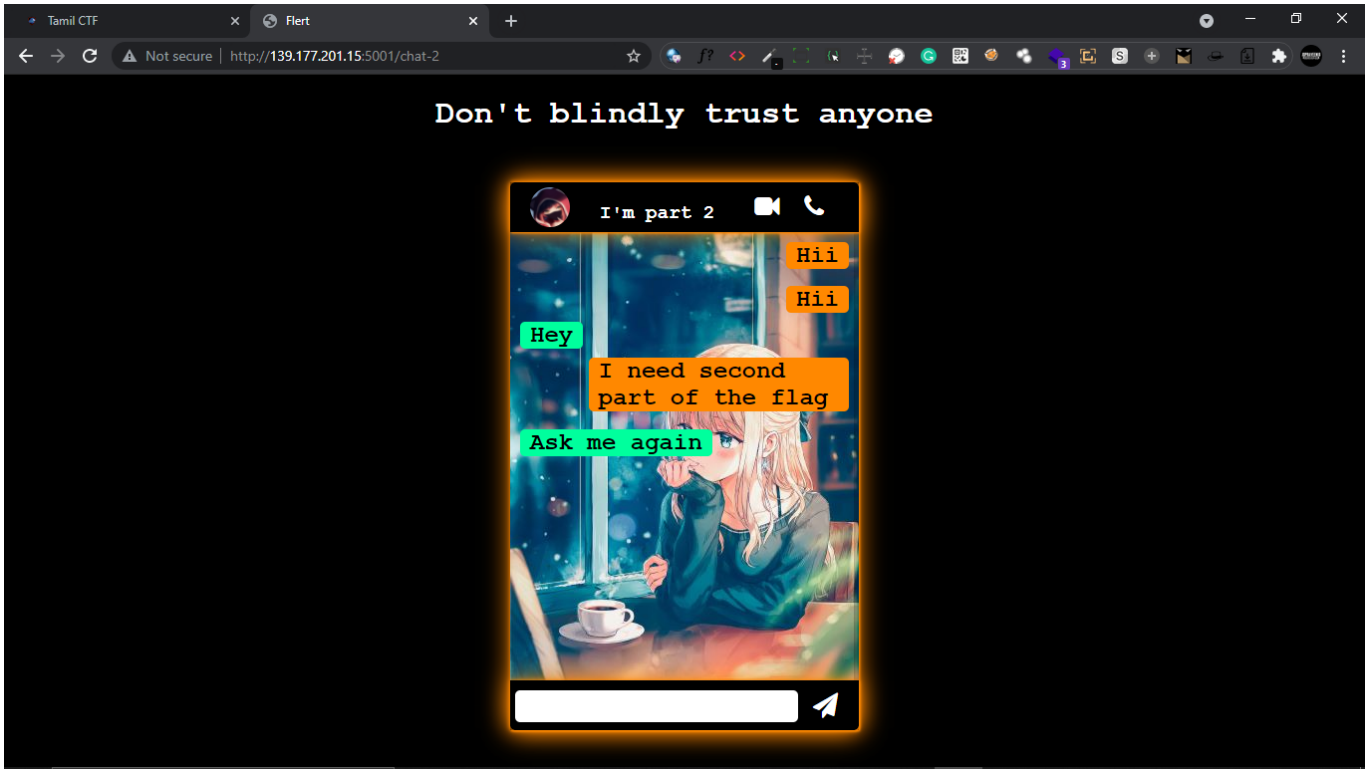
- And saving this output in `out.txt` so we can uniquely sort things easily
- sort the unique things
- and arrange it with thos indexes
- Cool we arranged the hex value
- Now let's convert this **Hex to Ascii**

```
TamilCTF{0.0_w0w_Sh3_
```

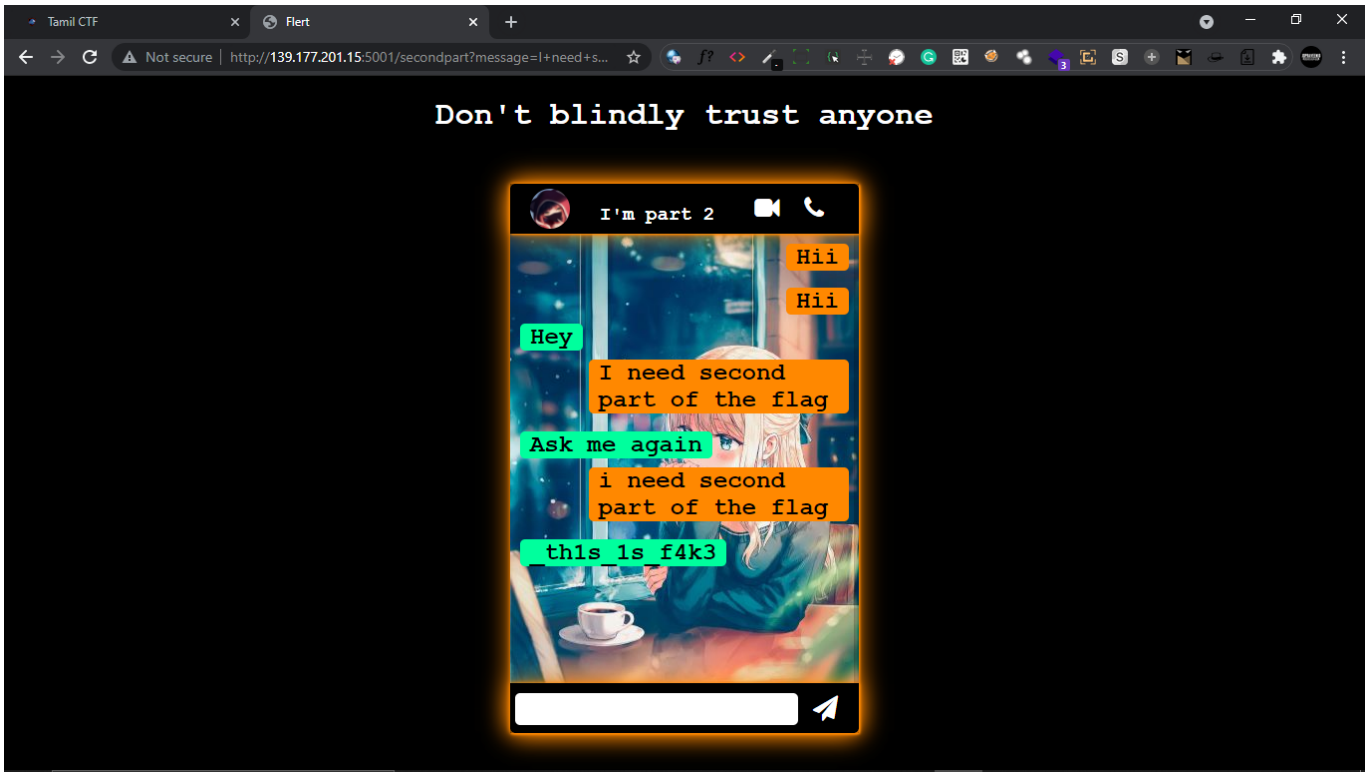
- Finnaly we got the first part of the flag
- Let's go for the second part

Second part

- Let's go to part 2

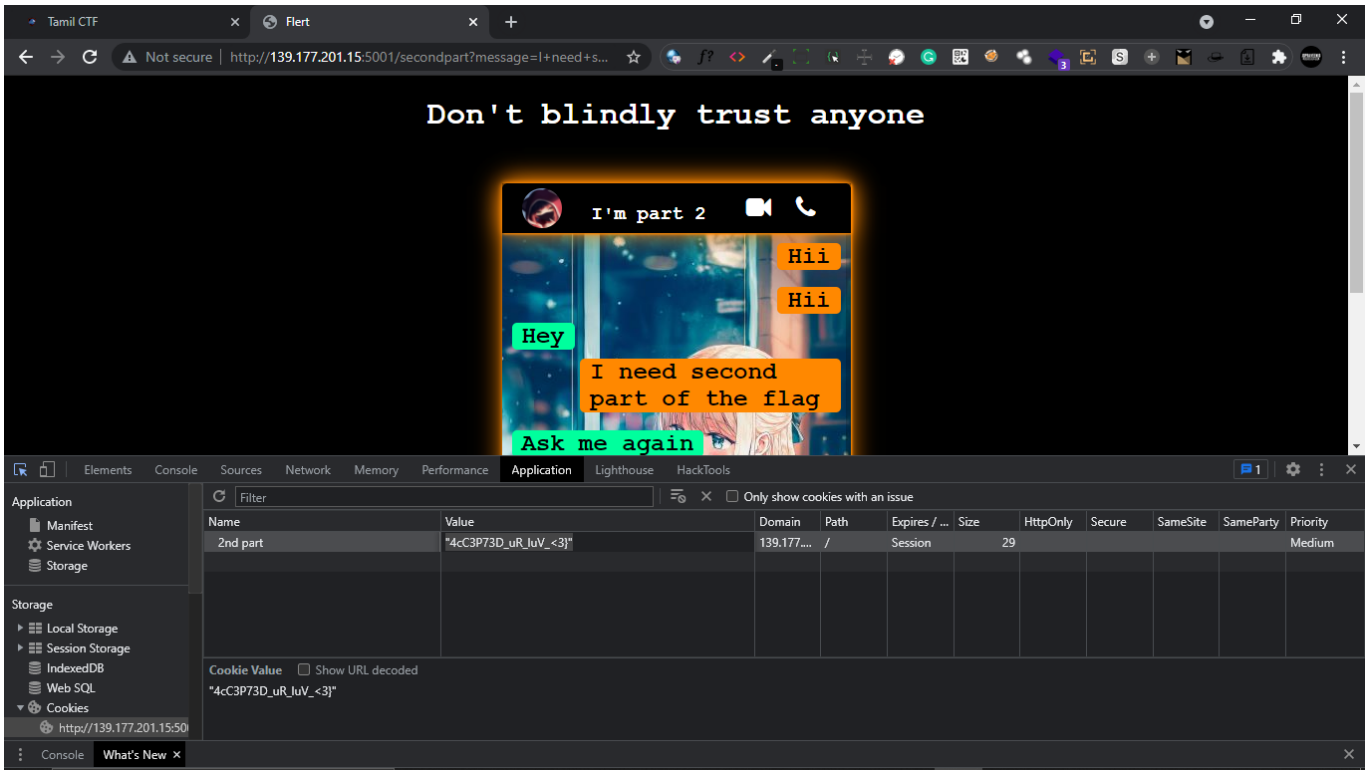


- Some chat's are here, and she said to ask that again
- Let's send `I need second part of the flag` this



- We got `_th1s_1s_f4k3` but I think it's fake flag
- See the title `Don't blindly trust anyone`
- Flag is not in source

- Let's check cookies



- Wow it's here, finnaly we got second part also
- `4cC3P73D_uR_luV_<3}`
- Let's join part1 and part2

`TamilCTF{0.0_w0w_Sh3_4cC3P73D_uR_luV_<3}`

- Thats the flag