Challenge Writeup

Title : can you hack this screenshot service

Category : Web

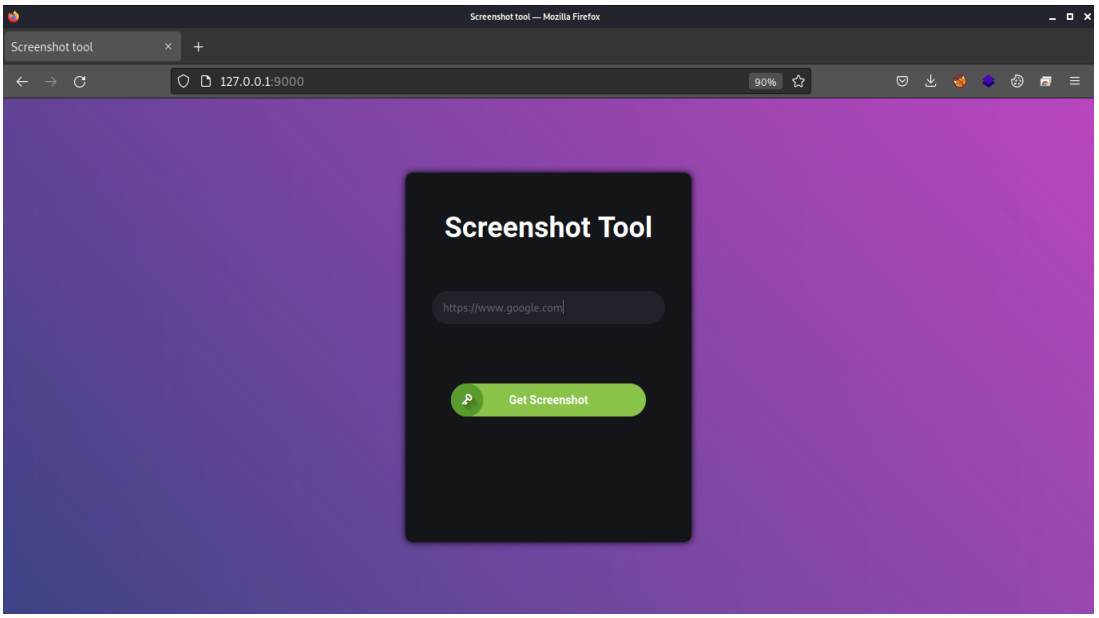
Author : Gokul

Description:
  This screenshot tool can take screenshot of any url that you give as input but before publishing this to the internet i need to check for any security issues , i need help of some ethical hackers to check it and find the flag.

Points : 200

Walkthrough:

- Home page

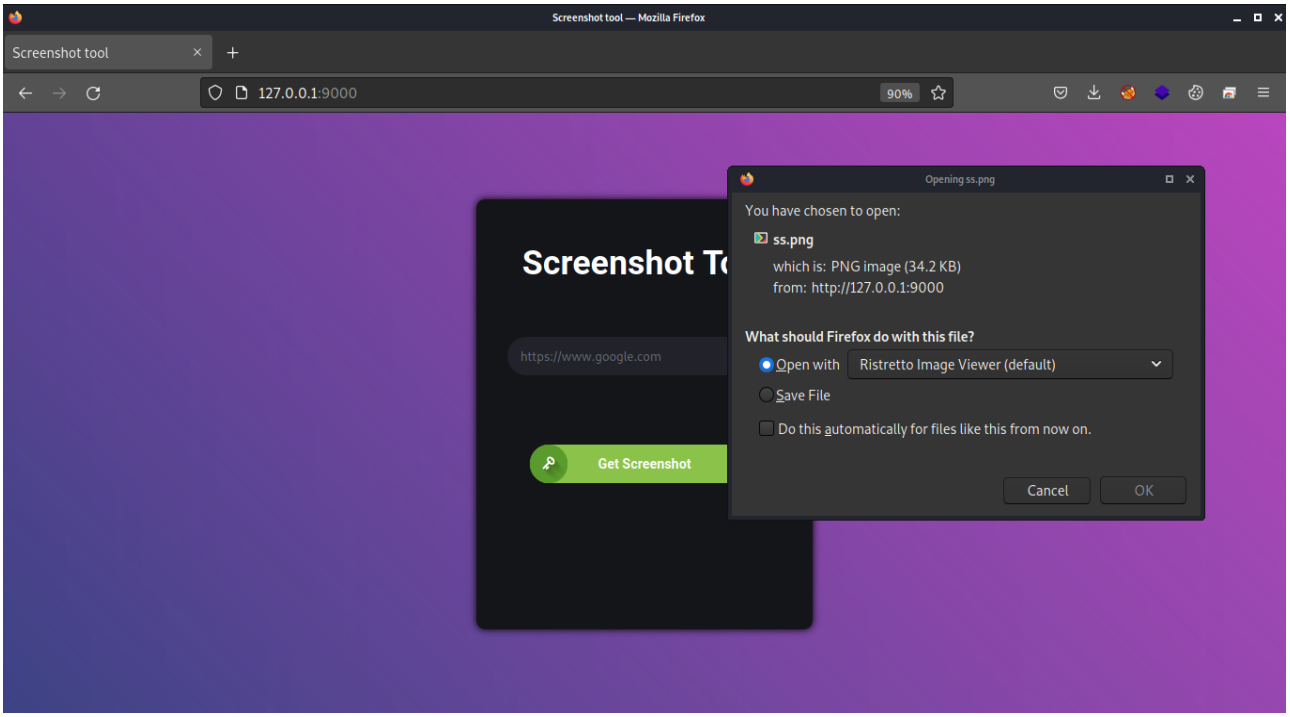


The Home page looks like this and its a screenshot tool which gives us the screenshot of the URLs or Website that we enter !

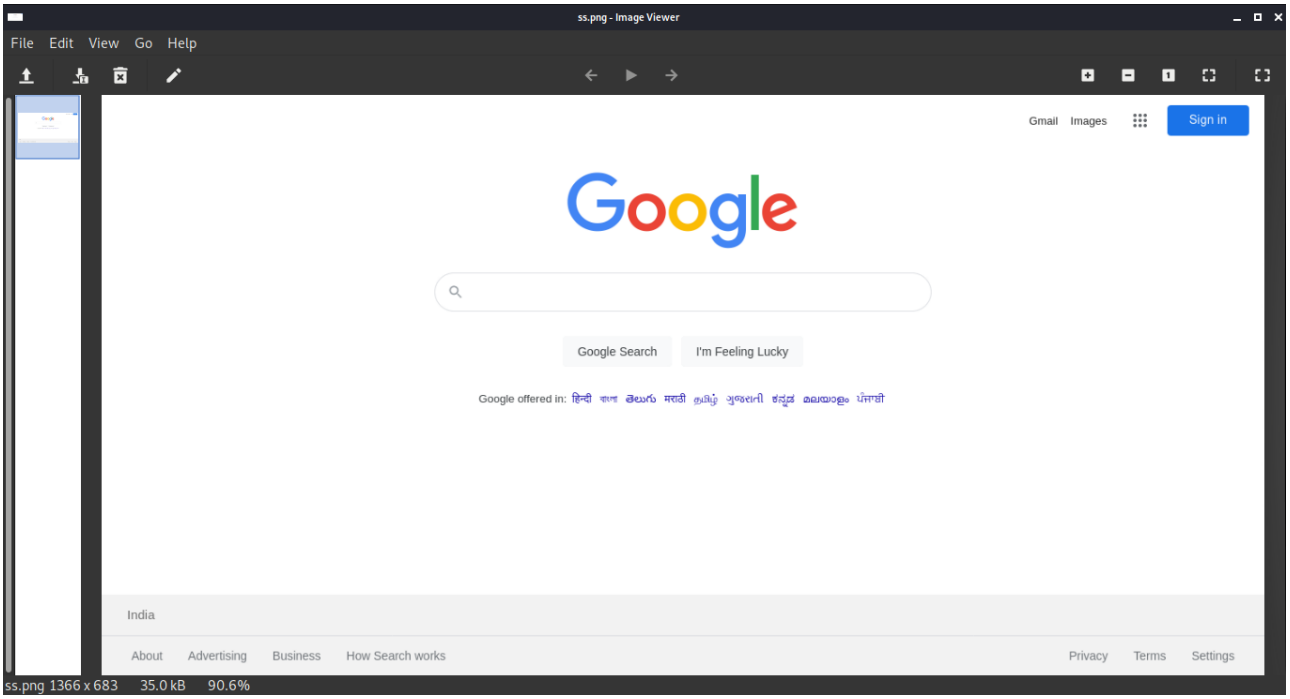
Lets give some url (https://www.google.com) and check it

Once we give the URL and click get screenshot we can get the screenshot downloaded

And it looks like a normal screenshot service provider



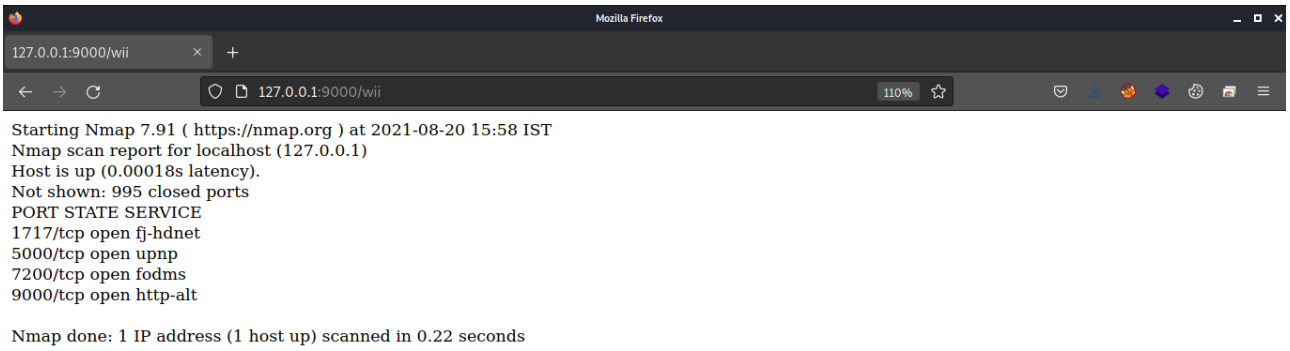
Once we open that downloaded image we can see the correct screenshot of the Entered URL



After that there is no information on that site in comments or cookies or in headers , Lets check some hidden paths with gobuster

Once run a directory bruteforce we can find a path /wii and lets check that path

/wii path shows the nmap scan on a localhost and we can see 4 ports are open

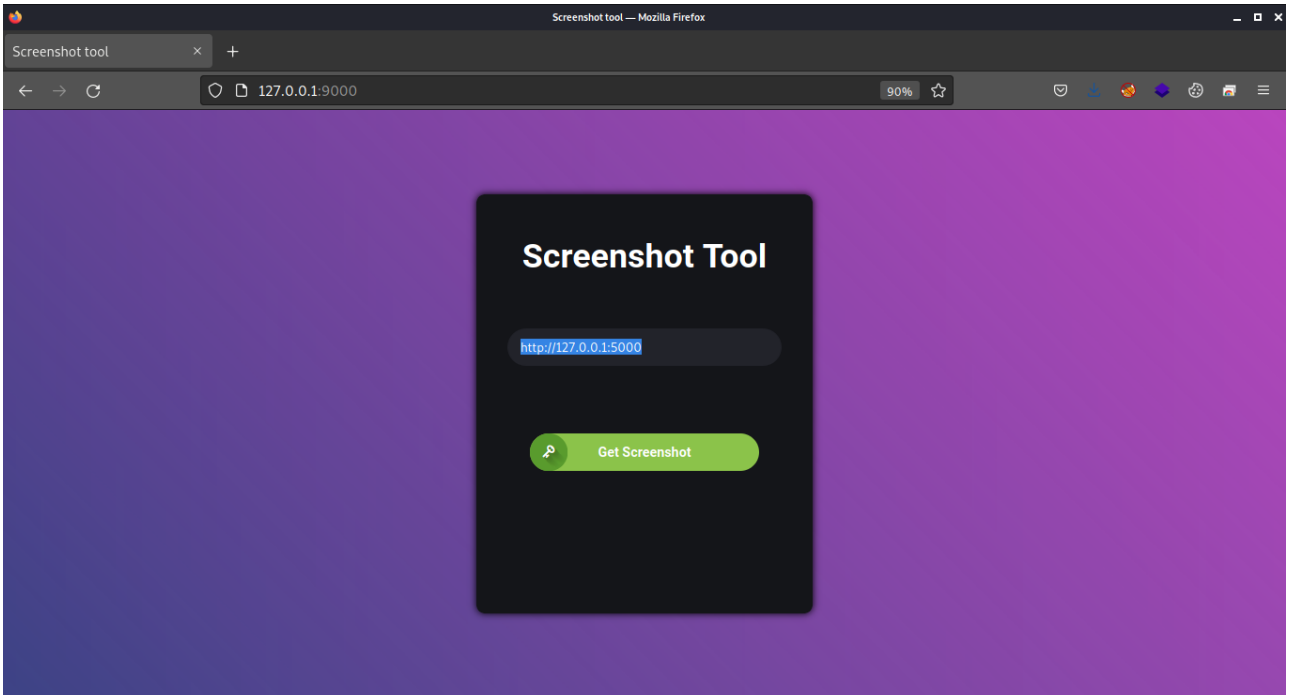


We can see 4 ports open on localhost but we are not able to connect it

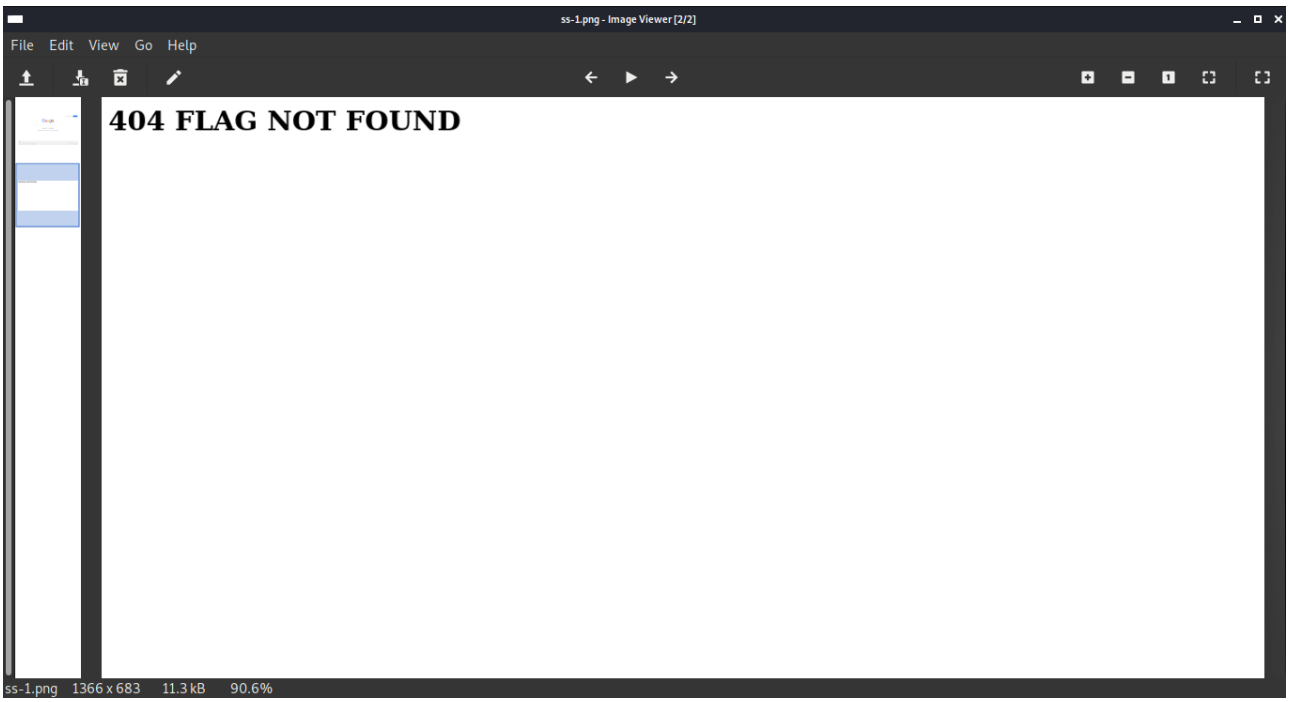
Yes we have the screenshot service on this machine , that can access these services running locally

Lets try to input the URL http://127.0.0.1:5000

And lets see what does the screenshot shows

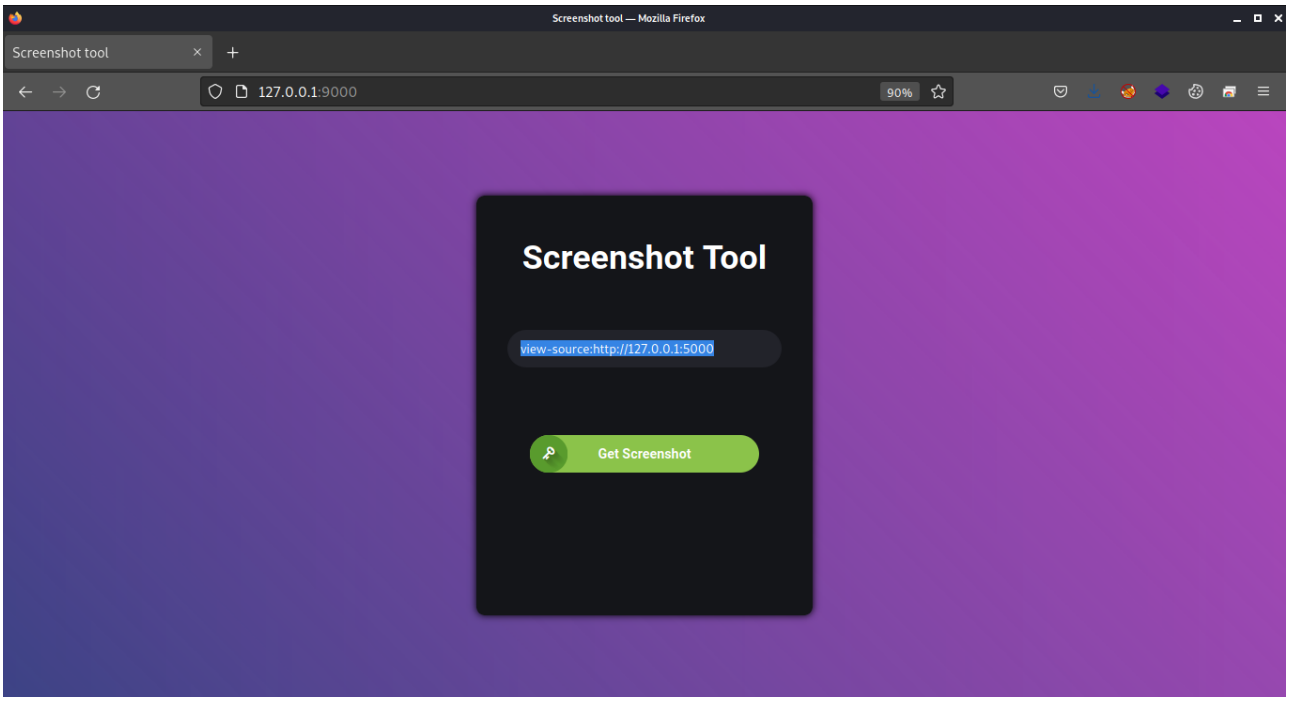


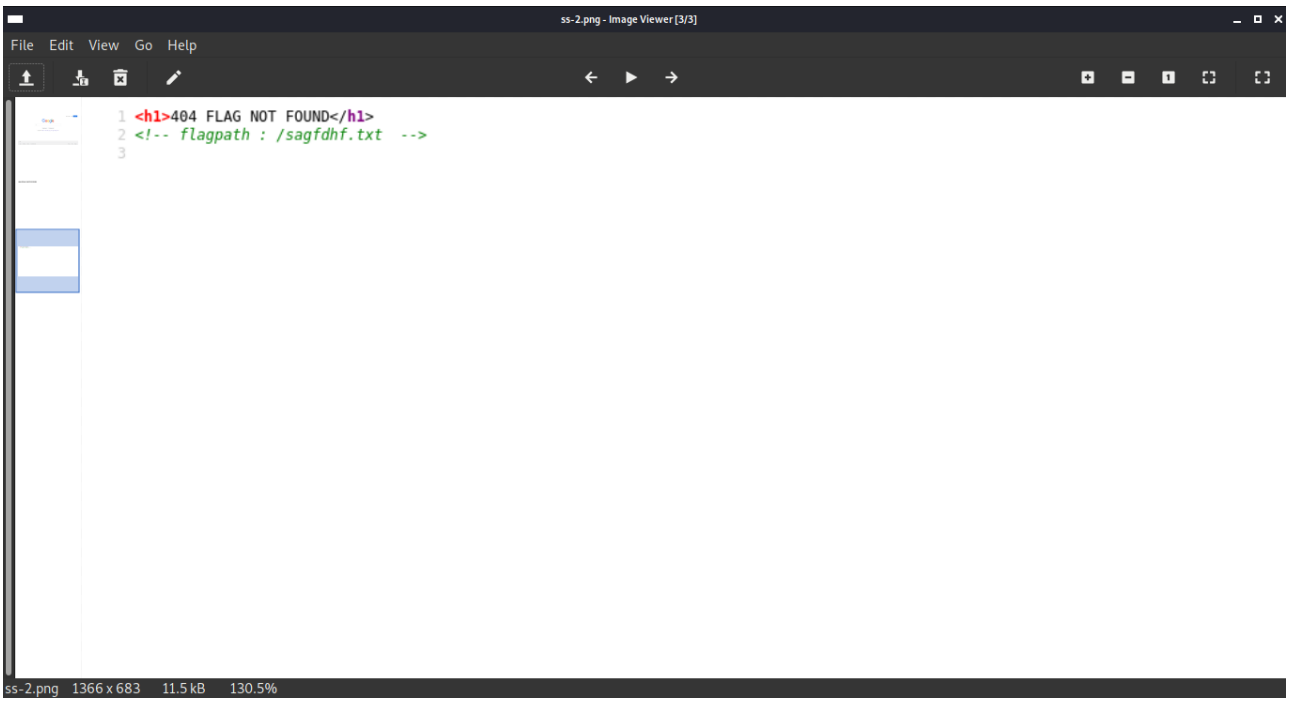
It says 404 Flag not found but we have guessed correct , Usually if we find this in web, we will check its source code to see for any hints
But here how to see the source code ?



We see the source code of the website by adding view-source before the url so lets give a try with

view-source:http://127.0.0.1:5000

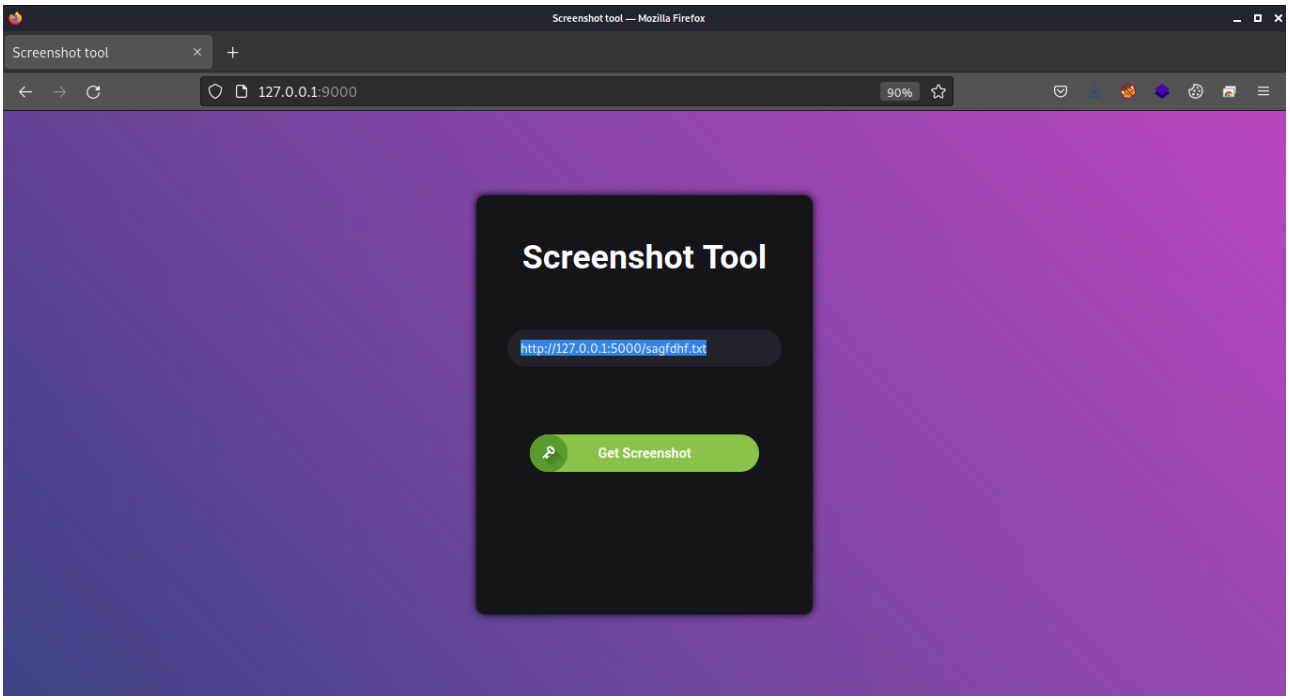


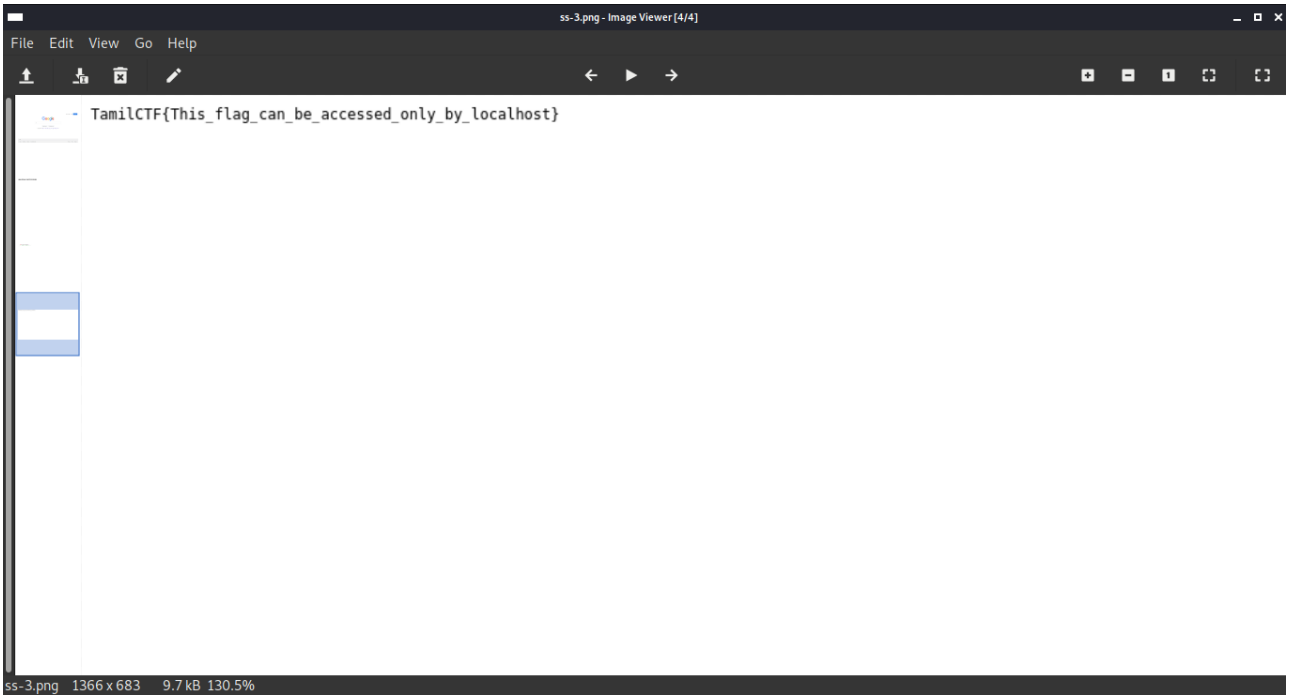


Yeah the path of the flag is in the comments !!

Now we can get the flag easily add the found path on the previous step

http://127.0.0.1:5000/saghdhf.txt





Yeah we got the flag screenshot finally :)