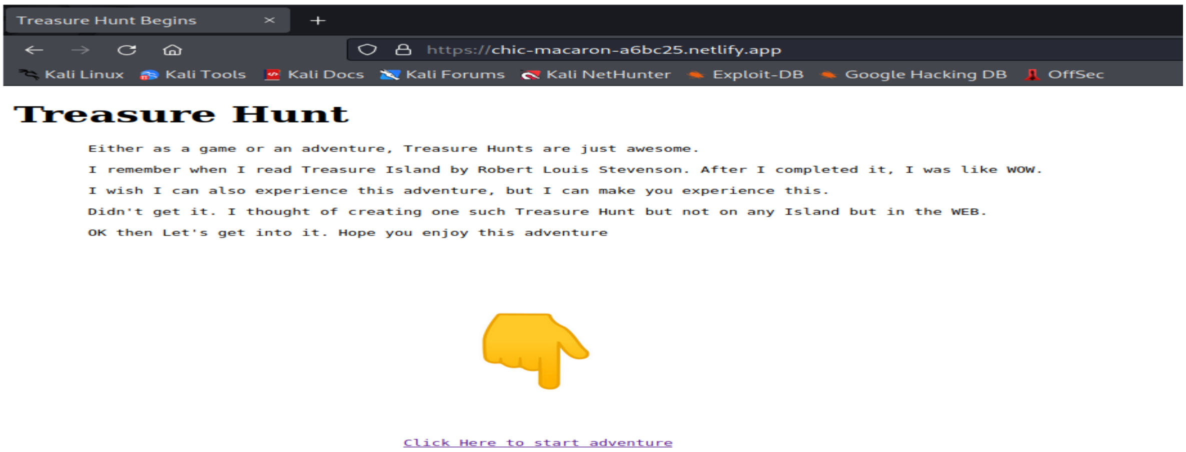
Writeup for the challenge Treasure Hunt

The question starts with a link given as https://chic-macaron-a6bc25.netlify.app/

After clicking the above link, a page opens up which has a text paragraph written about treasure hunt. This page has the link to the next step of the question given as :

<Click Here to start adventure>

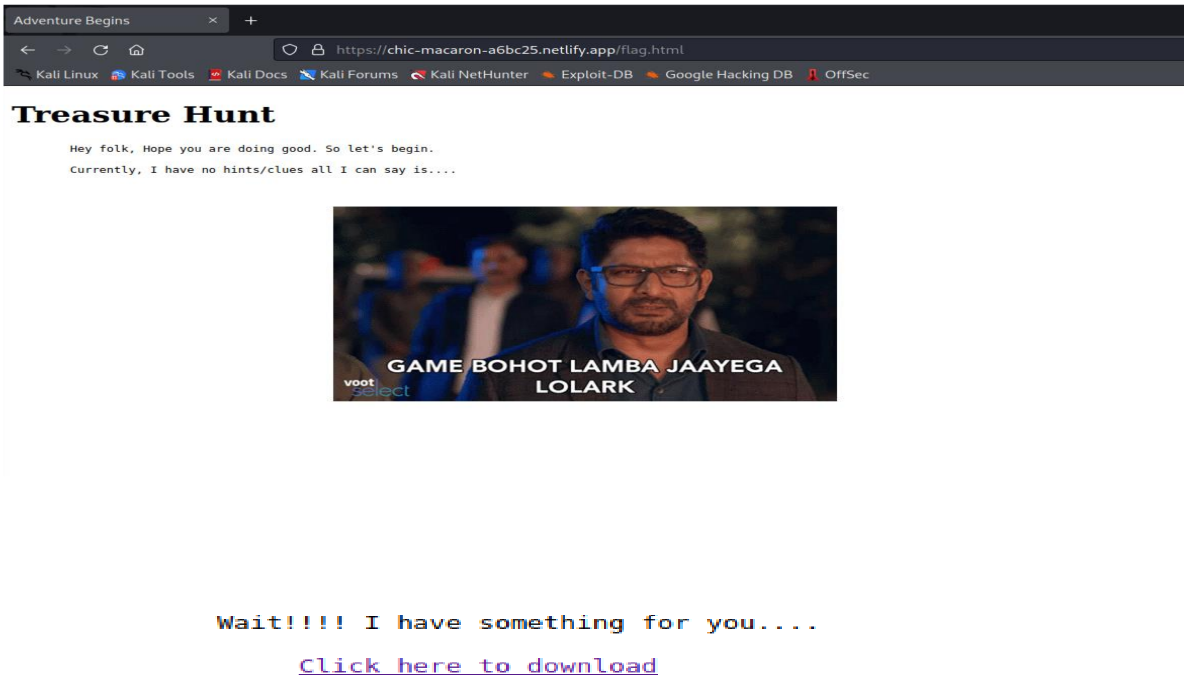


Treasure Hunt

Either as a game or an adventure, Treasure Hunts are just awesome.
I remember when I read Treasure Island by Robert Louis Stevenson. After I completed it, I was like WOW.
I wish I can also experience this adventure, but I can make you experience this.
Didn't get it. I thought of creating one such Treasure Hunt but not on any Island but in the WEB.
OK then Let's get into it. Hope you enjoy this adventure

Click Here to start adventure

After clicking the above link, a new page opens with some message as "I have no hints/clues…." and a gif is shown and also a zip file is given to download.



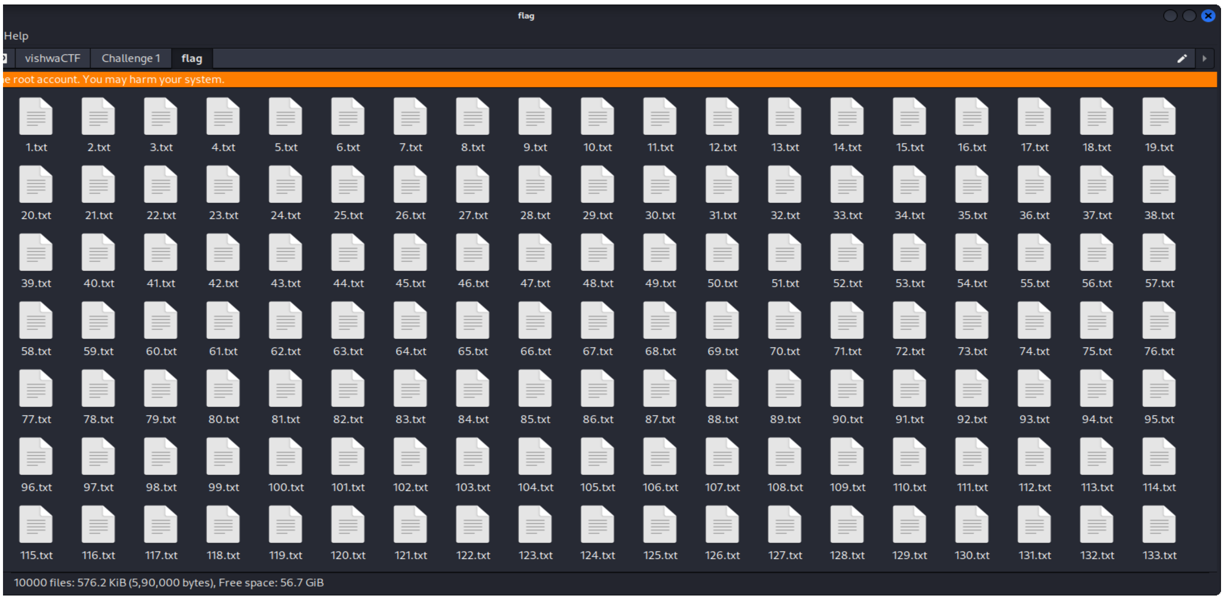
Treasure Hunt

Hey folk, Hope you are doing good. So let's begin.
Currently, I have no hints/clues all I can say is....

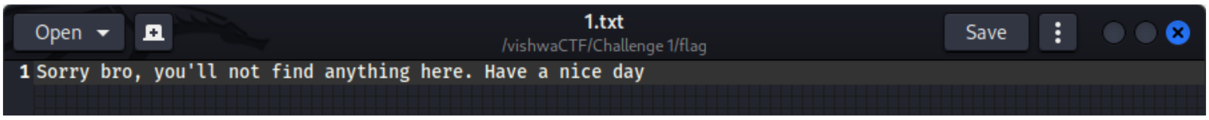
Wait!!!! I have something for you....

Click here to download

After extracting the zip file, a folder appears which consists of 10000 text file all of with same size and message as “Sorry bro, you’ll not find anything here. Have a nice day”


flag
Help
vishwaCTF
Challenge 1
flag
e root account. You may harm your system.
1.txt 2.txt 3.txt 4.txt 5.txt 6.txt 7.txt 8.txt 9.txt 10.txt 11.txt 12.txt 13.txt 14.txt 15.txt 16.txt 17.txt 18.txt 19.txt
20.txt 21.txt 22.txt 23.txt 24.txt 25.txt 26.txt 27.txt 28.txt 29.txt 30.txt 31.txt 32.txt 33.txt 34.txt 35.txt 36.txt 37.txt 38.txt
39.txt 40.txt 41.txt 42.txt 43.txt 44.txt 45.txt 46.txt 47.txt 48.txt 49.txt 50.txt 51.txt 52.txt 53.txt 54.txt 55.txt 56.txt 57.txt
58.txt 59.txt 60.txt 61.txt 62.txt 63.txt 64.txt 65.txt 66.txt 67.txt 68.txt 69.txt 70.txt 71.txt 72.txt 73.txt 74.txt 75.txt 76.txt
77.txt 78.txt 79.txt 80.txt 81.txt 82.txt 83.txt 84.txt 85.txt 86.txt 87.txt 88.txt 89.txt 90.txt 91.txt 92.txt 93.txt 94.txt 95.txt
96.txt 97.txt 98.txt 99.txt 100.txt 101.txt 102.txt 103.txt 104.txt 105.txt 106.txt 107.txt 108.txt 109.txt 110.txt 111.txt 112.txt 113.txt 114.txt
115.txt 116.txt 117.txt 118.txt 119.txt 120.txt 121.txt 122.txt 123.txt 124.txt 125.txt 126.txt 127.txt 128.txt 129.txt 130.txt 131.txt 132.txt 133.txt

10000 files: 576.2 KiB (5,90,000 bytes), Free space: 56.7 GiB

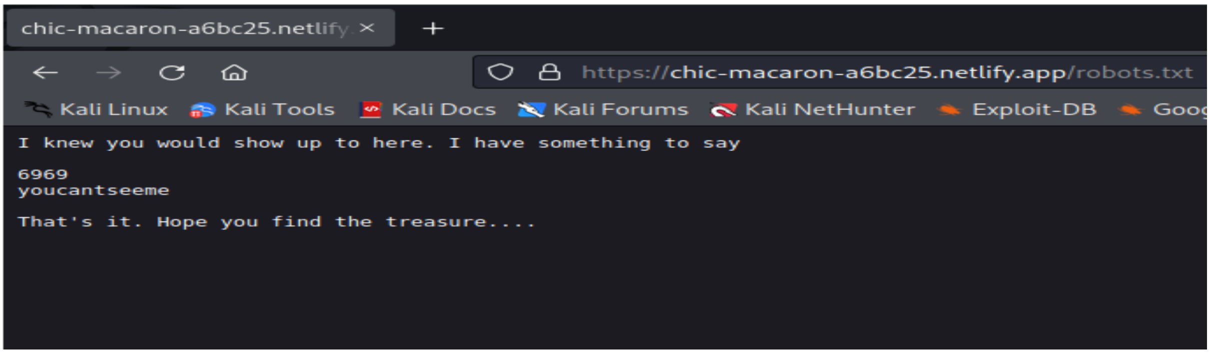


```
Sorry bro, you'll not find anything here. Have a nice day
```

Moving back to the website, in the /robots.txt file there are two hints given as:

1. 6969

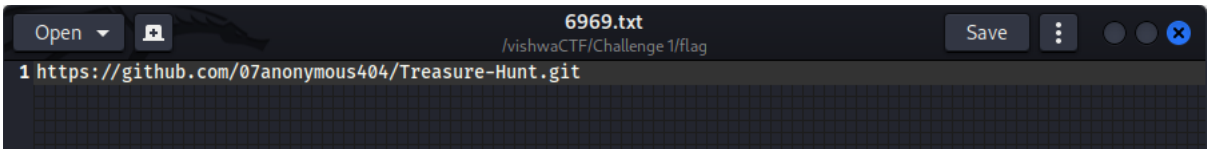
2. youcantseeme


chic-macaron-a6bc25.netlify
https://chic-macaron-a6bc25.netlify.app/robots.txt
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Goog

```
I knew you would show up to here. I have something to say

6969
youcantseeme

That's it. Hope you find the treasure....
```

As we had 10000 text files in the zip file, opening the file 6969.txt gives the hint for the next step. There is a github link gives which is as follows:

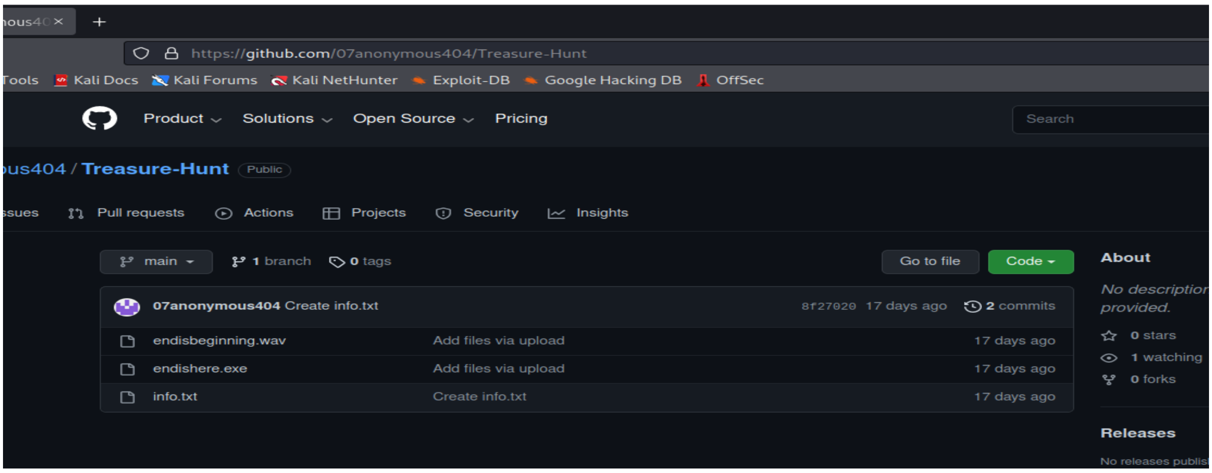
https://github.com/07anonymous404/Treasure-Hunt.git/



```
https://github.com/07anonymous404/Treasure-Hunt.git
```

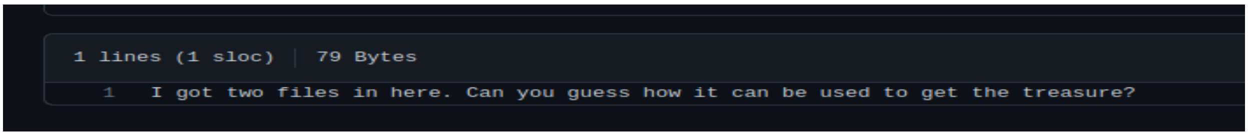
which contains three files namely,

endisbeginning.wav, endishere.exe and info.txt.


https://github.com/07anonymous404/Treasure-Hunt
Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec
Product | Solutions | Open Source | Pricing | Search
ous404 / Treasure-Hunt Public
ssues | Pull requests | Actions | Projects | Security | Insights
main | 1 branch | 0 tags | Go to file | Code
About
No description provided.
0 stars
1 watching
0 forks
Releases
No releases publis

```
07anonymous404 Create info.txt                          8f27020  17 days ago   2 commits
endisbeginning.wav      Add files via upload                                  17 days ago
endishere.exe           Add files via upload                                  17 days ago
info.txt                Create info.txt                                       17 days ago
```

After opening the info.txt file we can see a hint given as "I got two files in here. Can you guess how it can be used to get the treasure?"



```
1 lines (1 sloc)  |  79 Bytes
  1   I got two files in here. Can you guess how it can be used to get the treasure?
```

From above hint we can assume that the flag might be in any of the two given files.

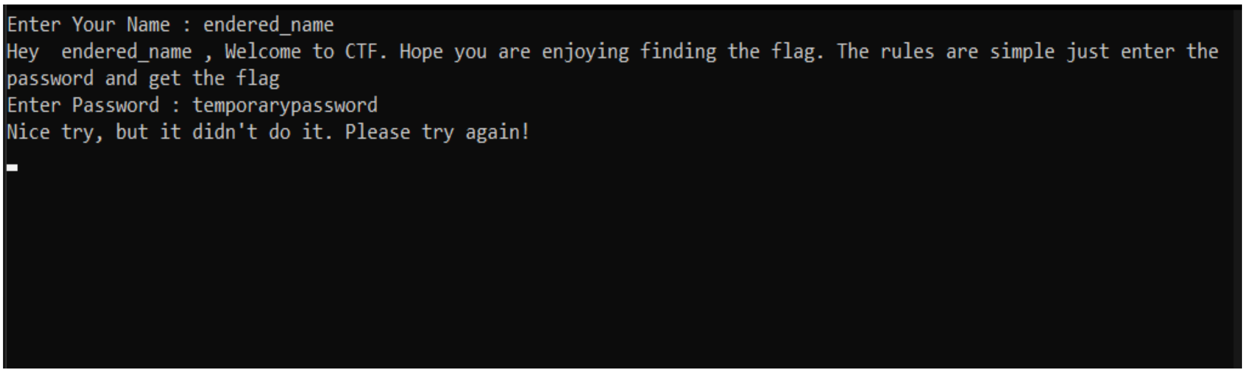
Starting from the endishere.exe file, since it is an executable file it can be run only in the windows operating system and not in any other. After running it, it asks for our name after entering our name it displays some message as :

"Hey entered_name, Welcome to CTF. Hope you are enjoying finding the flag. The rules are simple just enter the password and get the flag"

and it asks for the password.

For an incorrect input of the password, it gives a message as :

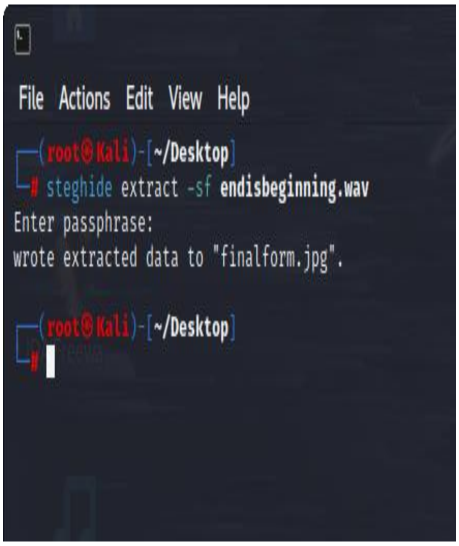
"Nice try, but it didn't do it. Please try again!" and stops after 10 sec.



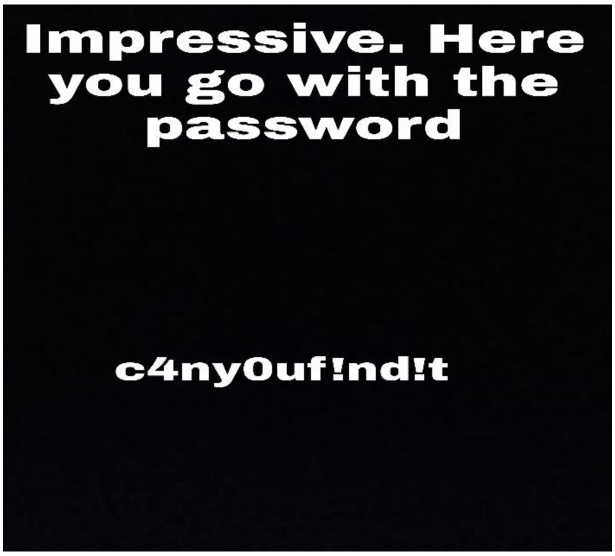
```
Enter Your Name : endered_name
Hey  endered_name , Welcome to CTF. Hope you are enjoying finding the flag. The rules are simple just enter the
password and get the flag
Enter Password : temporarypassword
Nice try, but it didn't do it. Please try again!
```

We can assume the password for the endishere.exe file maybe hidden in the endisbeginning.wav file.

So looking for some steganographic tools in Kali Linux, we can find few like exiftool, steghide, etc. Trying to extract the password from the endisbeginning.wav file using steghide, a passphrase is required to extract which can be found in the robots.txt from the website. Entering the passphrase as “youcantseeme”, a jpg file with password gets extracted which is “c4ny0uf!nd!t”.



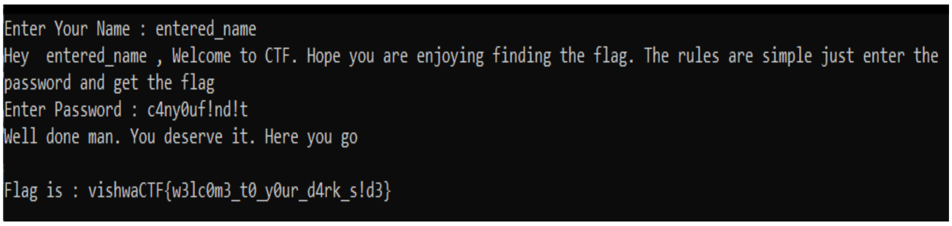
```
┌──(root㉿Kali)-[~/Desktop]
└─# steghide extract -sf endisbeginning.wav
Enter passphrase:
wrote extracted data to "finalform.jpg".

┌──(root㉿Kali)-[~/Desktop]
└─# 
```



Impressive. Here you go with the password

c4ny0uf!nd!t

Entering this password in the endishere.exe file, it gives us the flag which is



```
Enter Your Name : entered_name
Hey  entered_name , Welcome to CTF. Hope you are enjoying finding the flag. The rules are simple just enter the
password and get the flag
Enter Password : c4ny0uf!nd!t
Well done man. You deserve it. Here you go

Flag is : vishwaCTF{w3lc0m3_t0_y0ur_d4rk_s!d3}
```

Flag : vishwaCTF{w3lc0m3_t0_y0ur_d4rk_s!d3}