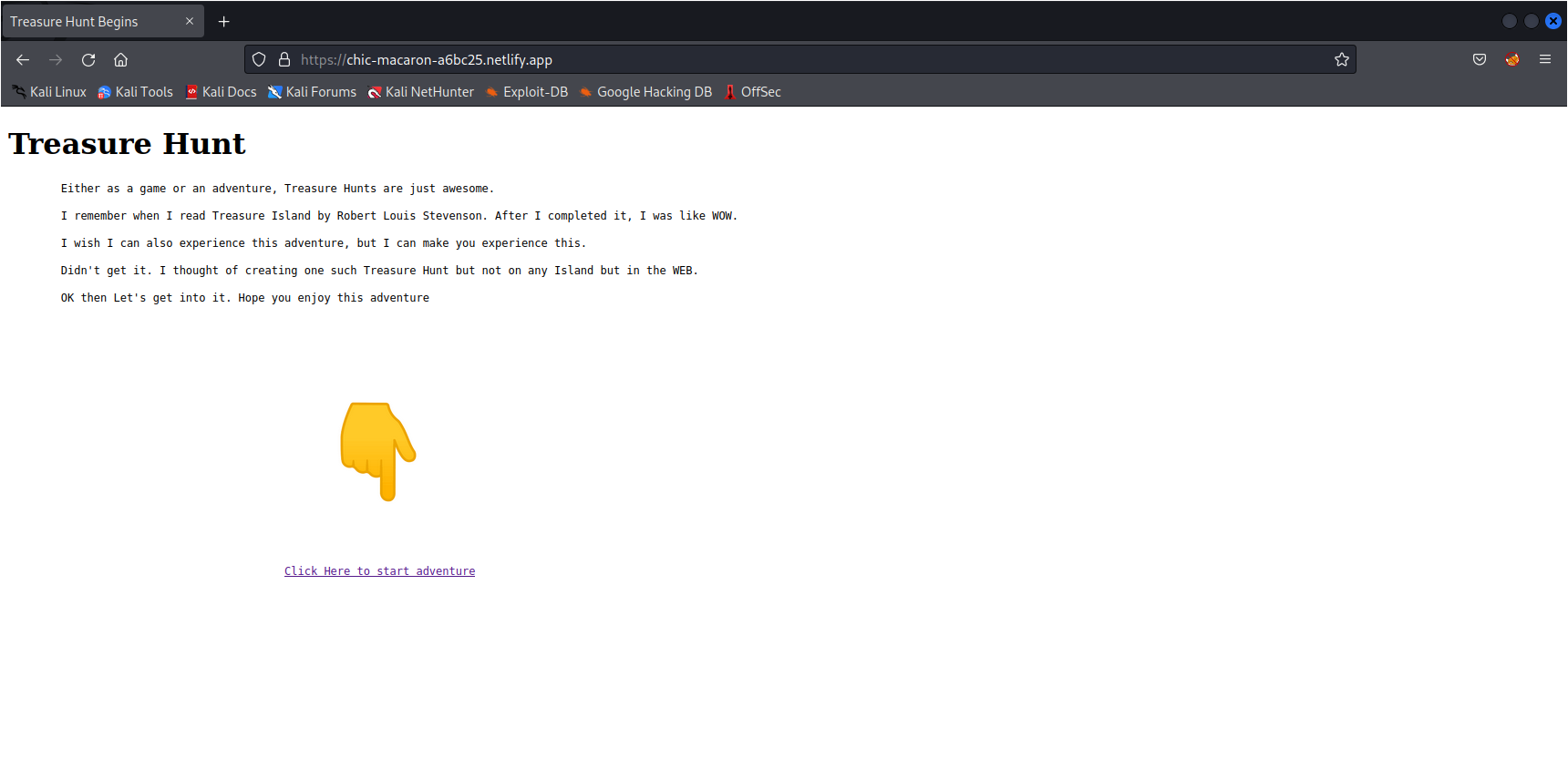
Writeup for the challenge Treasure Hunt

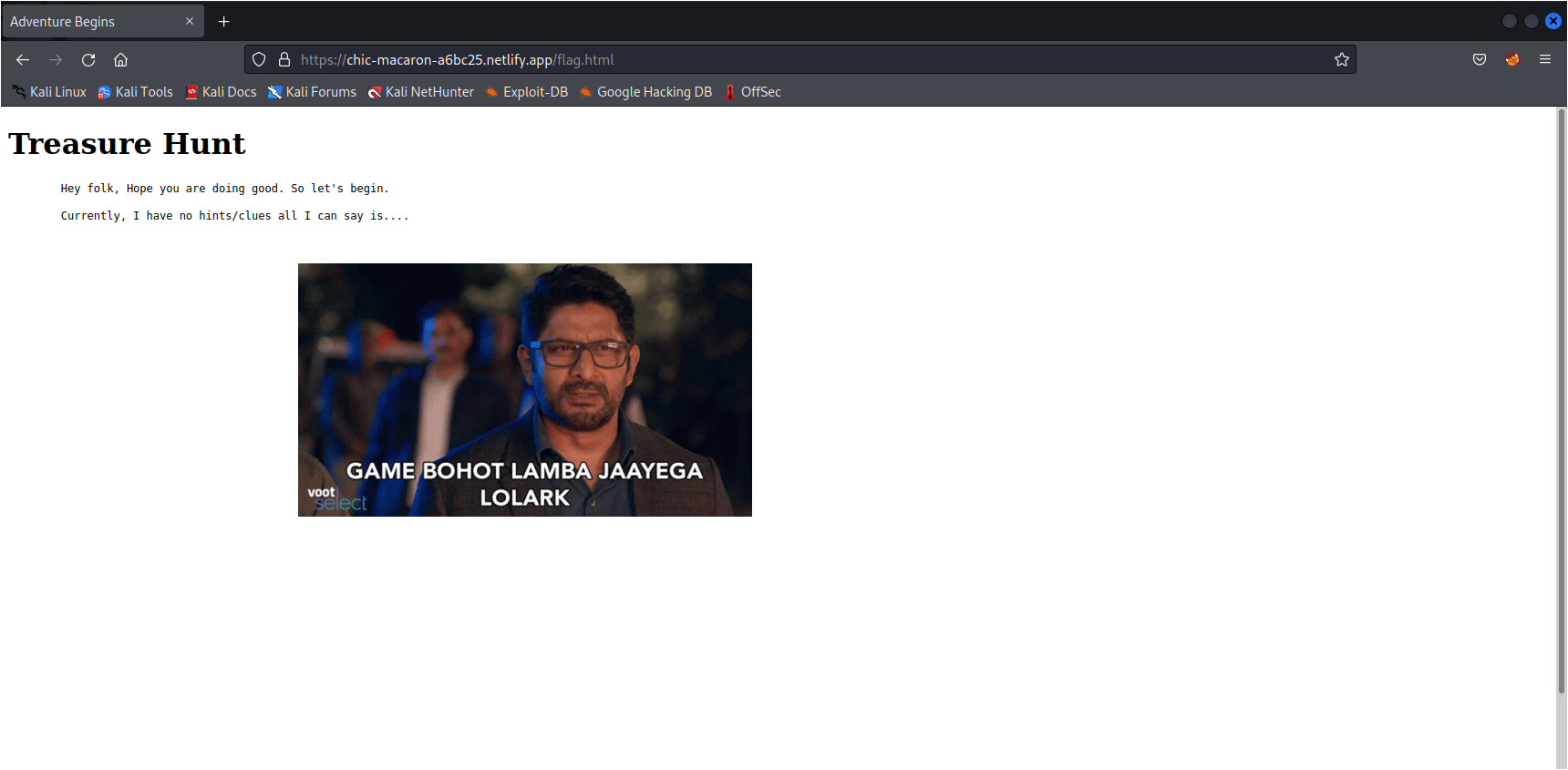
The question starts with a link given as <https://chic-macaron-a6bc25.netlify.app/>

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>



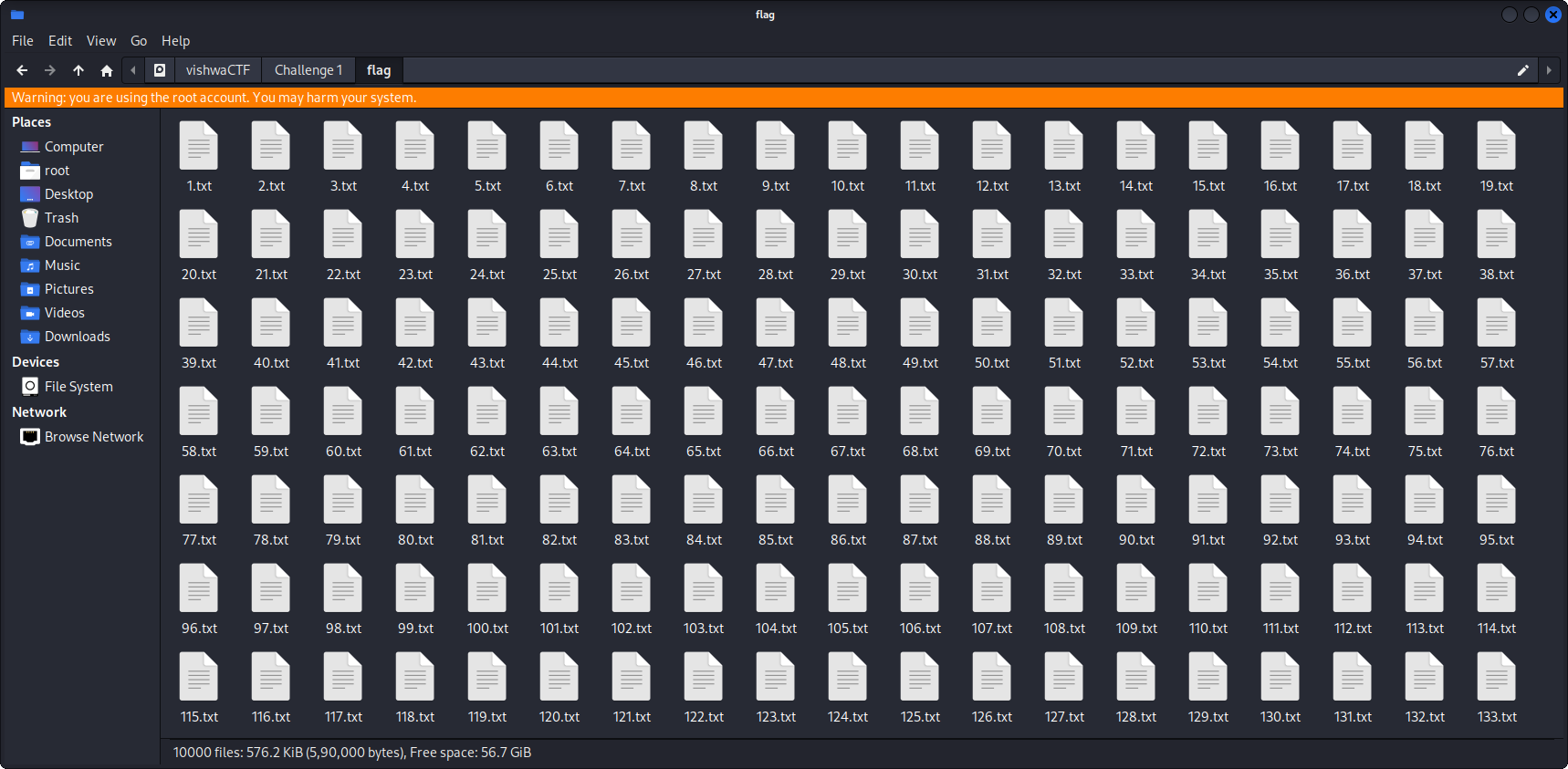
After clicking the above link, a new page opens with some message as “I have no hints/clues….” and a gif is shown and also a zip file is given to download.

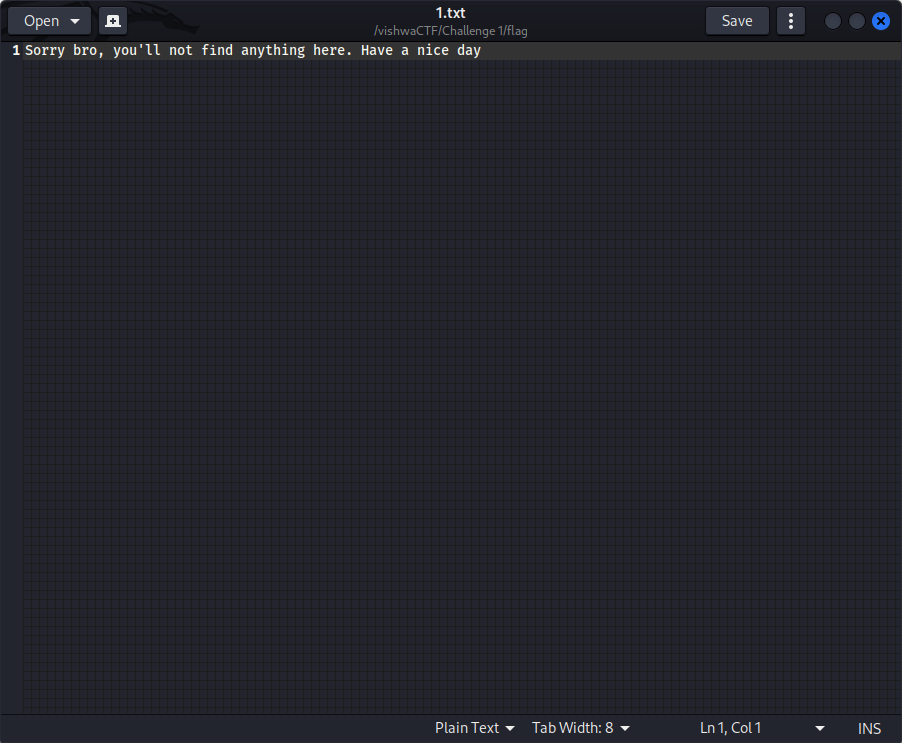


Graphical user interface, website

Description automatically generated

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”

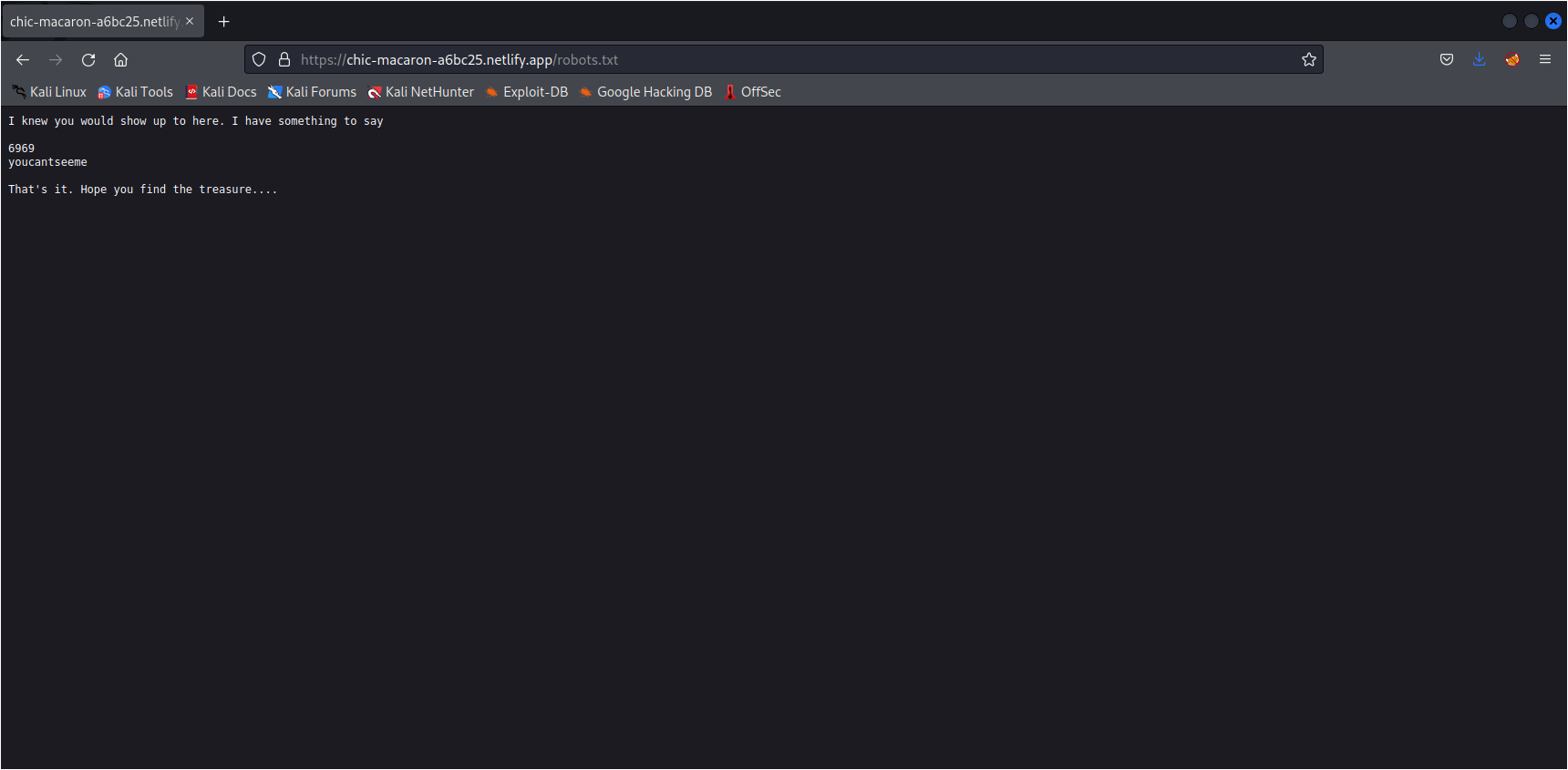




Moving back to the website, in the /robots.txt file there are two hints given as:

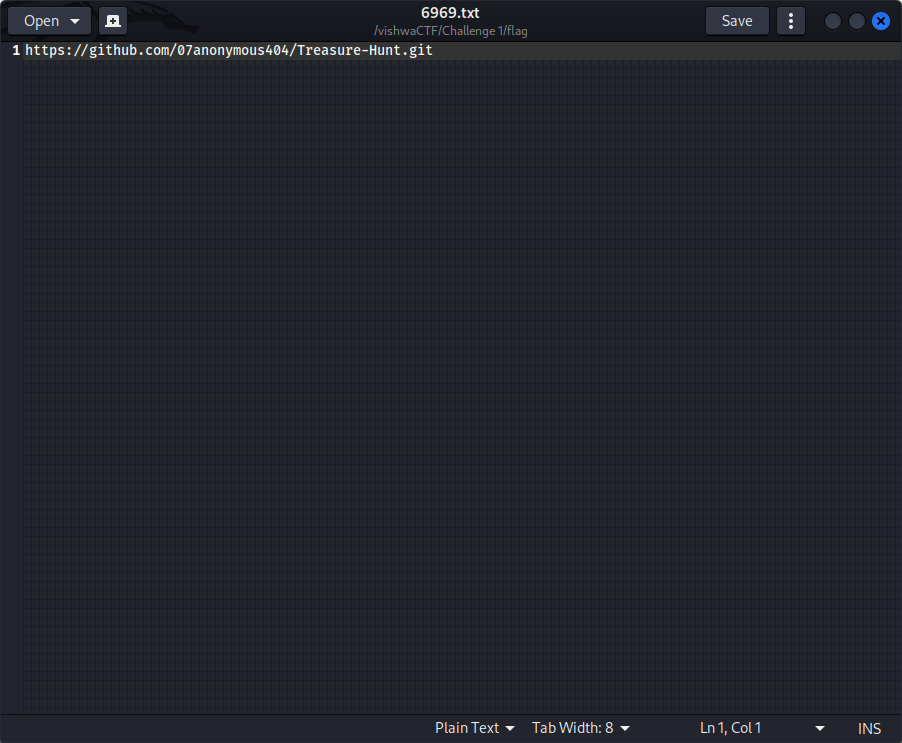
1. 6969

2. youcantseeme



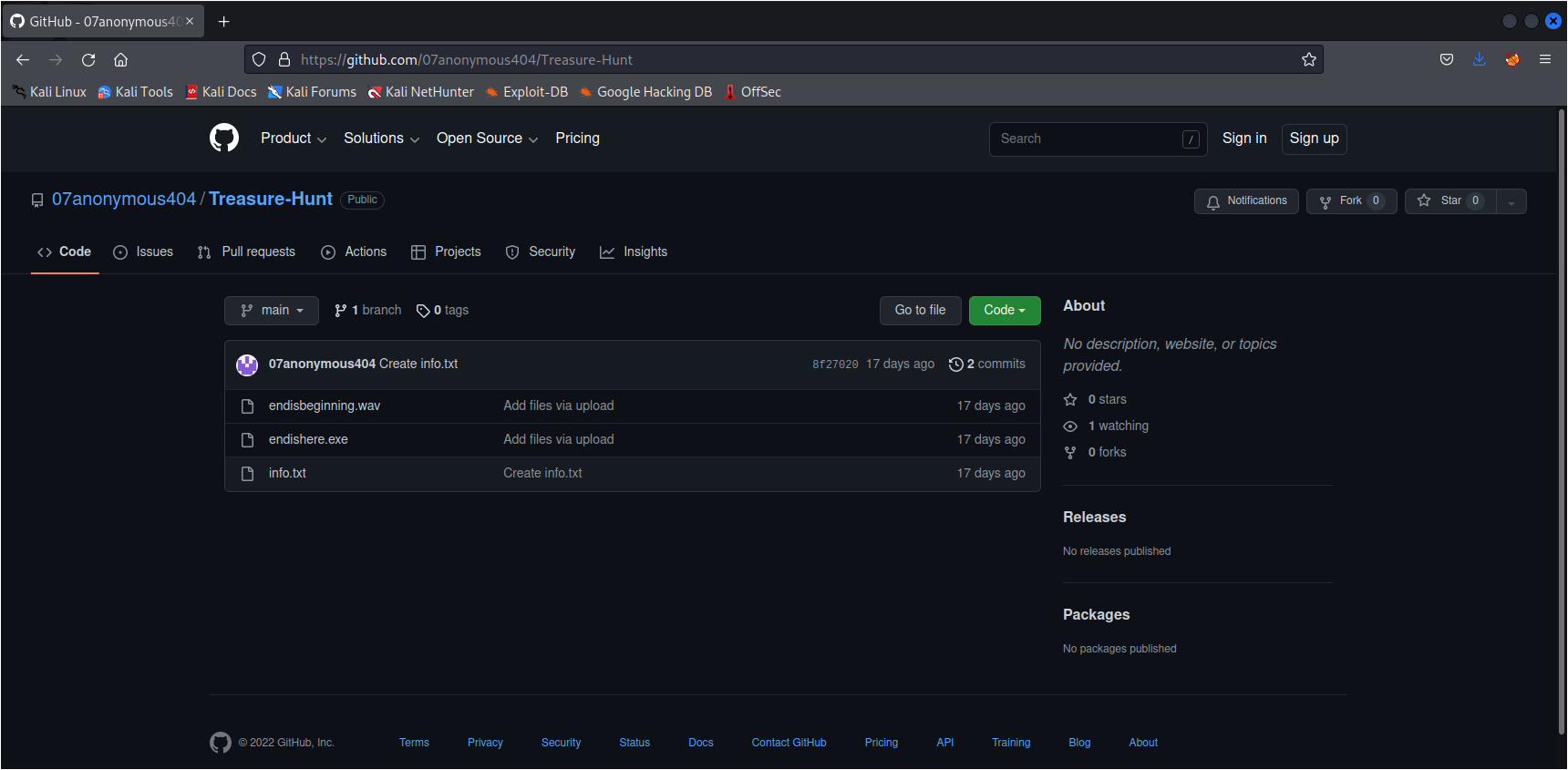
As we had 10000 text files in the zip file, opening the file 6969.txt gives the hint for the next step. There is a github link gives which is as follows:

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

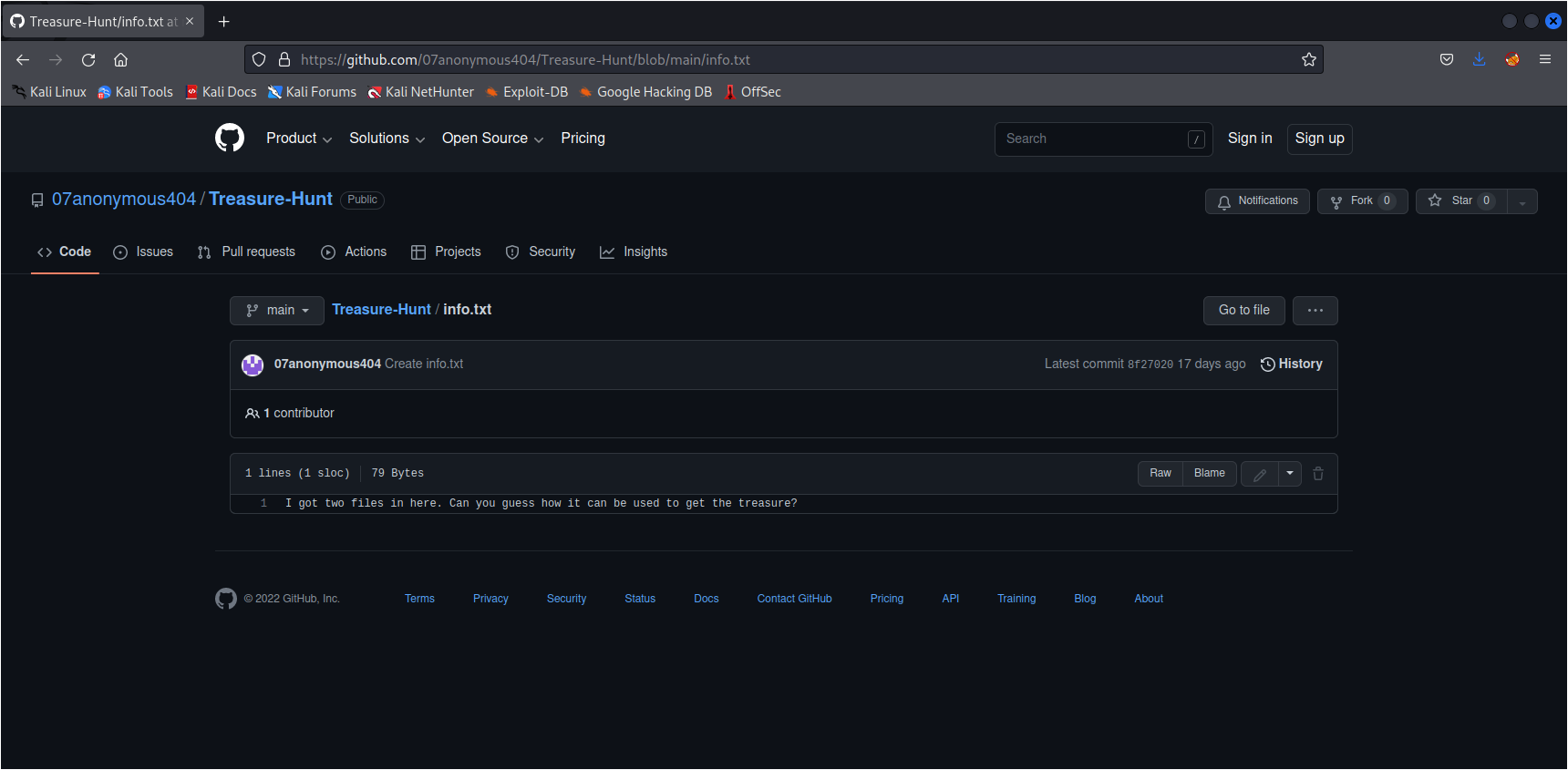


which contains three files namely,

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



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?”



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

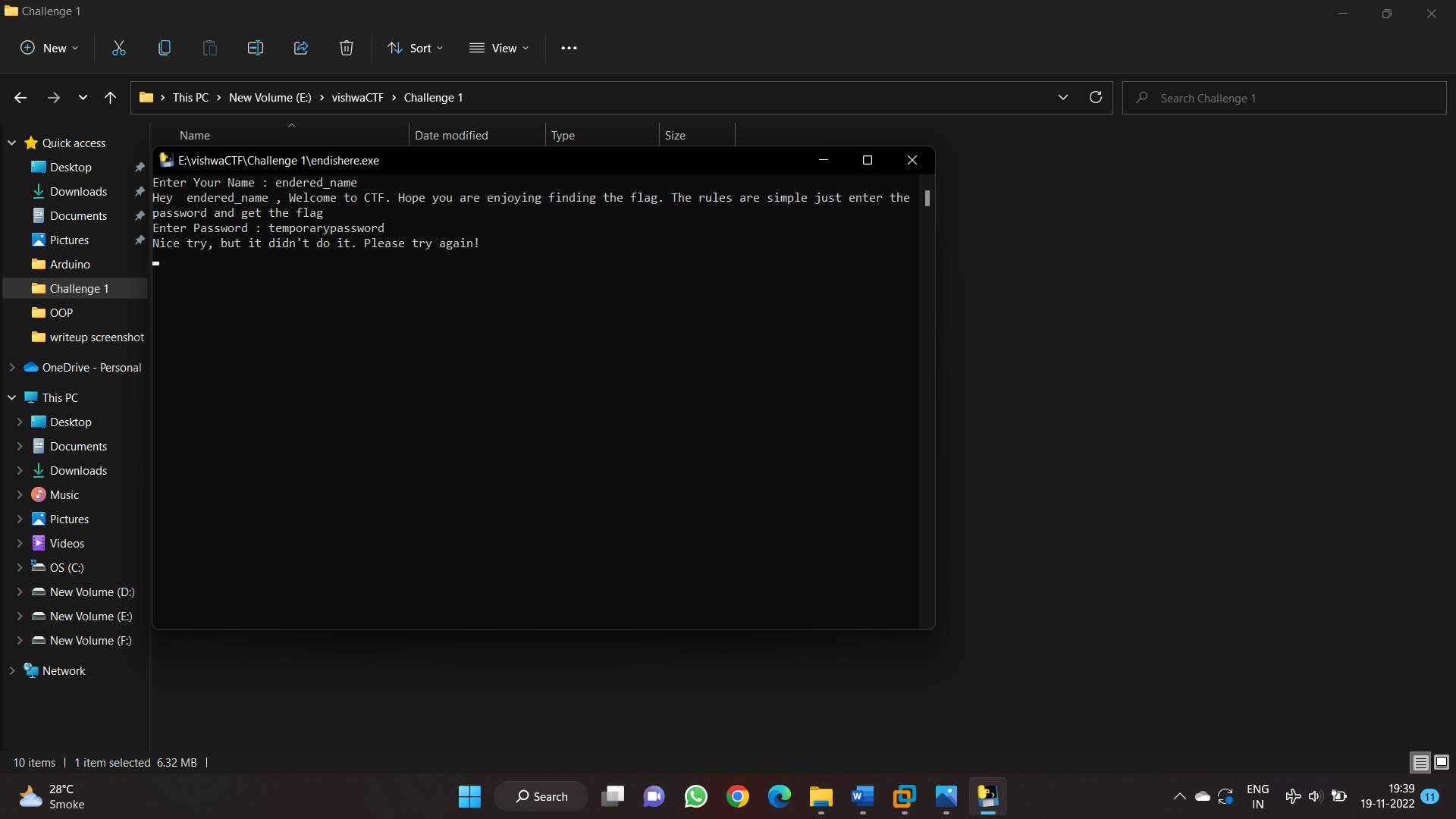
Starting from the endishere.exe file, since it is an executable file it can be run only in the windows operating system and not in any other. After running it, it asks for our name after entering our name it displays some message as :

“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.

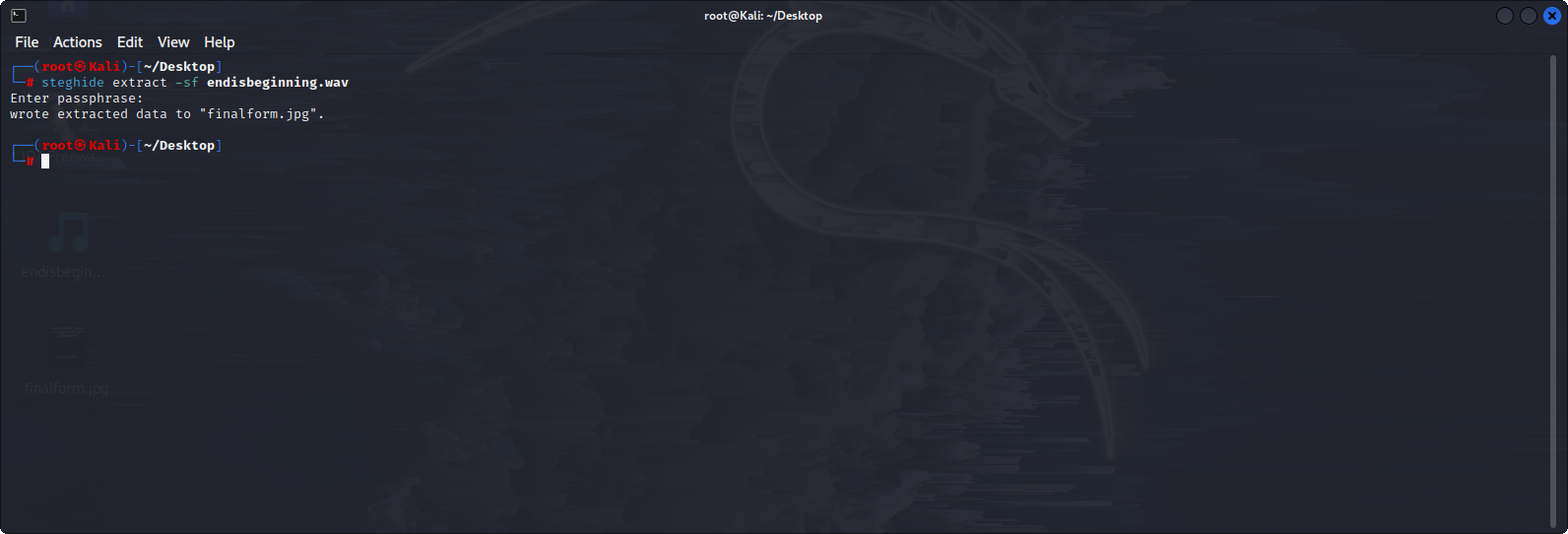
For an incorrect input of the password, it gives a message as :

“Nice try, but it didn’t do it. Please try again!” and stops after 10 sec.



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

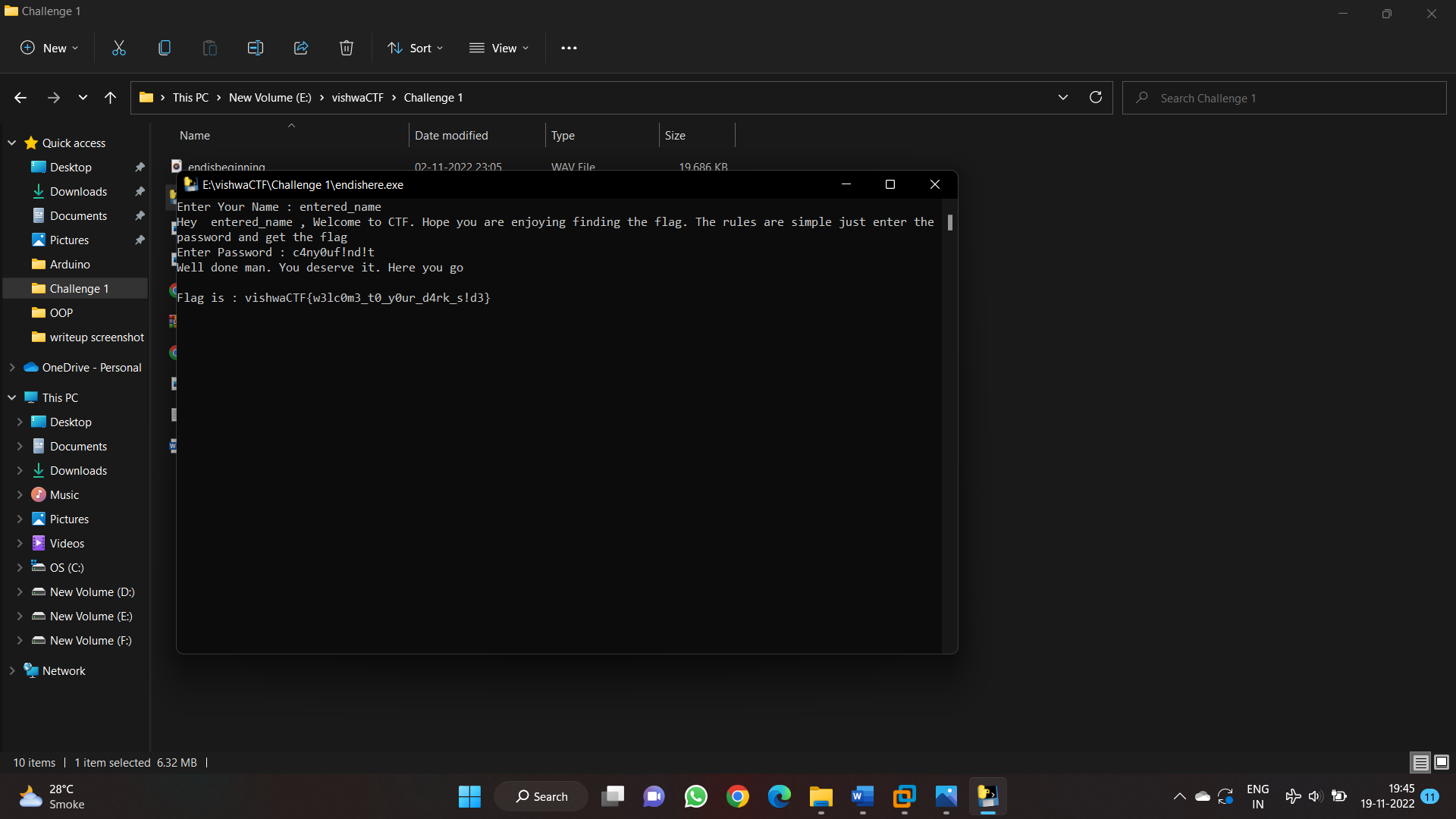
So looking for some steganographic tools in Kali Linux, we can find few like exiftool, steghide, etc. Trying to extract the password from the endisbeginning.wav file using steghide, a passphrase is required to extract which can be found in the robots.txt from the website. Entering the passphrase as “youcantseeme”,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



Text

Description automatically generated

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



Flag : vishwaCTF{w3lc0m3\_t0\_y0ur\_d4rk\_s!d3}