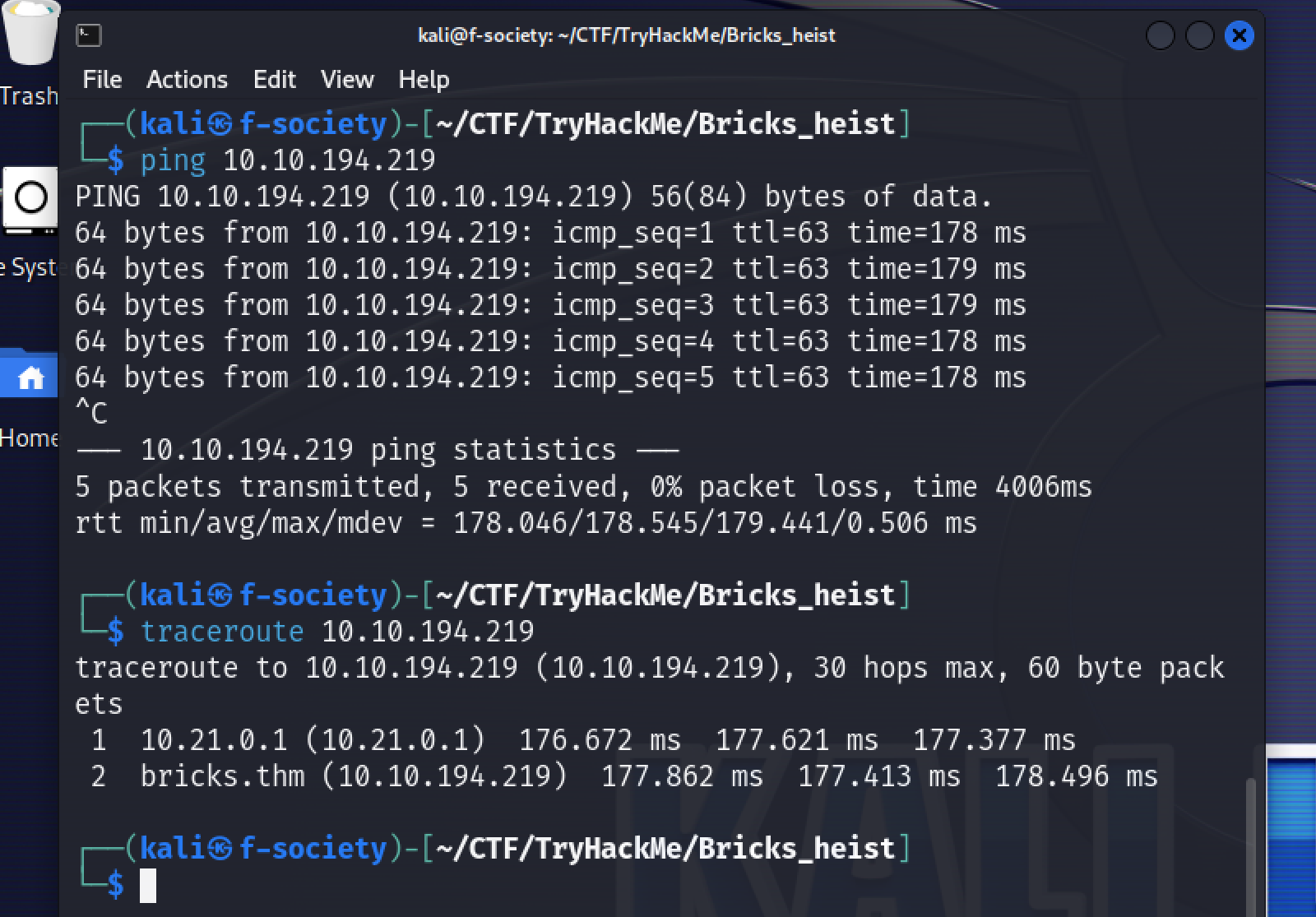
**BRICKS HEIST TRYHACKME**

To hack this machine, we do the following:

1. As always, first we connect our vpn
2. Next, we check if our machine is online by pinging



1. Before we start our enumeration, we are told to add the target ip to our **/etc/hosts** file. So, navigate to the file and add the ip:

* sudo mousepad /etc/hosts

A screenshot of a computer

Description automatically generated

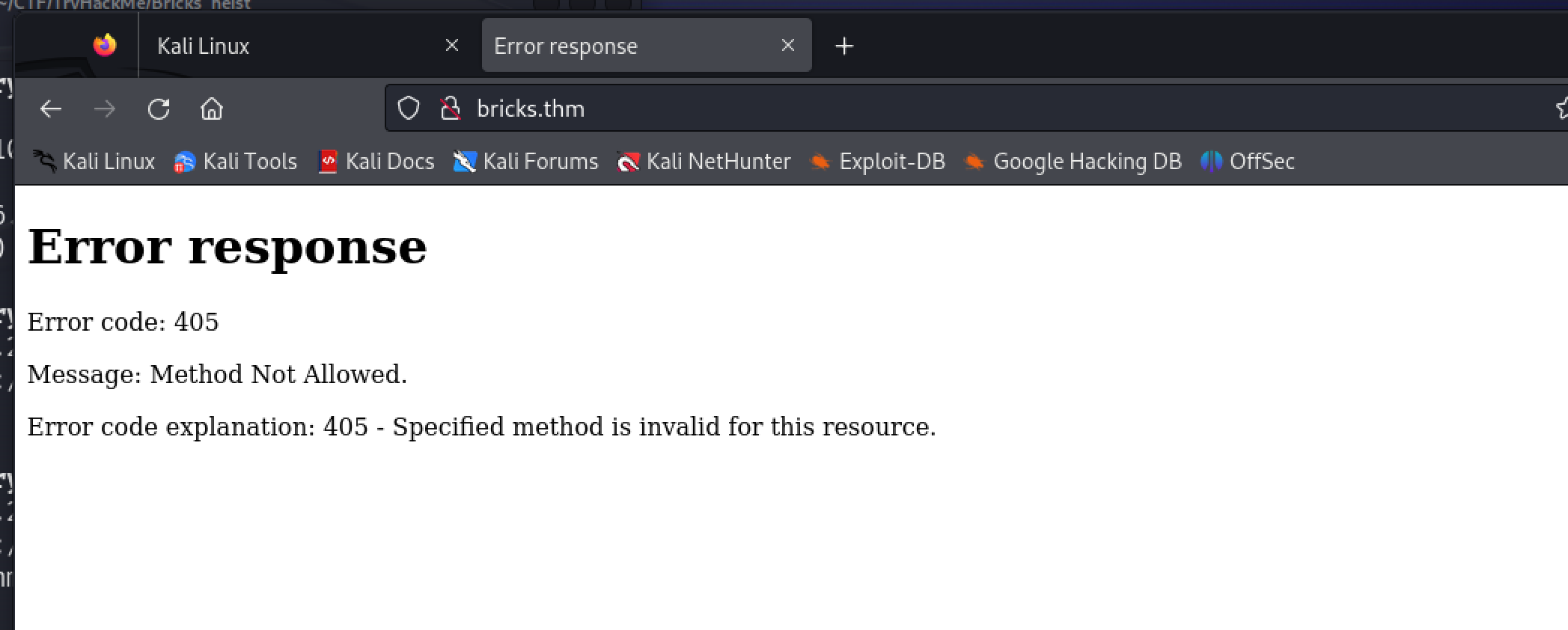
1. Now let’s scan our target ip using nmap and find the open ports.

* nmap -F -Pn -sV {target\_ip} -o {file\_name}
* -F = fast mode
* -Pn = no ping

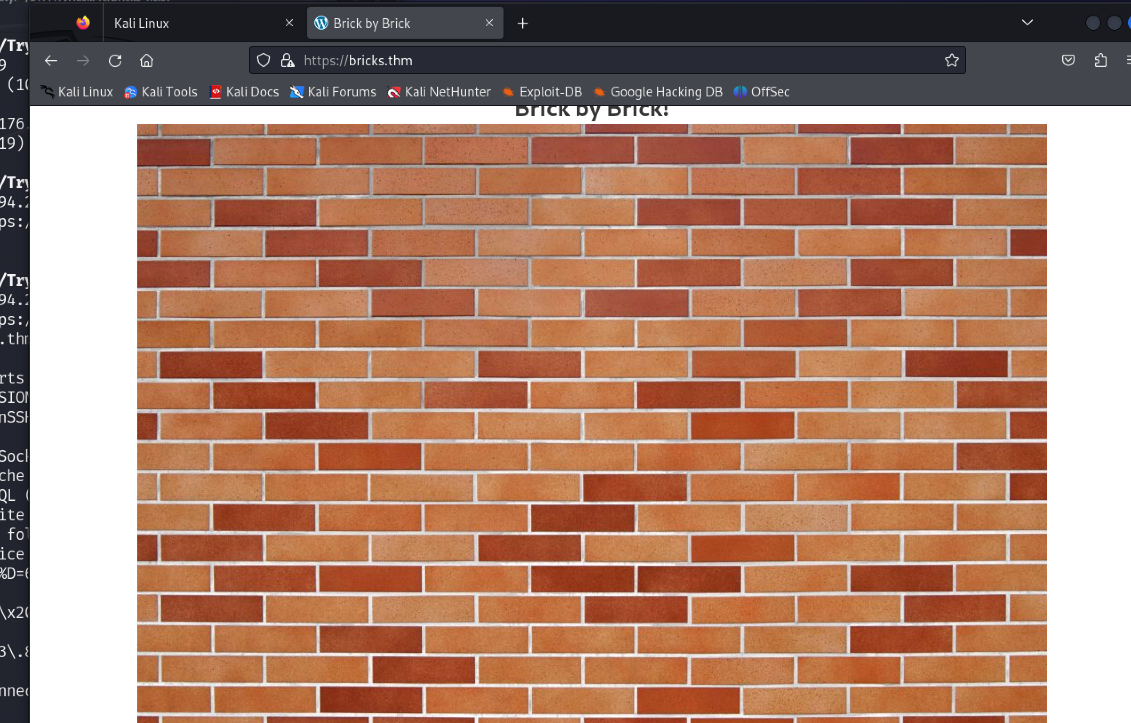
A computer screen shot of a computer program

Description automatically generated

1. Since we found that http and https are open, let’s check the website on our browser. But unfortunately, http is is displaying 405 error (method not allowed).



* So, we use https to access the website and it works.



1. Now let’s view the source page of the website by right clicking and opening source page and we find that the website is made using wordpress.

A computer screen shot of text

Description automatically generated

1. So, let’s run our gobuster to check for subdomains if there are any.

* gobuster dir -u <https://bricks.thm> -w /usr/share/dirb/wordlists/common.txt

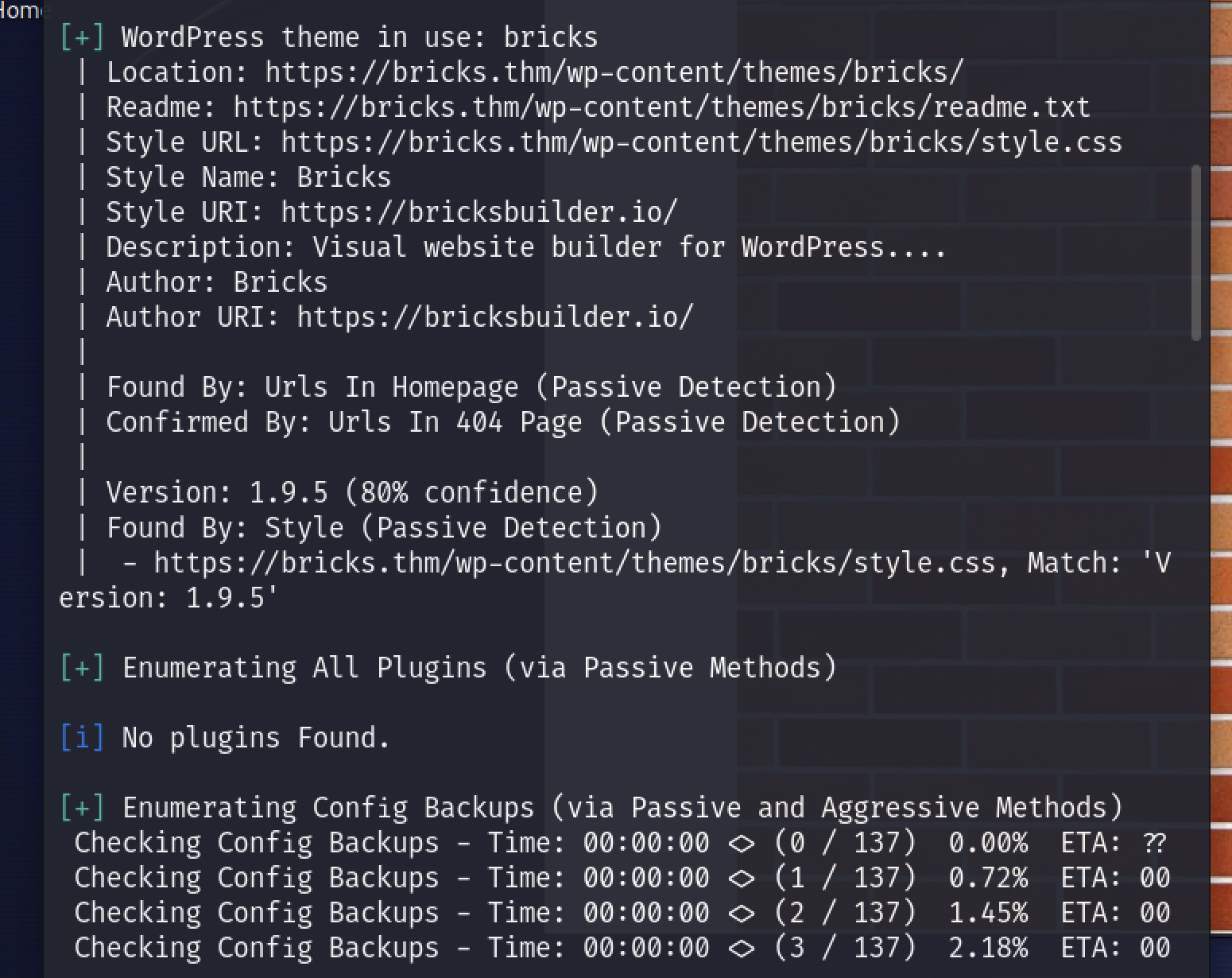
A screen shot of a computer

Description automatically generated

* Even though we found some subdomains, there is nothing there it is a dead end.

1. Now let’s use a tool called **wpscan** which is used to scan for vulnerabilities in wordpress sites and it is built-in in kali.

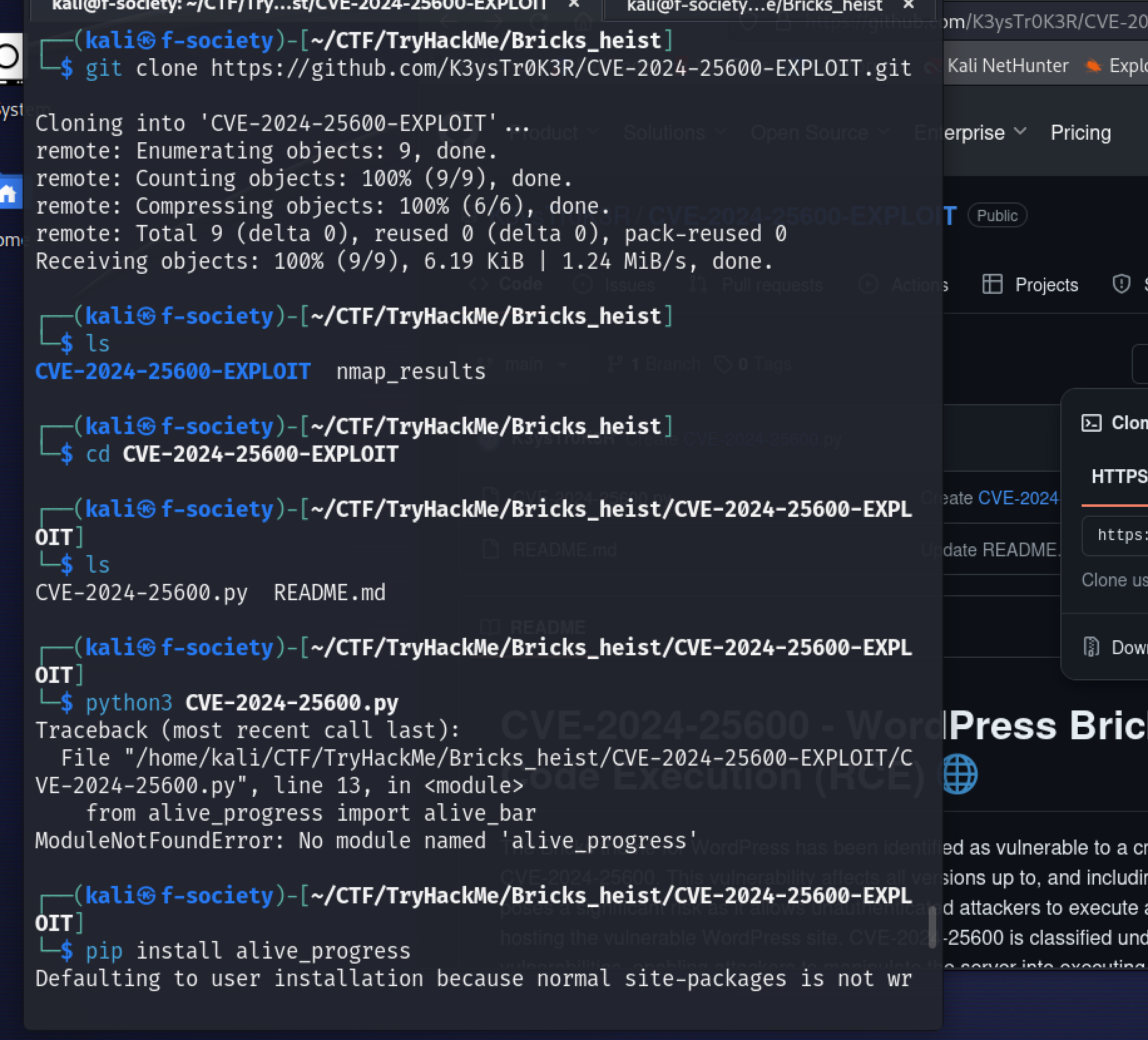
* wpscan - - url <https://bricks.thm>



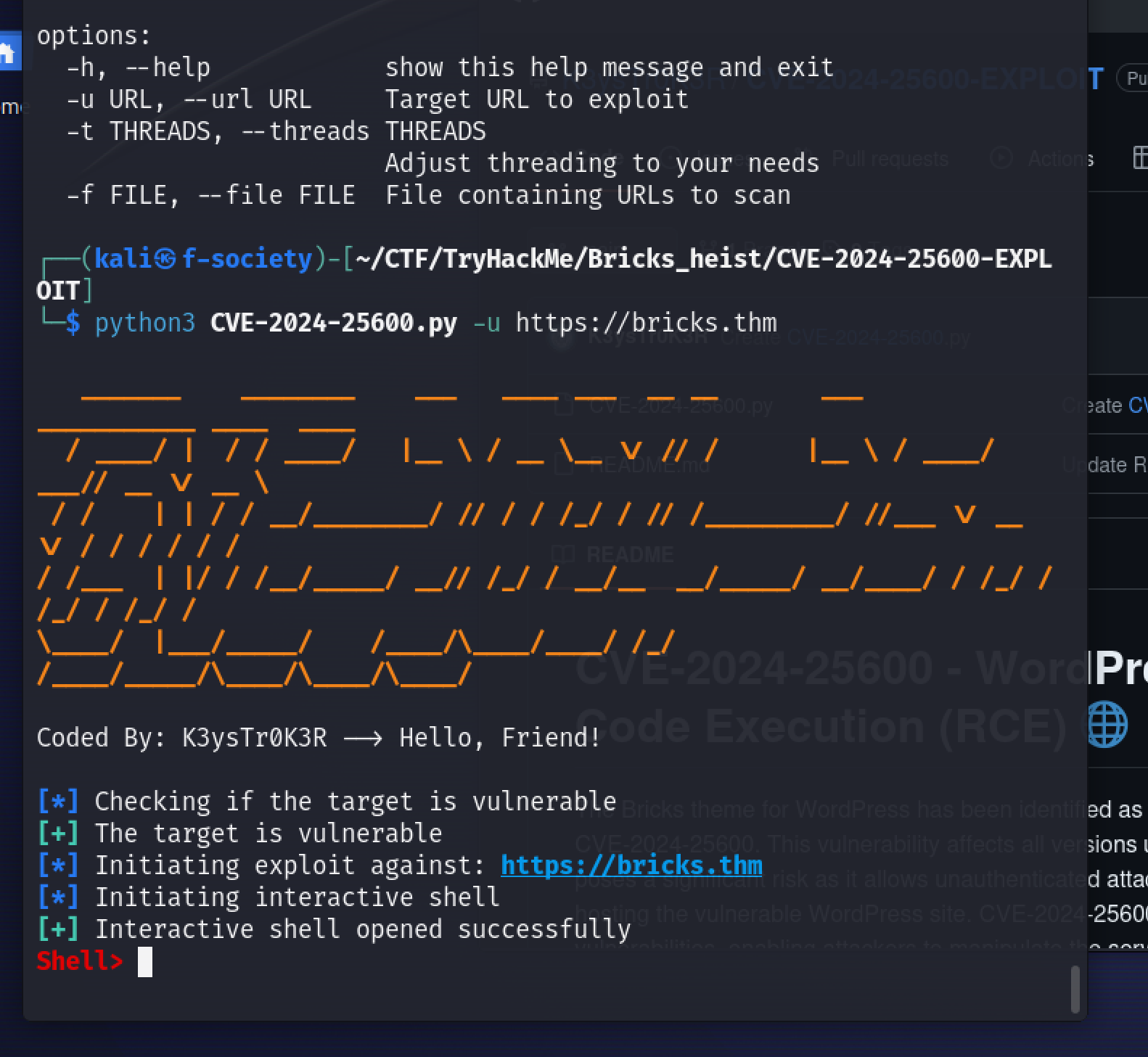
* Here we find some juicy informations and one of them is the version of the wordpress.
* Version: 1.9.5

1. Now we go to our friend “google” and search for an exploit if there is any for wordpress version 1.9.5.
2. We found an exploit with the name **CVE-2024-25600** on github and it is a python script to get access to the shell. So, let’s clone it:

* git clone {github\_link}



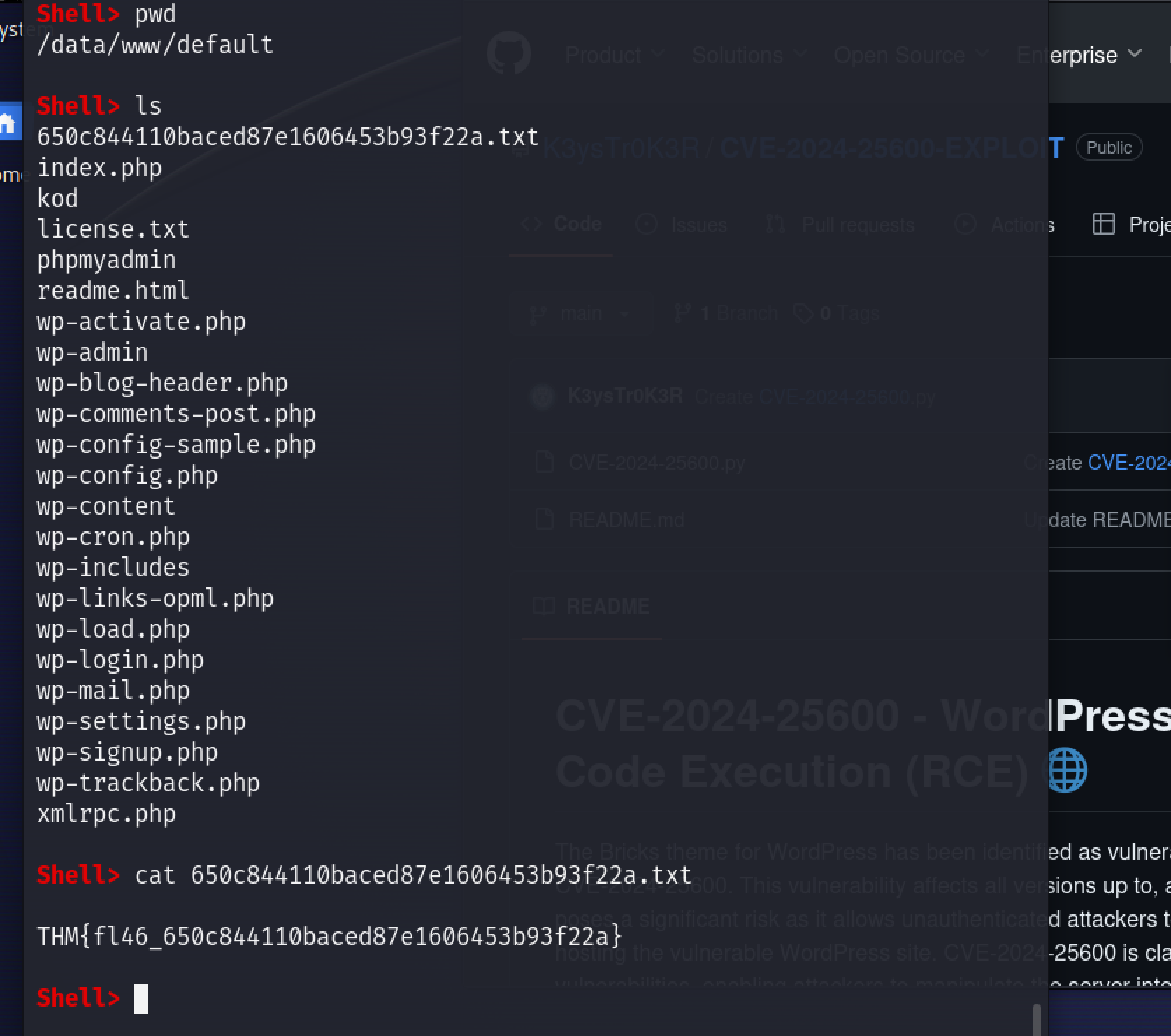
* Now after cloning the python script let’s run our script to get access.
* -u = url of target



* **BOOM SHAKALAKA** we got access.

1. Now on our shell let’s try to see the file by using file listing command.

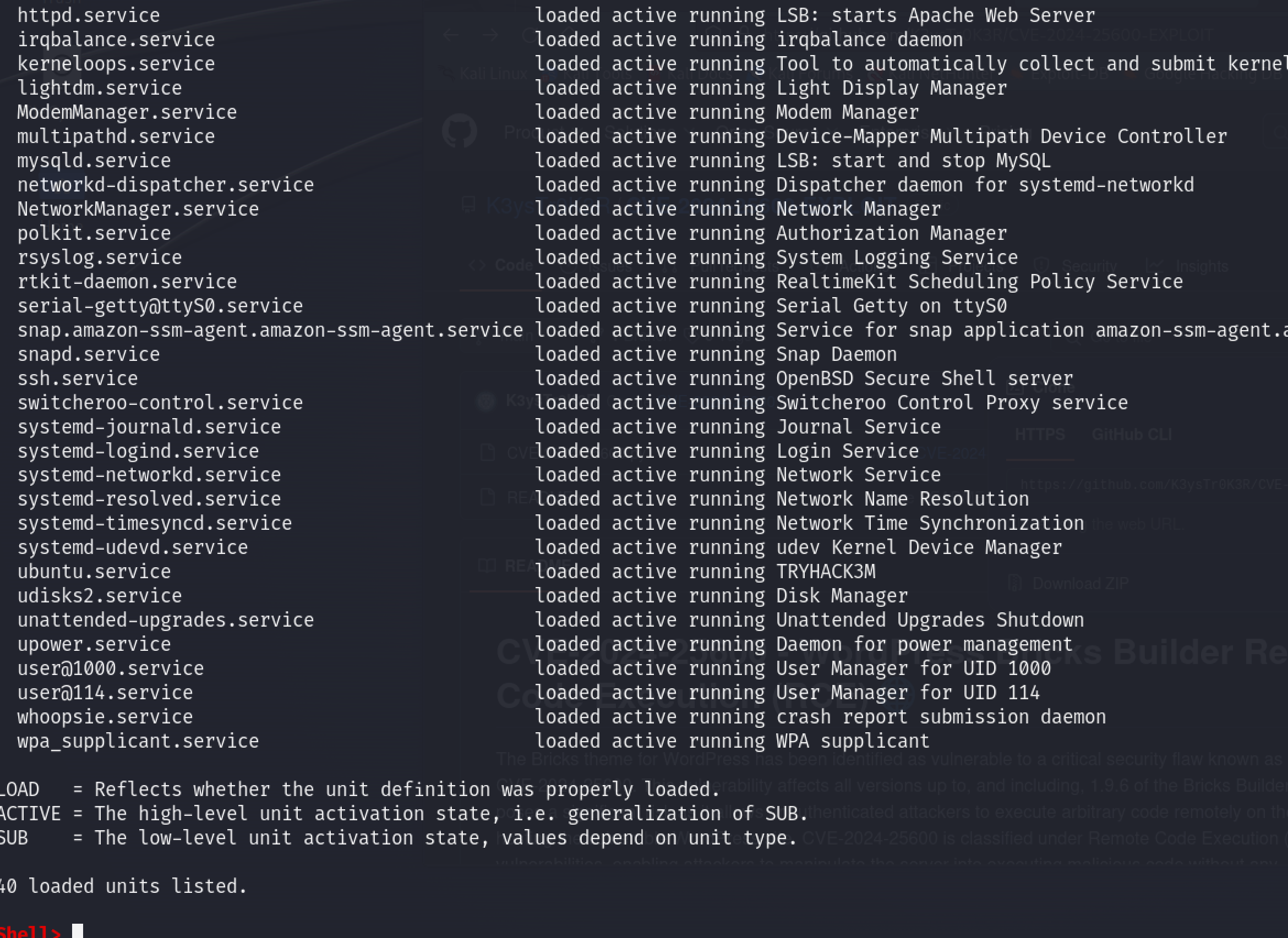
* **“ls”** and we find files and one is text file with numbers.
* So, we use the command “**cat”** to display the text file.



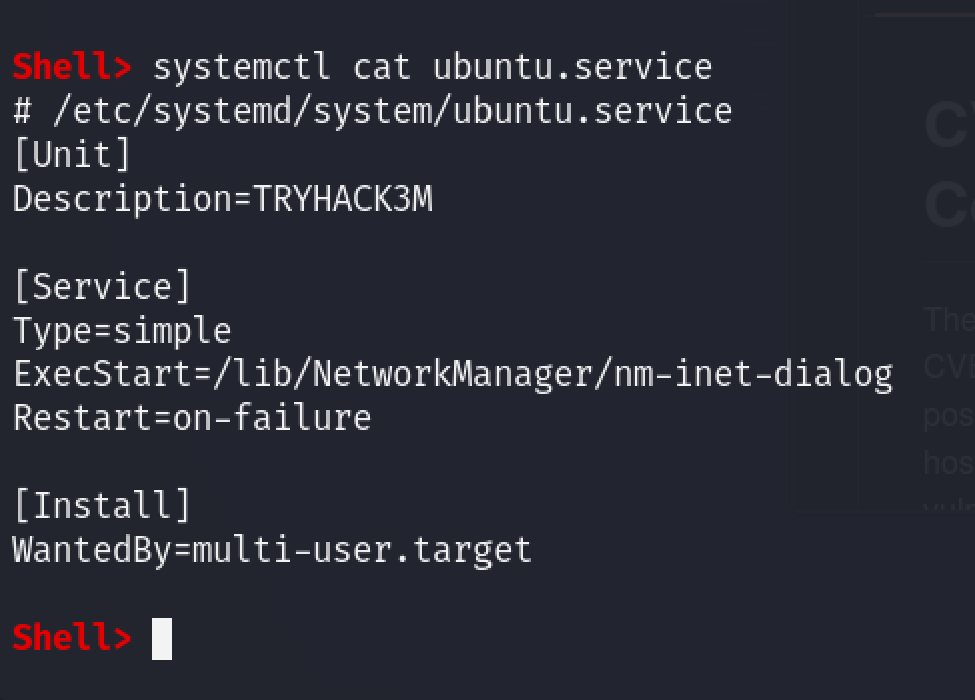
* **BOOYA** here is our hidden text.

1. Next, we find the services that are running using the command **systemctl** and try to find a suspicious process.

* systemctl list-units - - type=service - - state=running
* -- type = show what is the process
* -- state = show in what state the process is, is it running or not.
* Among the services that are running we see there is a description that says **TRYHACK3M** so that got be the suspicious process.



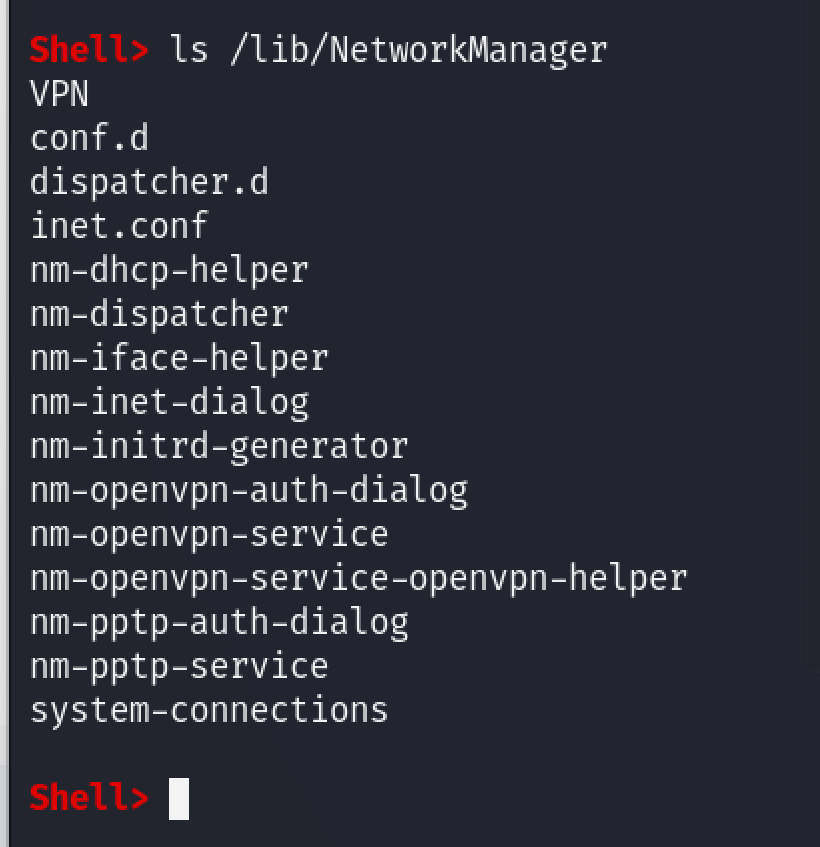
* When we view the service by its name, which is **ubuntu.service** we find the name of the process which is **nm-inet-dialog**.



* **BOOM** we just answered two questions at once, now let’s continue to our next question.

1. Since we know the path of the suspicious process, to find the log file we search in the directory where the process is.

* ls /lib/NetworkManager



* As you can see the log file name is **inet.conf** which we will prove on the next screenshot.

1. Running the log file, we will find what it does and an id which is ecoded.

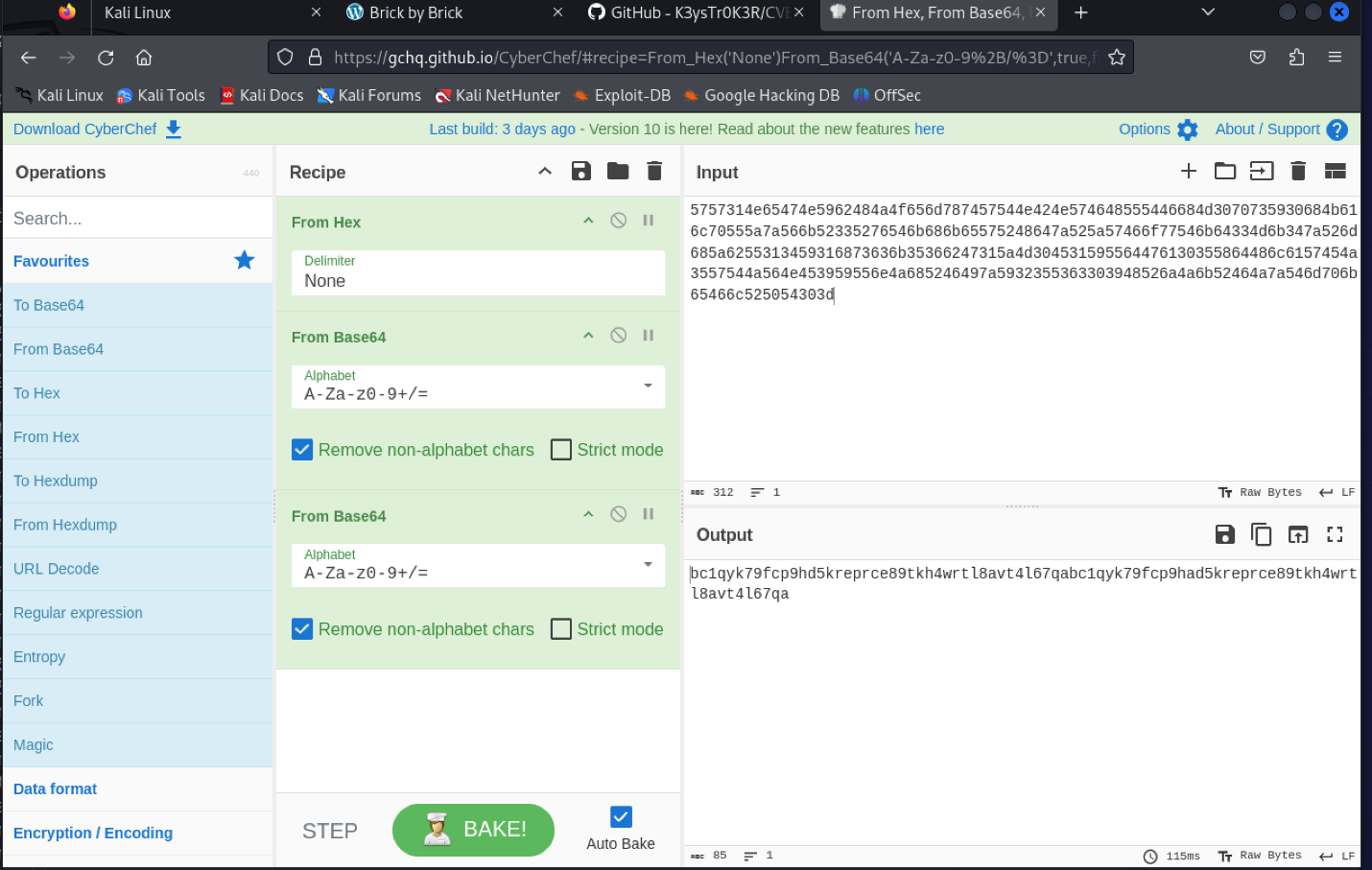
* The process is a miner
* To find the Id we must decode it.
* cat /lib/NetworkManager/inet.conf

A screenshot of a computer

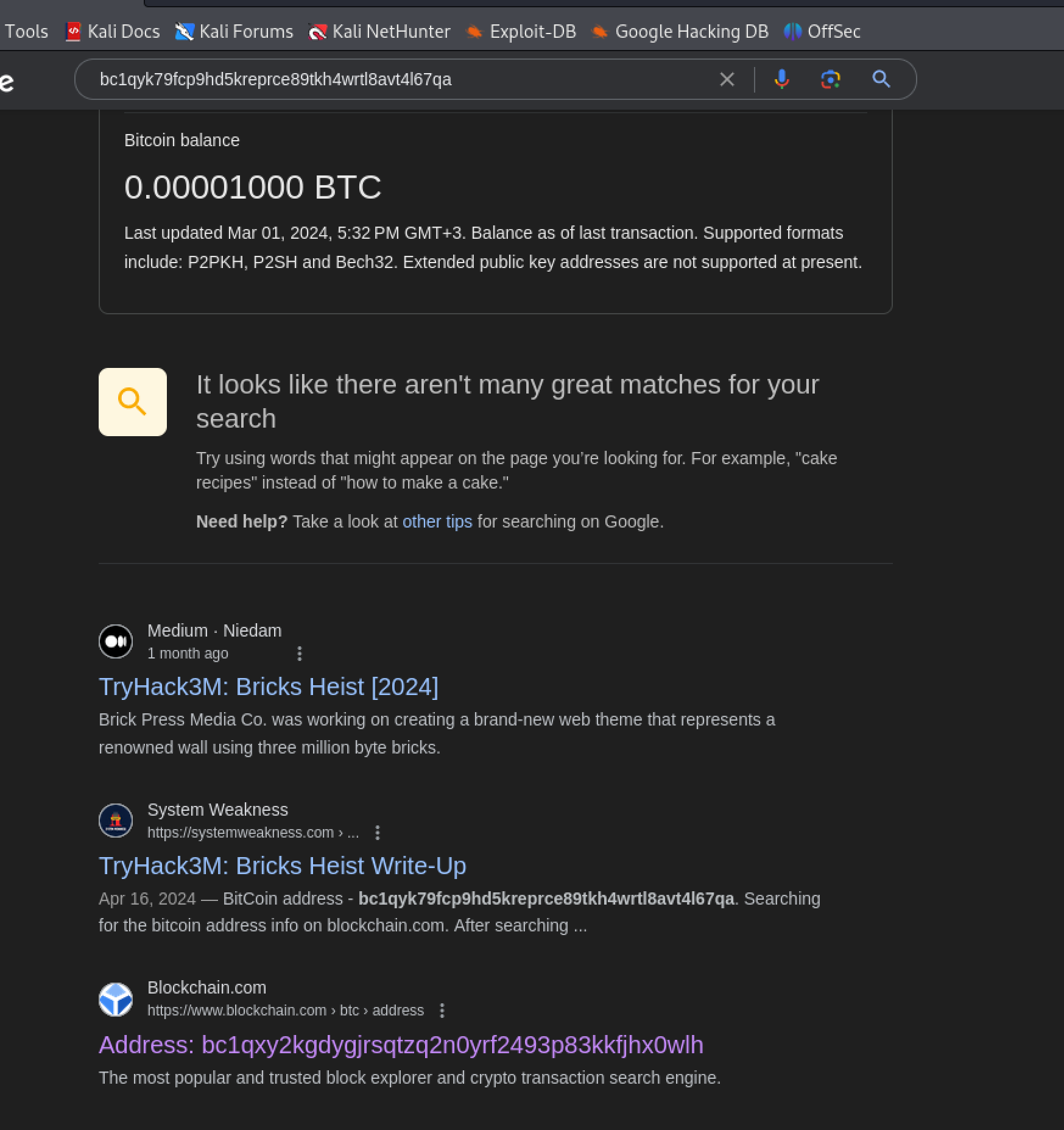
Description automatically generated

1. To decode the id, we will use cyberchef website

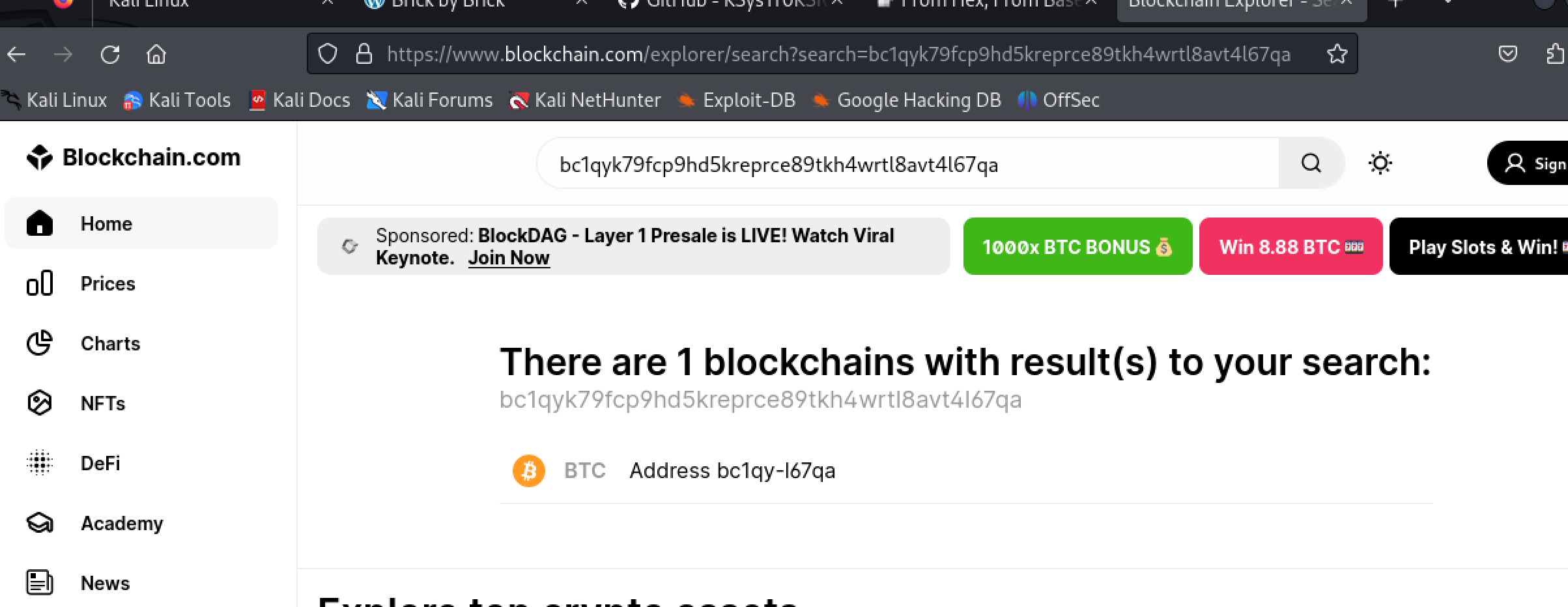
* On decoding it we found two duplicate keys with one letter (a) added to the second key.



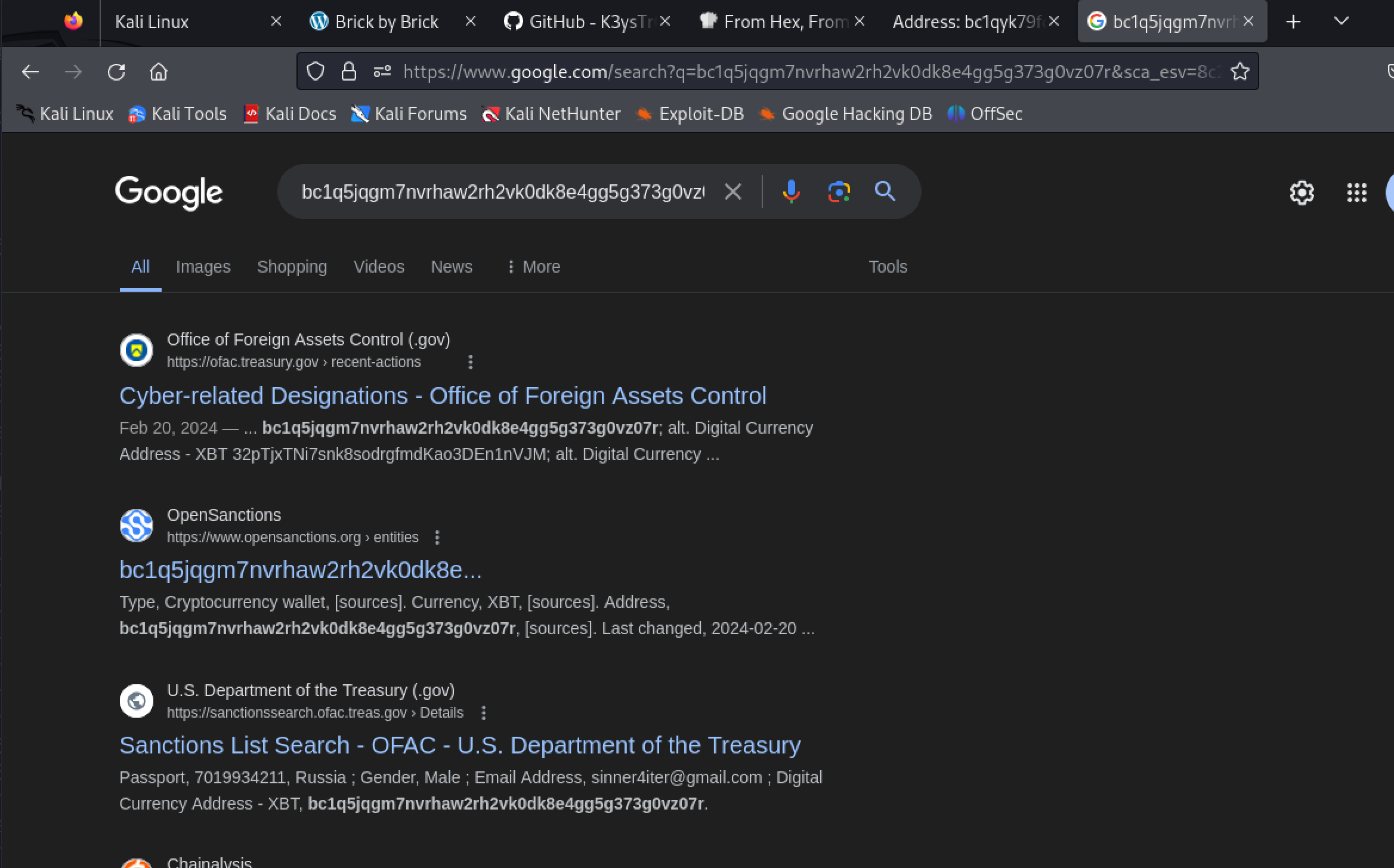
1. When we searched for the id we decoded it is a bitcoin wallet addres and we found the following search results.



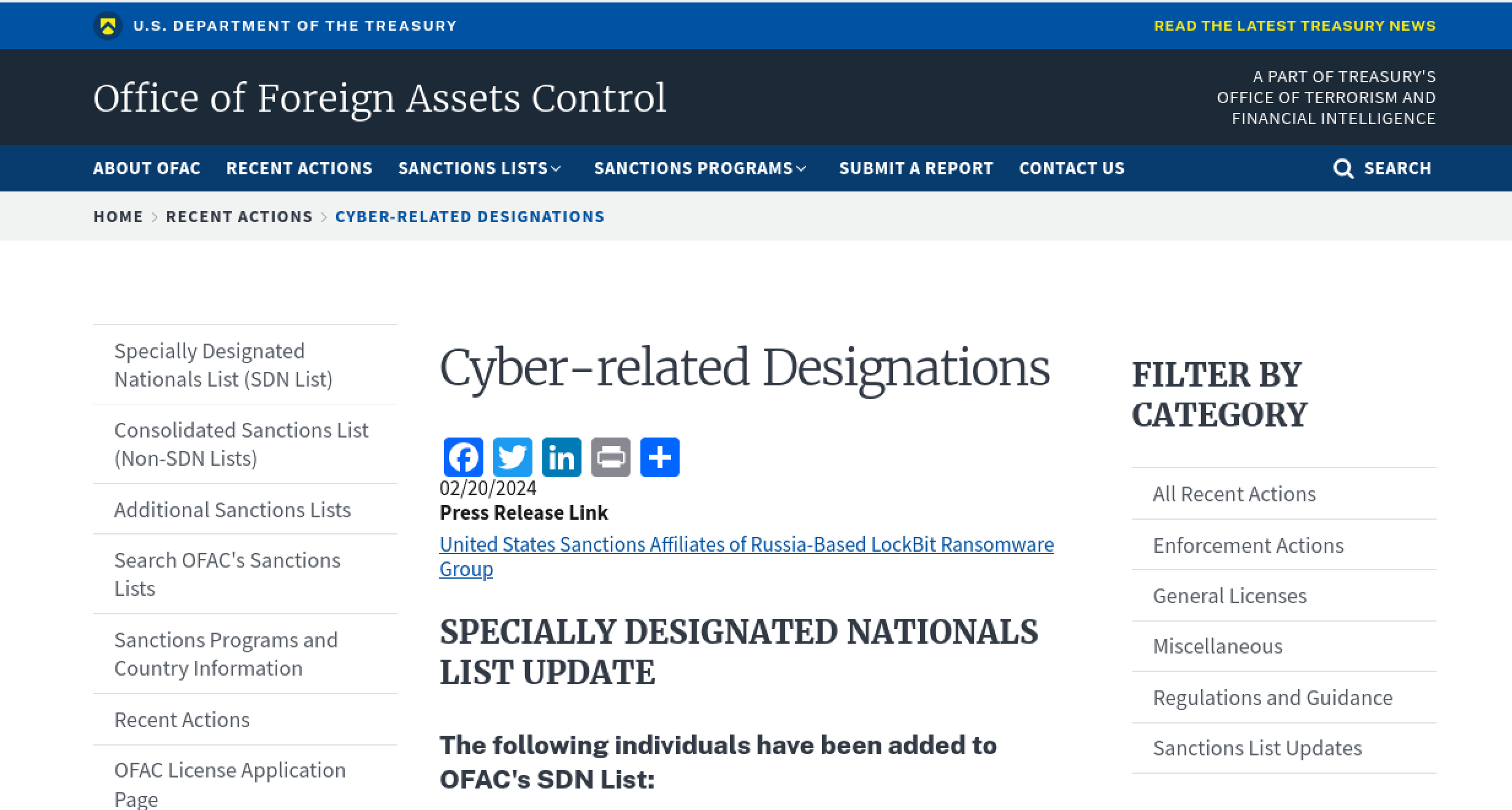
* From the search results we see that the blockchain.com website is showing us the address so let’s visit the website.
* On visiting the website and searching for the address we found a match for the wallet address.



* Going to the address we found that there are seven transactions and going to the first transaction we found another address. Searching for this address gave us the following results:



* Opening the first link and going through it we found Russian-based hacker group by the name of **LockBit Ransomware**.



1. Finally, here is the last screenshot for you. Thank you…...

