004. TwoMillion

CTF Name :TwoMillion
Player Name : Fr3y
Platform : HTB
Difficulty : Easy

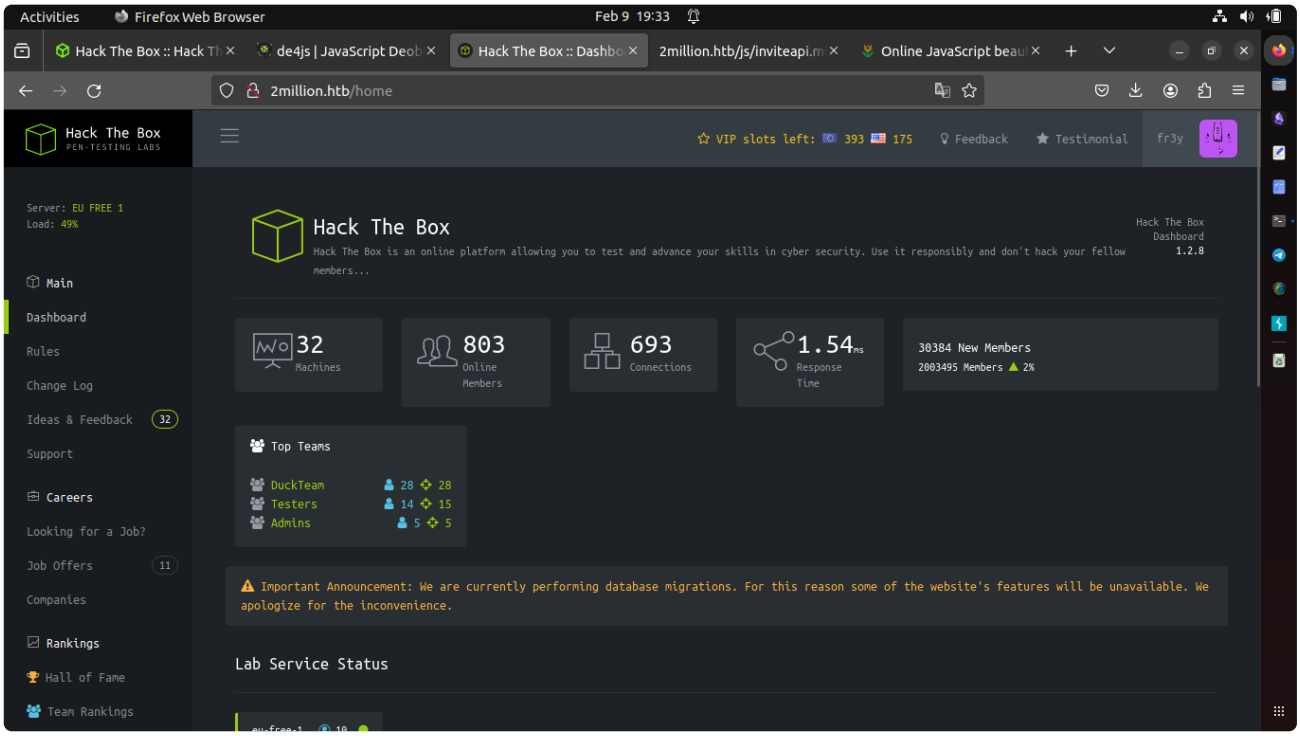
---

1 NAMP

Hey I'm back and this is 4th CTF of the year so Let's make it count
well As always start with nmap
lol but I did't do that but
there will br port 22 / 80 open as it foes with ssh and there is a website

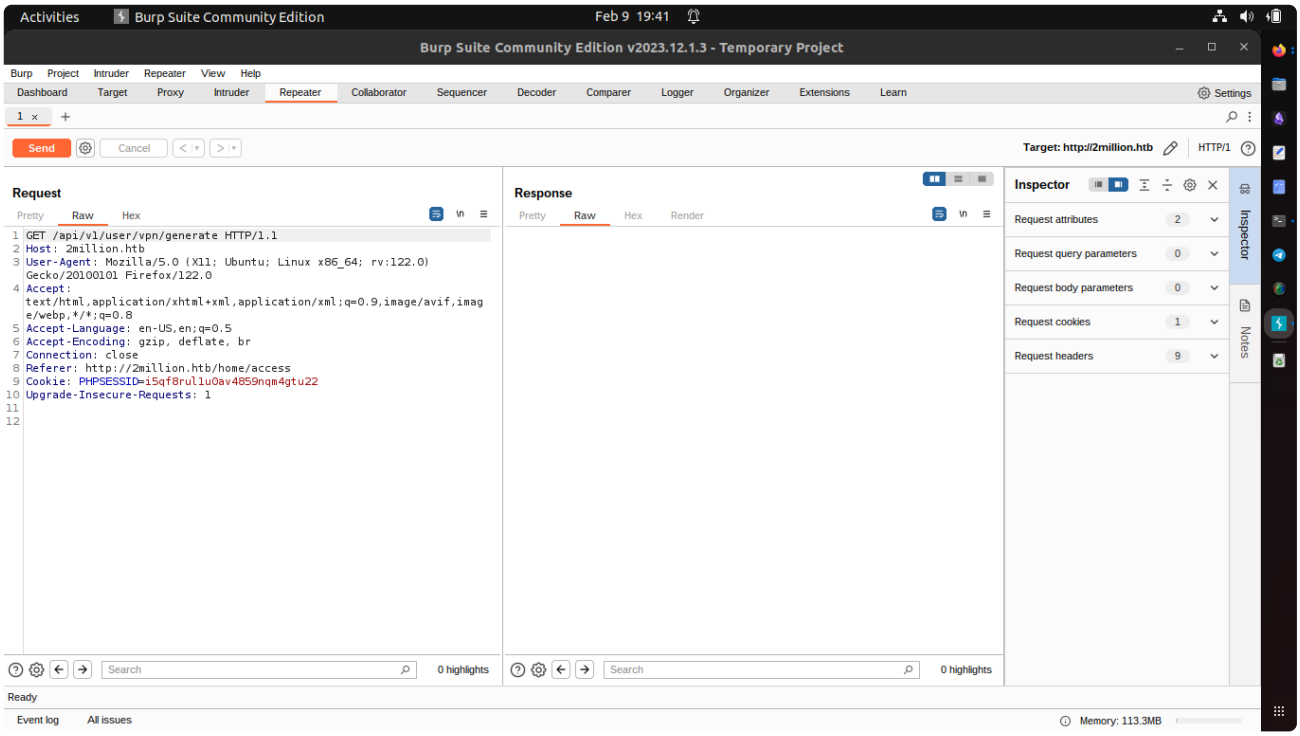
2 Web Discovery

I would Have use the tools but as soon I landed on the page 2million.htb I got what it is so we have to sign in but by access the invitation key you can have it through curl and and extracting the key (bas64) and decode it

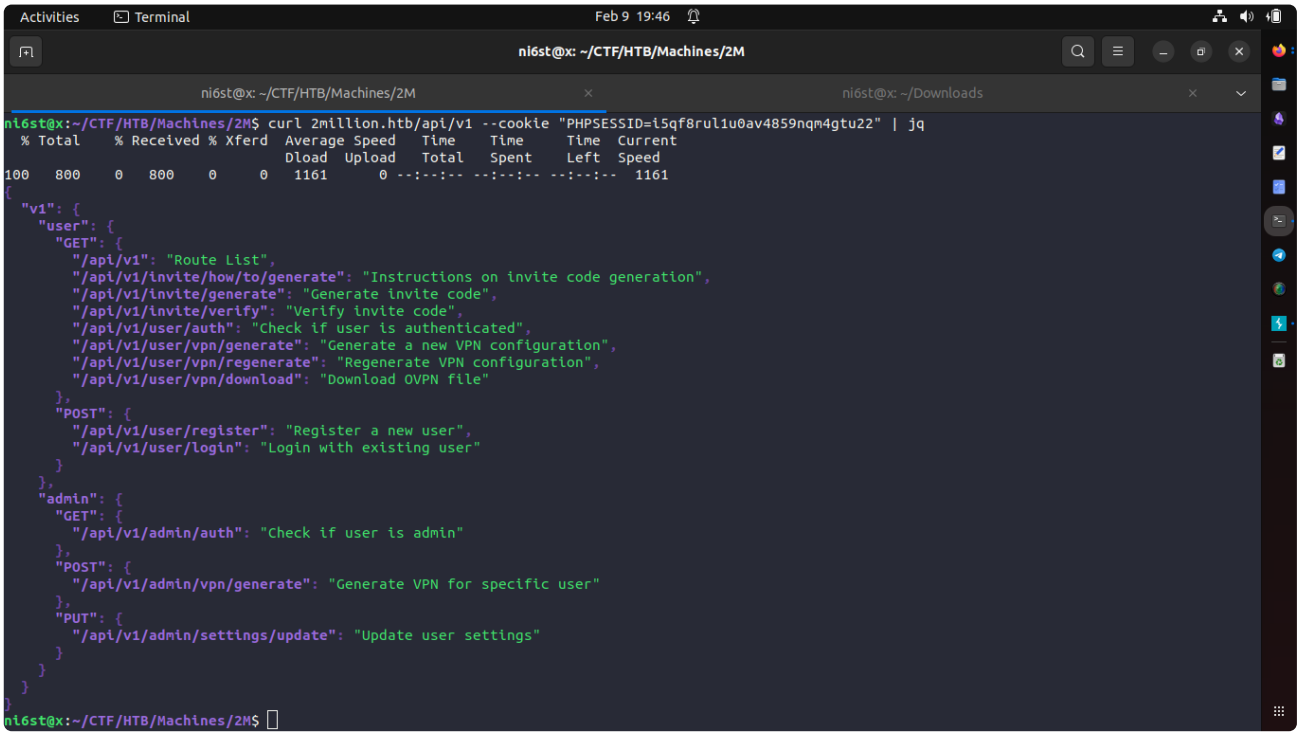


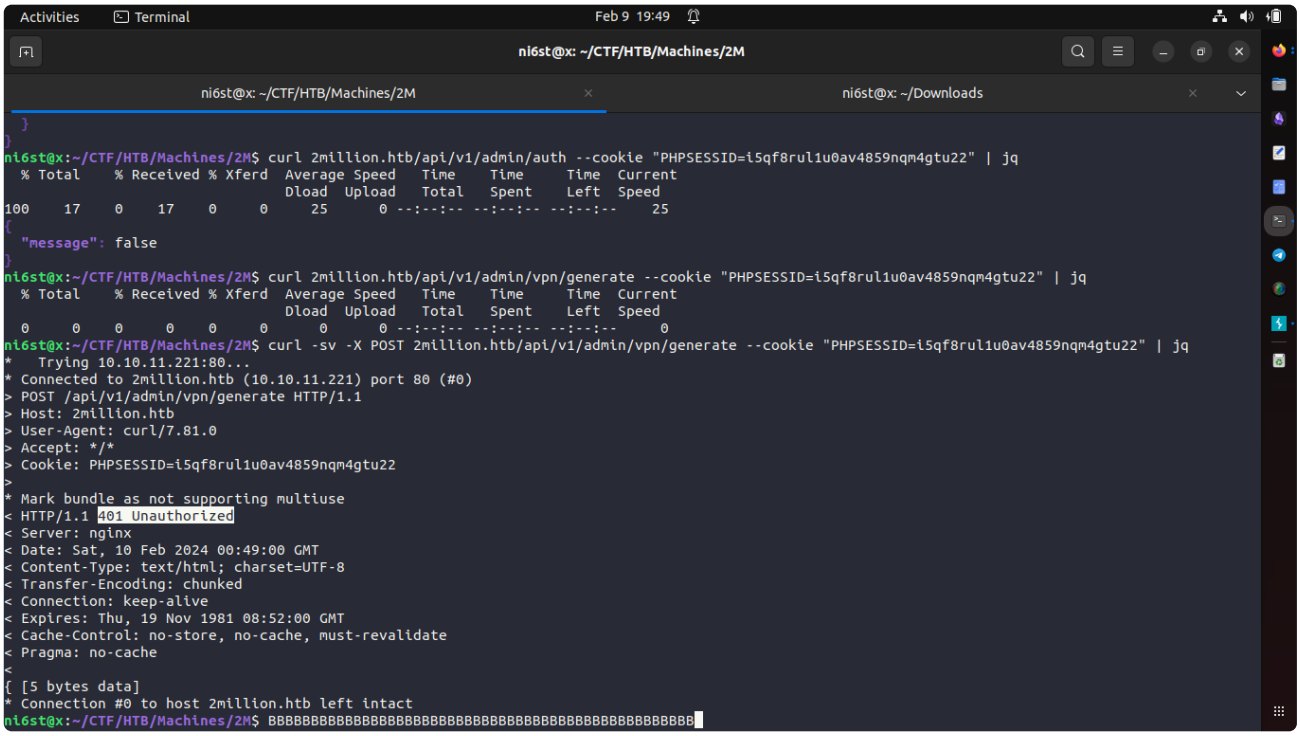
3 Making Response

Go to access and then open your burp and see the cookie but not eat it

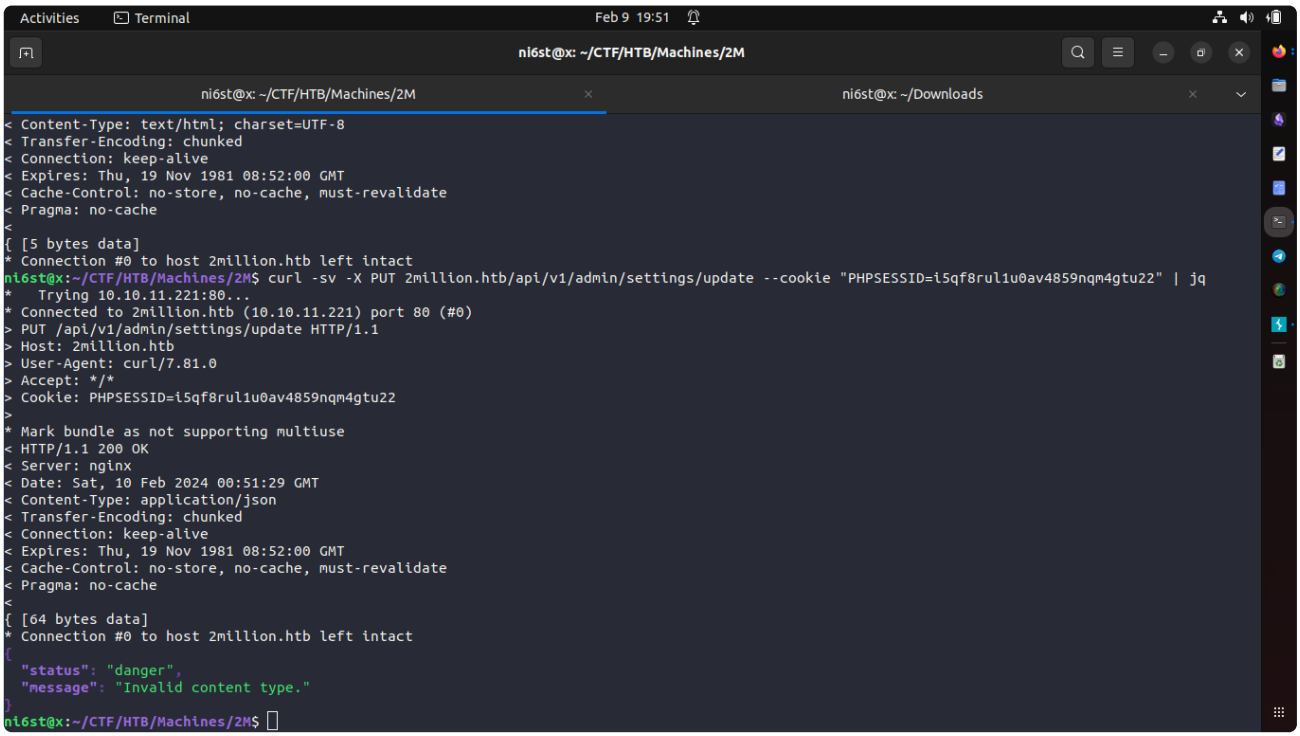


Here we can see our cookie tho save it somewhere



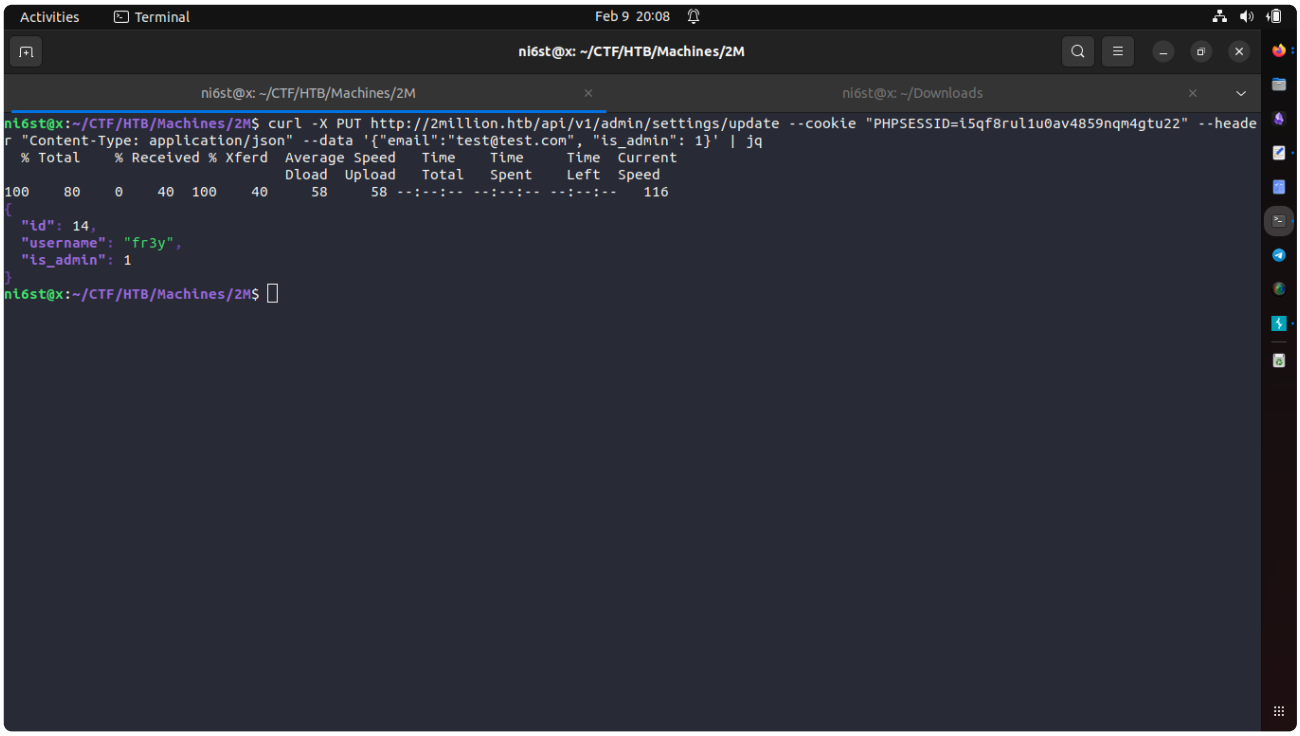


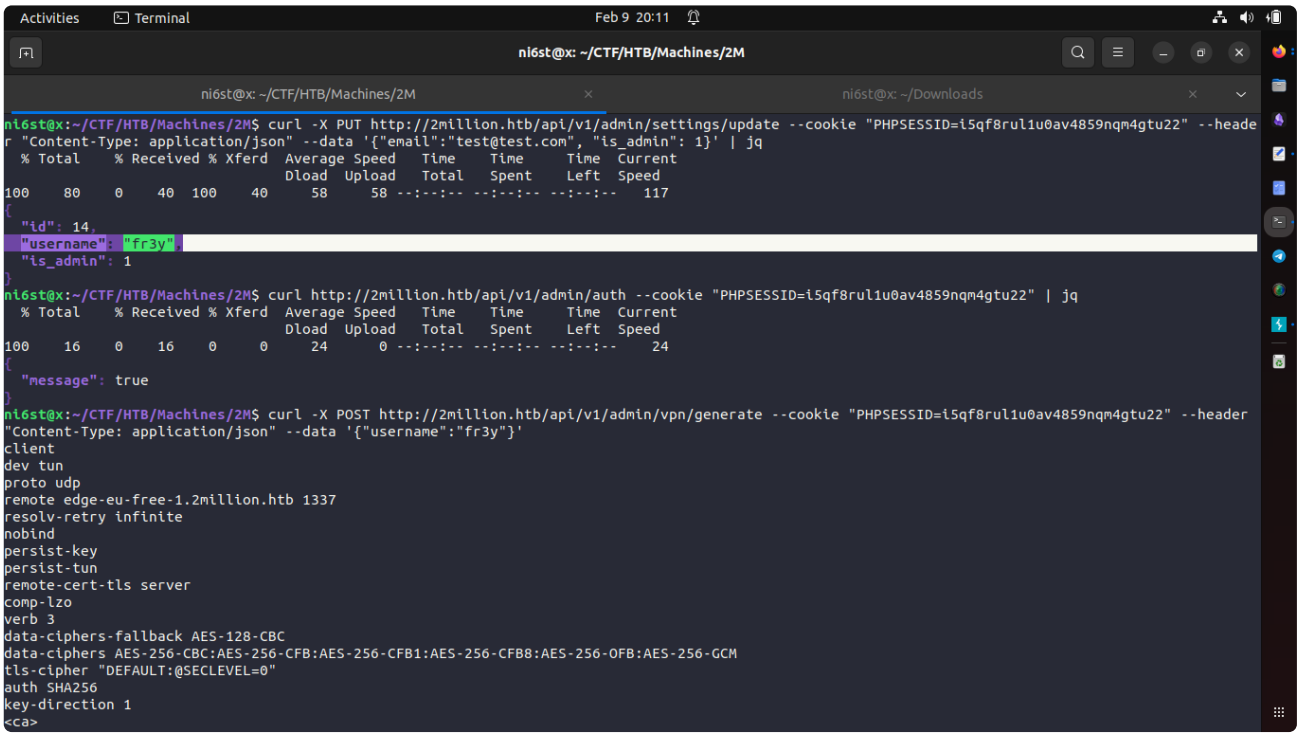
Now the things we have to do is to make a command execution with giving the response back to the site by the post respond but for that we have to be admin so for doing that we have to put our head with json responds jq will be your friend in it.



4 User Flag

I have spend almost 30-40 minutes in becoming admin giving my user the admin value but now it is easy as it give us the error back what is wrong and what values it ask for.

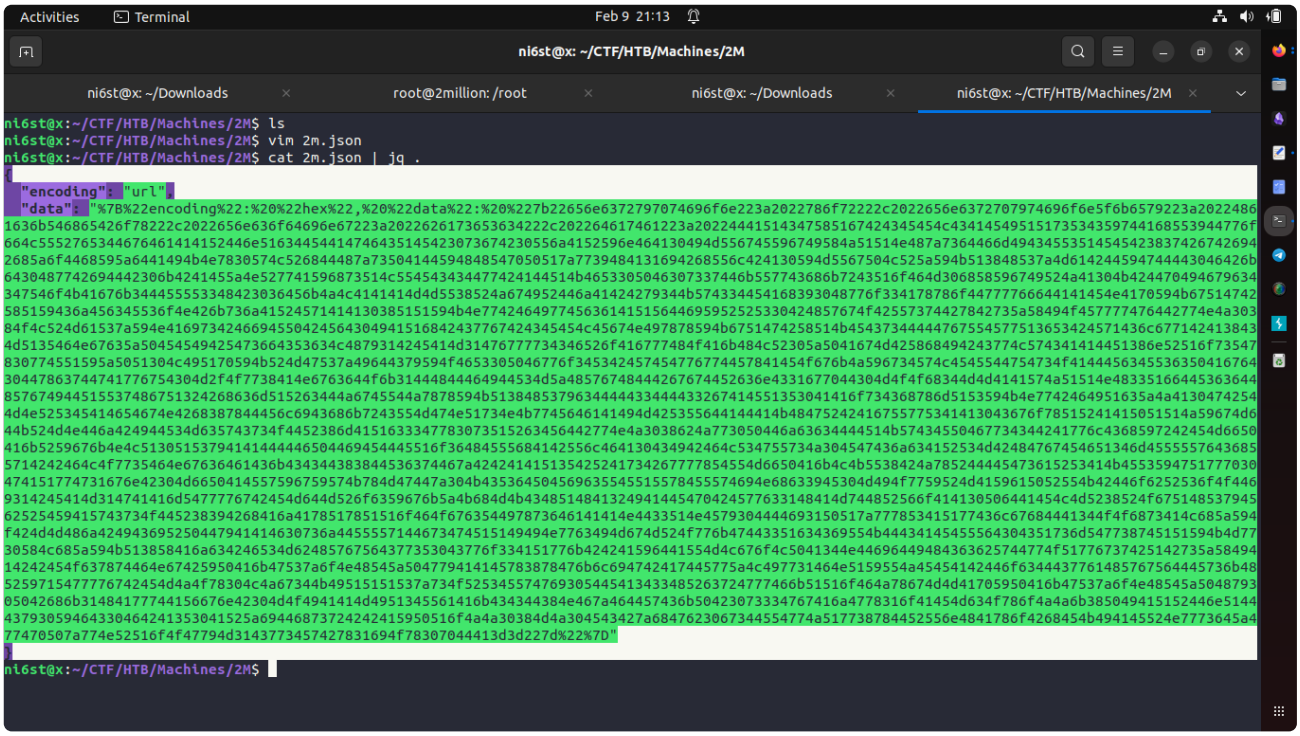




Now as we are user root fr3y is root with all the admin value we can run the command execution so here I test it with "whoami", "id" and it work now time for the payload as these commands work we can use bash reverse shell but we have to encode it in base64 no worries we can decode it in the coomad itseld with base64 -d

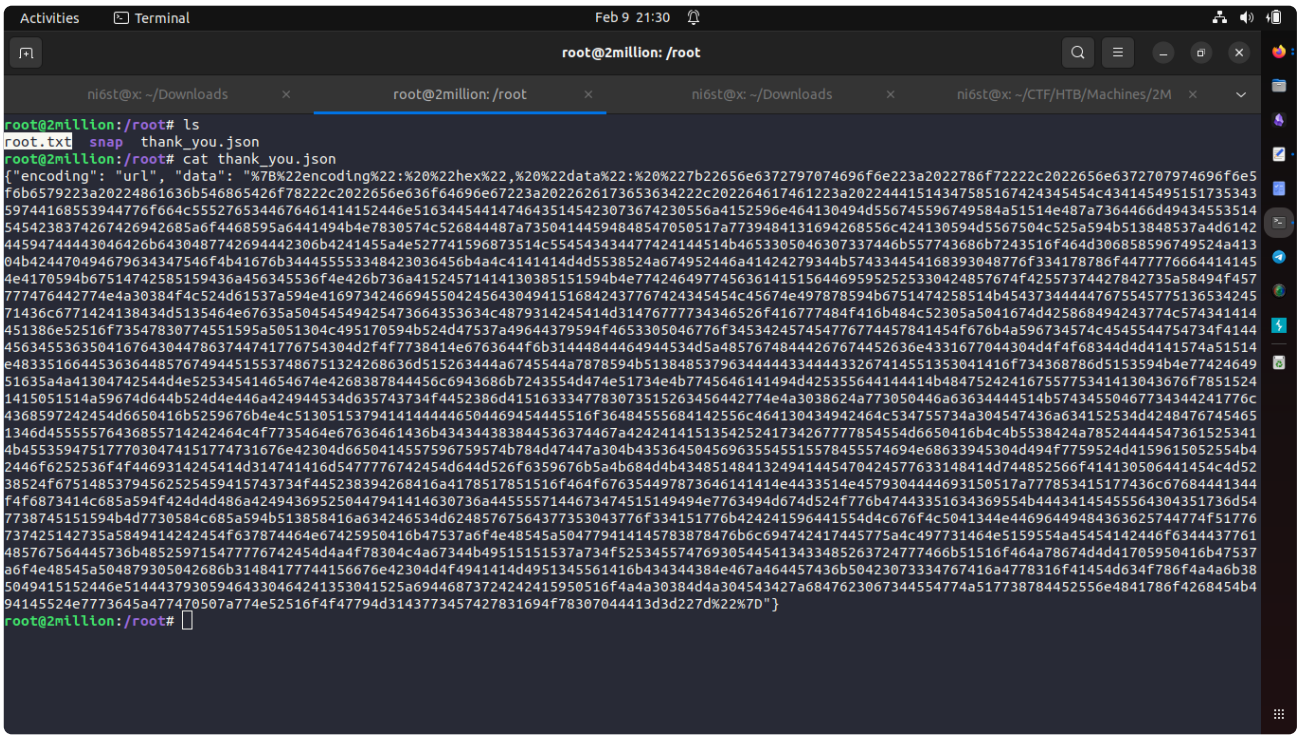
and you will be log in get the user flag

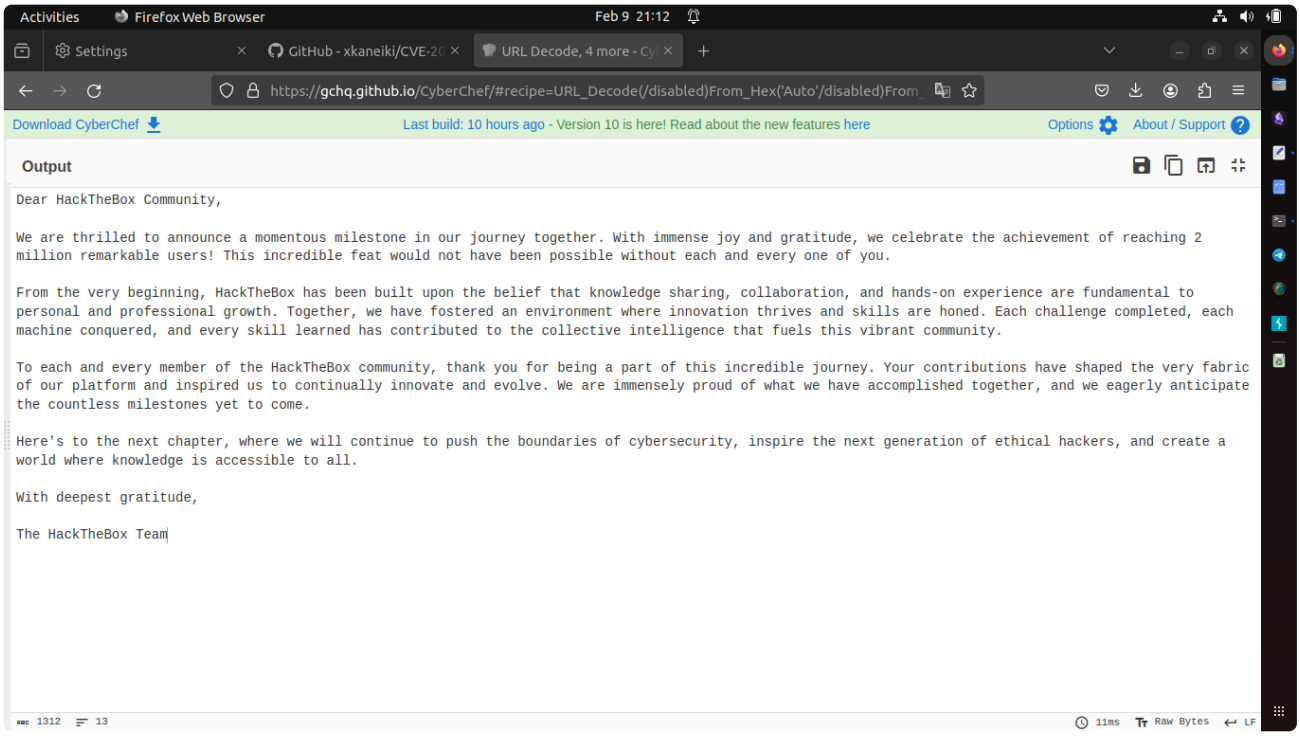
5 Root Flag



Root Flag is easy all you need to do is download this https://github.com/xkaneiki/CVE-2023-0386/blob/main/exp.c (CVE-2023-0386) and follow the commands it offer and you are root

6 Message





But I have my eyes on this file thank_you.json as this is something I want to get you have to decode it as it is in url decoded -> bas64 -> xor (latin1)

Thank you
Happy Hacking
Twitter : @fr3y0