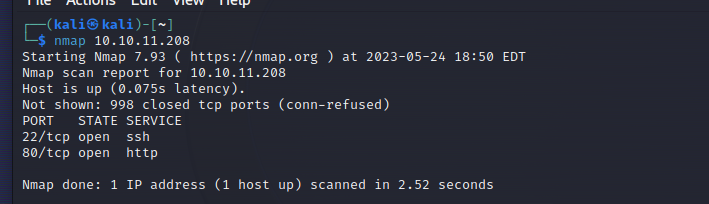
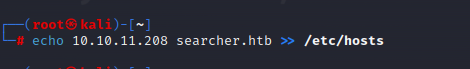
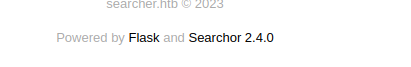
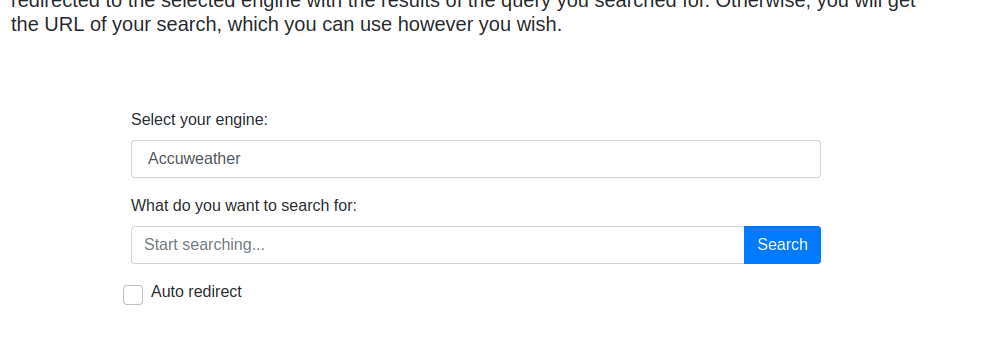
After connecting to the VPN I performed an nmap scan



Entering the ip address in my browser gave back a domain name

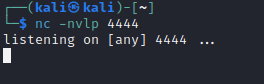
I then add it to my /etc/hosts

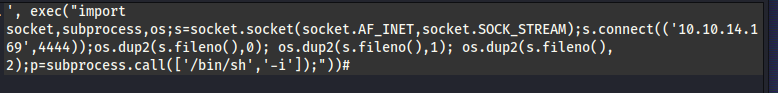
After returning to the website, I can see that it’s powered by flask and searchor. 

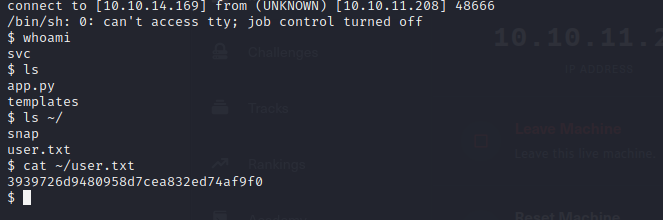
Searcheor has an exploit for version 2.4.0 and 2.4.2 making it vulnerable to injection.

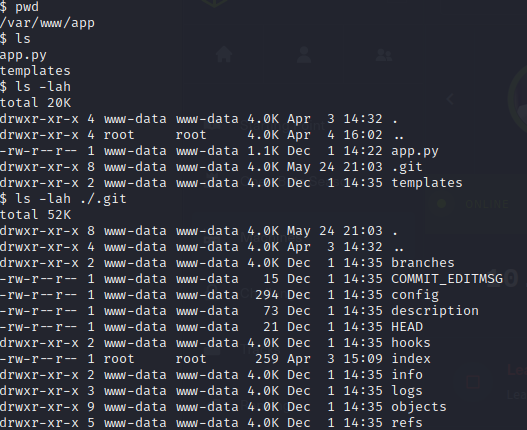
<https://github.com/jonnyzar/POC-Searchor-2.4.2>

I set up a listener

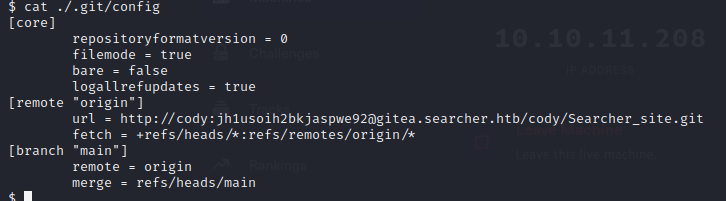


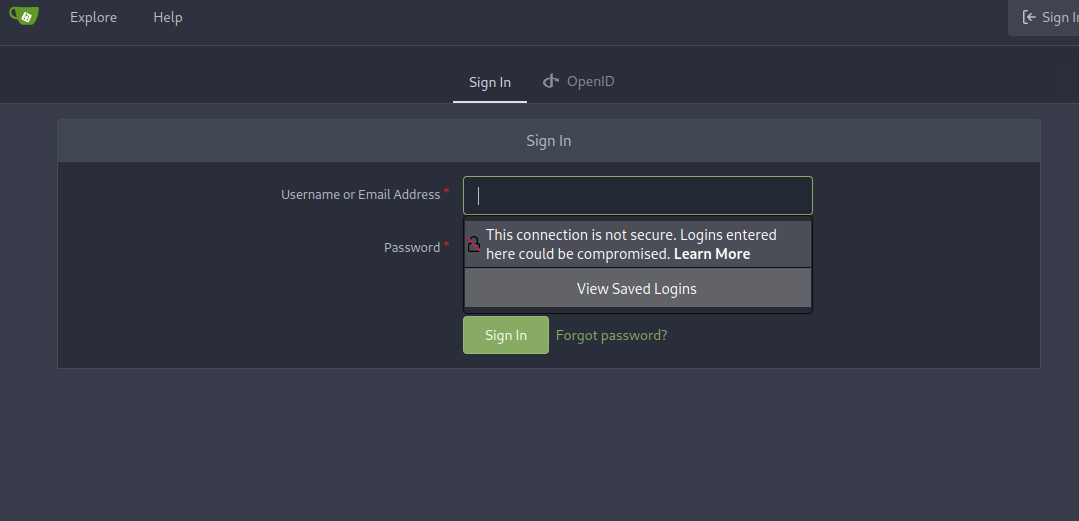
This is the reverse shell code that I used in the search bar for the site

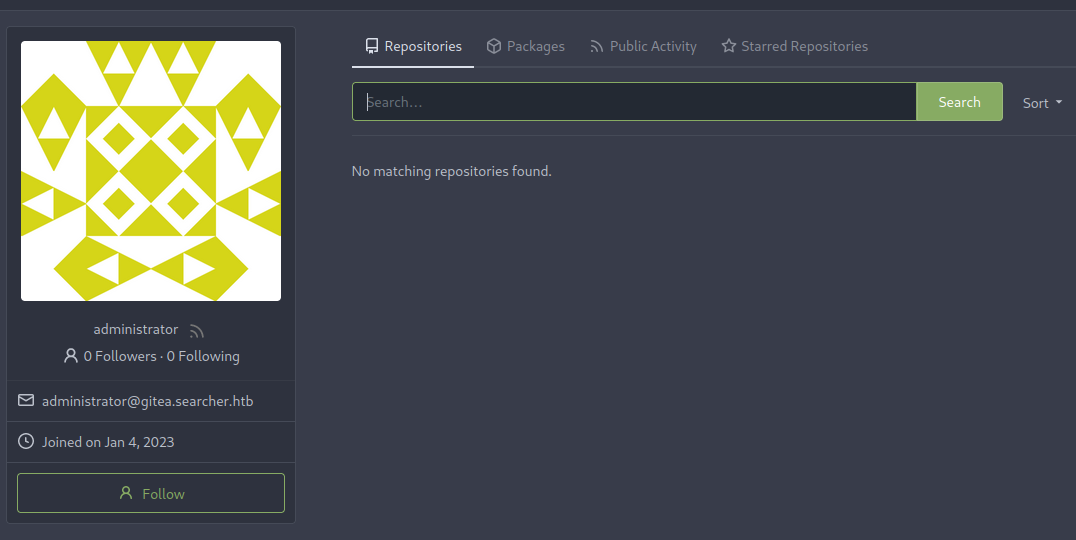
From here I can find out the user and cat the user.txt file giving me the user flag

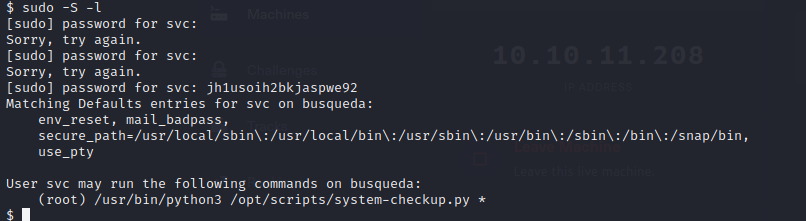
From there I can further enumerate and find a git file

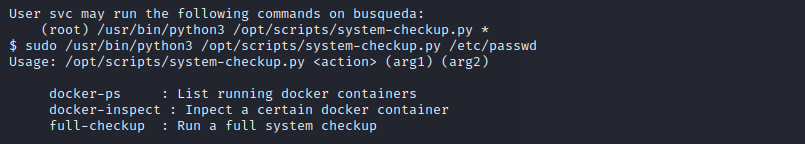
After reading the file I find a password for cody and a url link

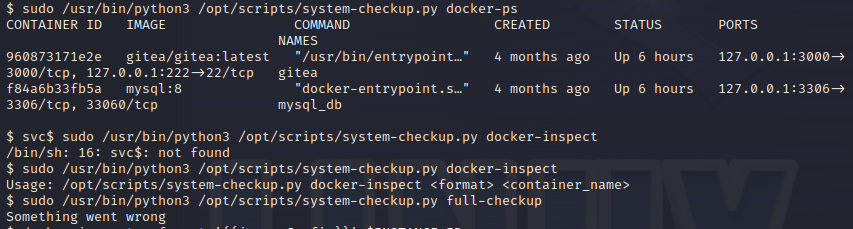


When opening the url I can login with the user cody and password jh1usoih2bkjaspwe92

The site doesn’t tell me much other than that there is another user named administrator.

Back at the terminal I can try to see if the password for cody will work here too and it does. 

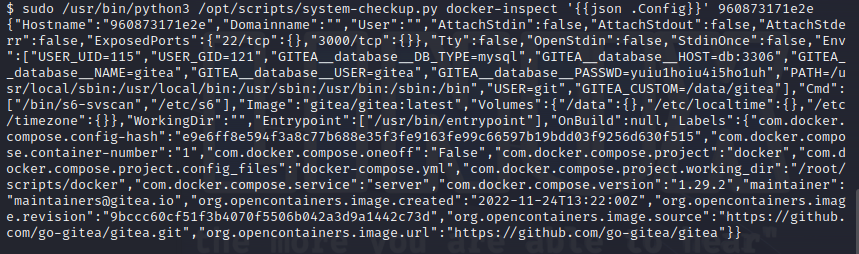
I can’t read any scripts but I can execute them.

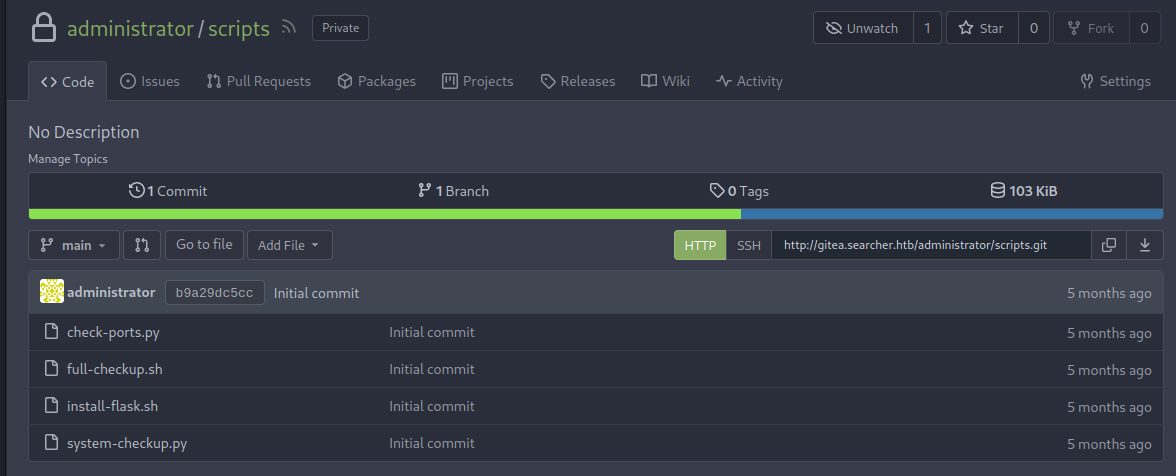
After testing each I can see that docker-inspect is asking for a format and container name. I can also see two containers, one for gitea and one for mysql.

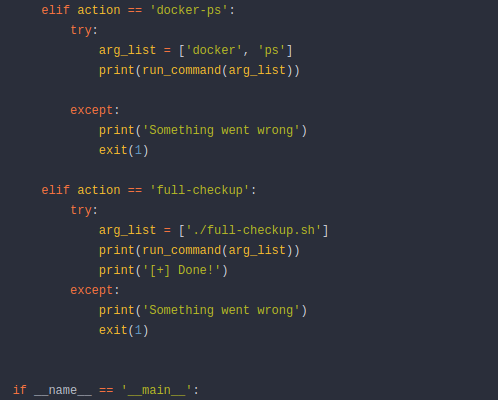
I can find the type of documentation for docker objects online here

<https://docs.docker.com/engine/reference/commandline/inspect/>

with this I can dump the config.

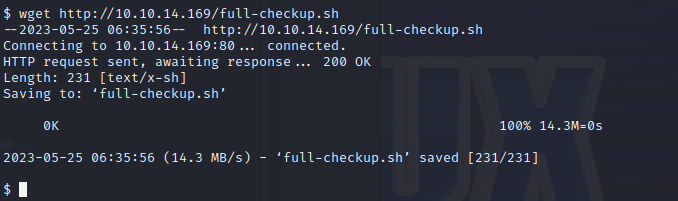
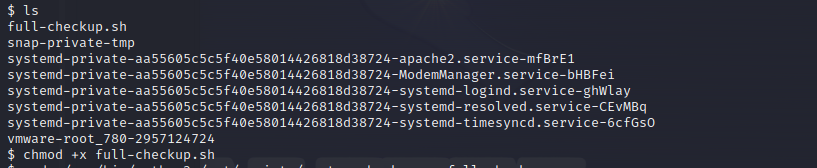
I dumped the config container for gitea and got a password. The sql container had a password also, but it ended up not being useful.

I went back the gitea.searcher.htb website and this time logged in as administrator using the password that I just found.

From here I can now read the file system-checkup.py and see that I can run the full-checkup.sh file

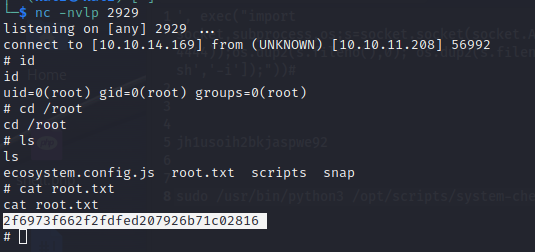
Now I save a reverse shell to my desktop that I get from online.I then check where it will be located

I then set up a http server

I download to the /tmp directory because I have write permissions there.I then run the command chmod to make the file executable.

I then set up a listener on port 2929

I go back and execute the file and it hangs

I can now get access to the root directory and cat the root text file.

I now have both flags and pwned the box.