

BUUCTF [ACTF2020 新生赛]Upload

原创

维多利亚蜜汁鱼 于 2021-07-12 15:26:49 发布 134 收藏 1

分类专栏: [CTF Web](#)

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/CrotZZ/article/details/118676099>

版权



CTF 同时被 2 个专栏收录

18 篇文章 0 订阅

订阅专栏

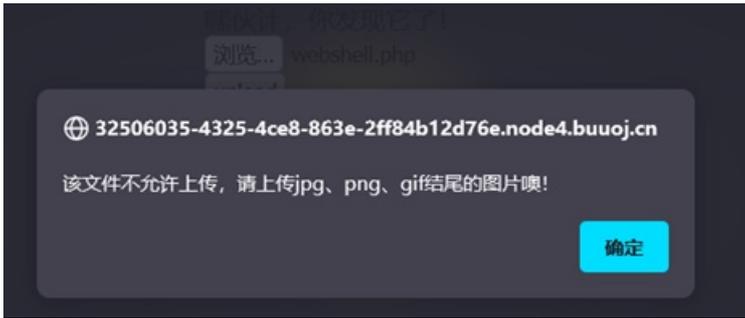


Web

16 篇文章 0 订阅

订阅专栏

先上传一句话木马试试



看到前端进行了过滤

检查下页面元素

```
height="128px" viewBox="0 0 128 128" enable-background="new 0 0 128 128" xml:space="preserve">
  <g id="s-bulb"></g>
  <g id="www-filament"></g>
</svg>
<div class="light">
  <span class="glow">
    <form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"></form> event
  </span>
  <span class="flare"></span>
  <div></div>
</div>
</div>
```

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

onsubmit 事件会在表单中的确认按钮被点击时发生。CheckFile检查某文件是否含相关代码内容
这里将其删去在传文件试试

```
nonono~ Bad file!
```

可以上传成功，但后端也有过滤，不过这个过滤没之前题目那么多（如极客大挑战2019的Upload），改个后缀为phtml就可以登录，极客大挑战2019Upload上传的文件也能用

```
Upload Success! Look here~ ./uplo4d/6bba837013452ad67f53ddce882b95ed.phtml
```

用蚁剑加上上面的路径，进行连接

```
编辑: /flag
/flag
1 flag{29ccf5b5-dd85-471e-8a10-fc3c40b83fa8}
2 |
```

找到flag