# buuctf初学者学习记录--[ACTF2020 新生赛]Upload

原创

pakho_C 已于 2022-02-03 23:46:26 修改 148 收藏

文章标签： web安全 安全

于 2022-02-01 23:55:15 首次发布



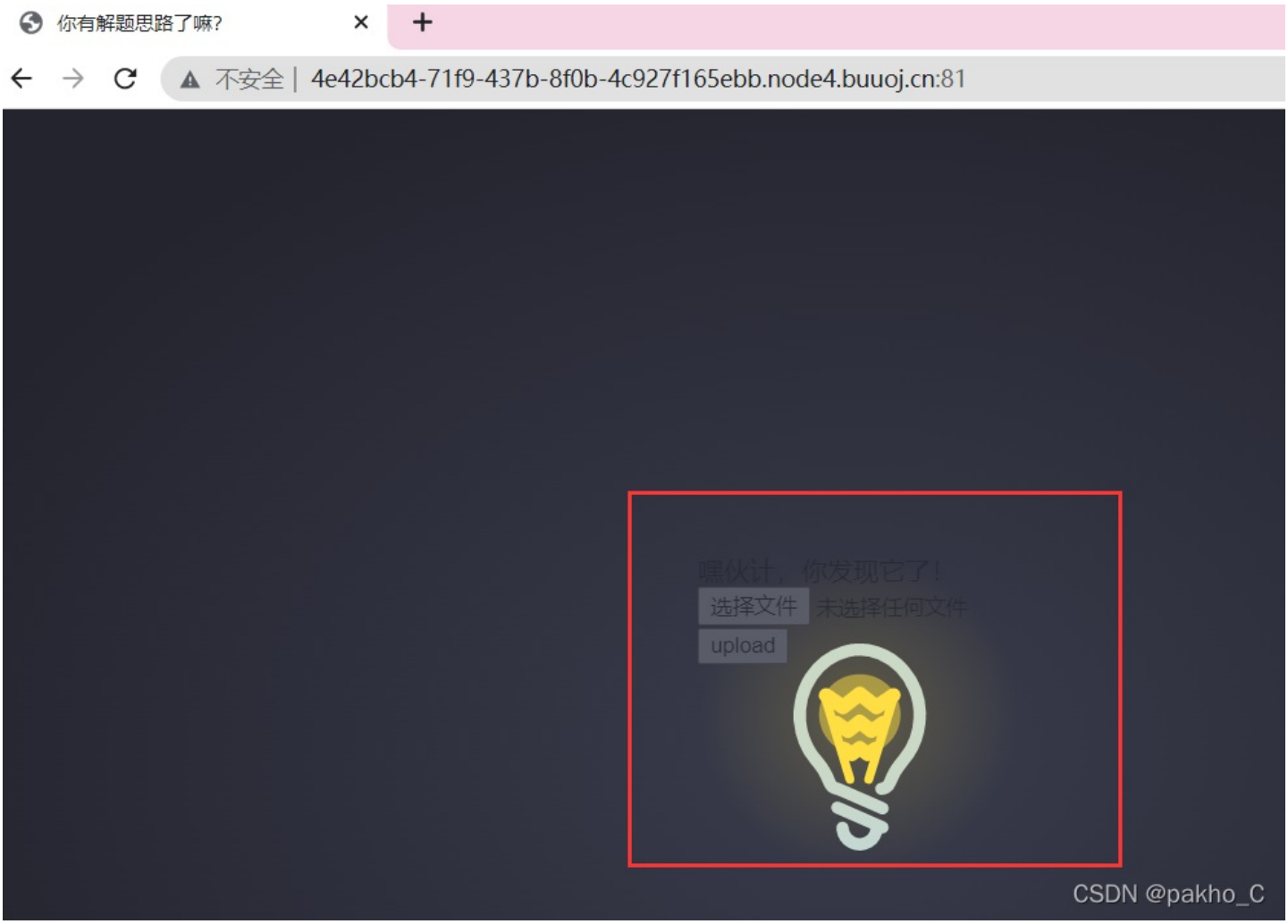
本文链接：https://blog.csdn.net/pakho_C/article/details/122766933



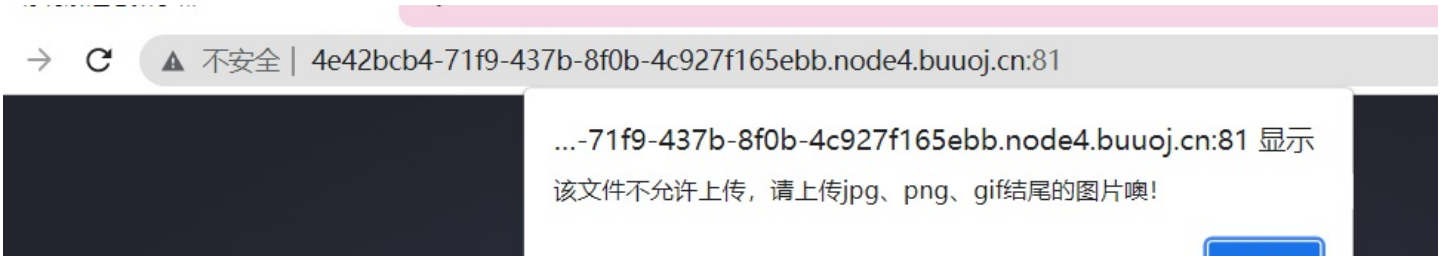
web第15题

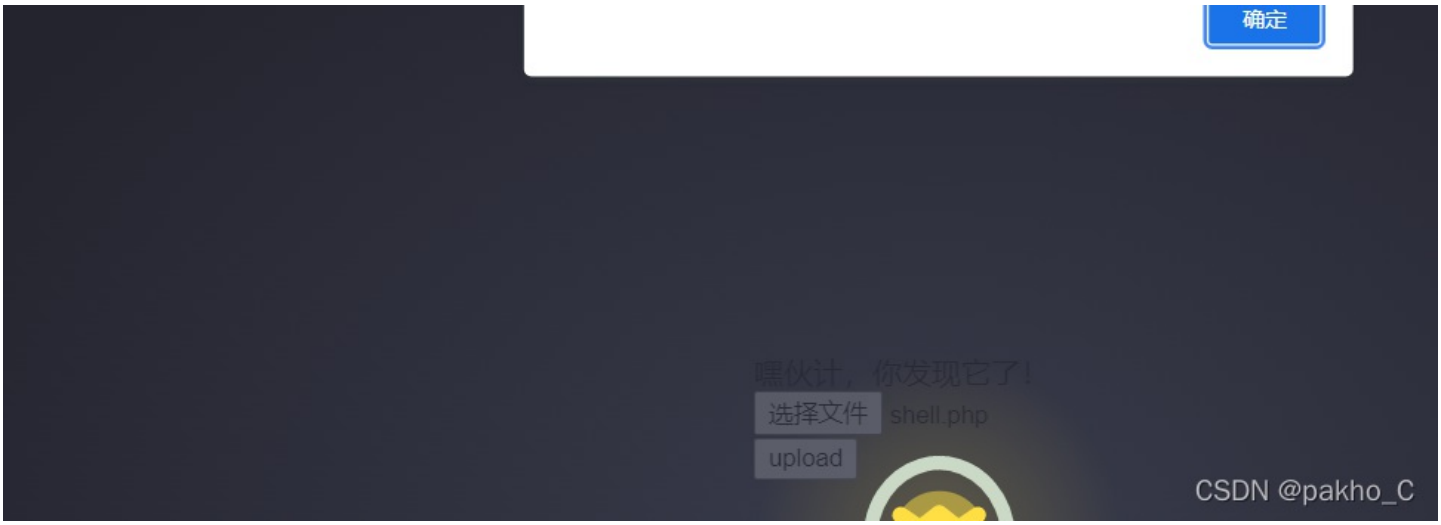
[ACTF2020 新生赛]Upload

打开靶场




显然是一个文件上传的题目，先直接尝试上传一句话木马

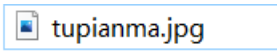





得到提示，应该是白名单验证，可能是只允许上传jpg,png,gif文件，尝试上传图片马
制作图片马

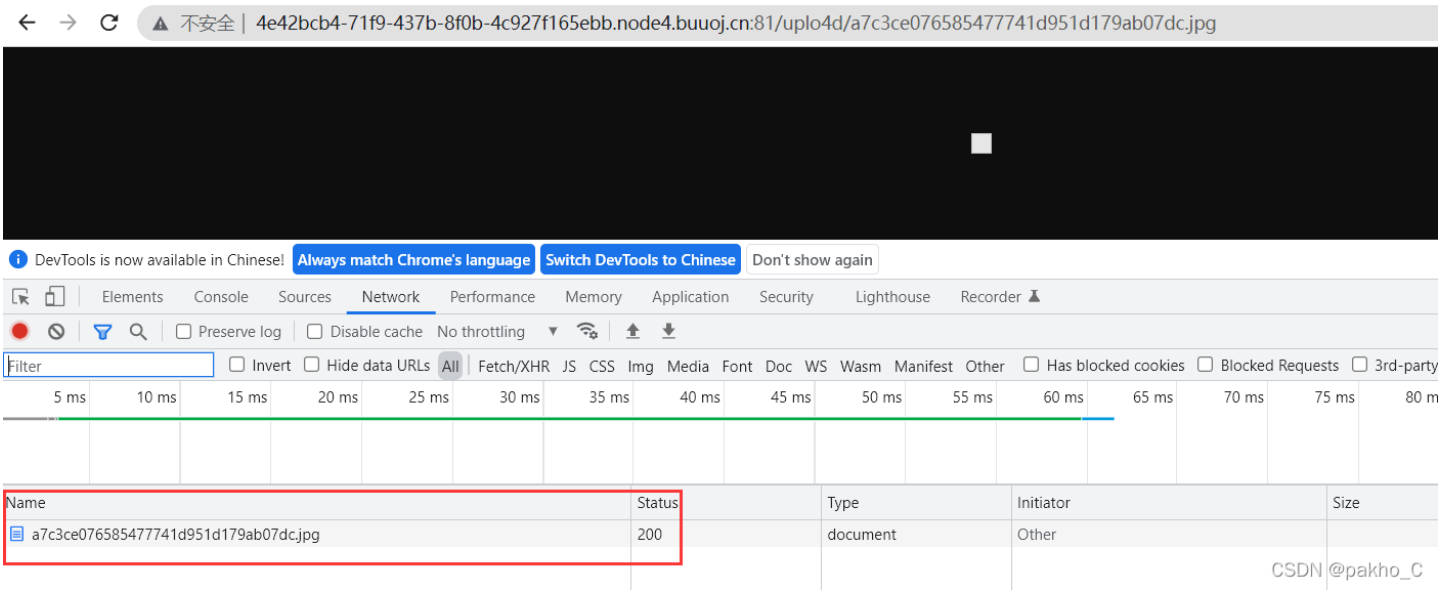
```
copy 1.jpg/b+shell.php/a tupianma.jpg
```

```
1.jpg
shell.php
已复制            1 个文件。
```




然后上传

上传成功，并且返回了文件路径
访问该路径，确实存在这么一个文件



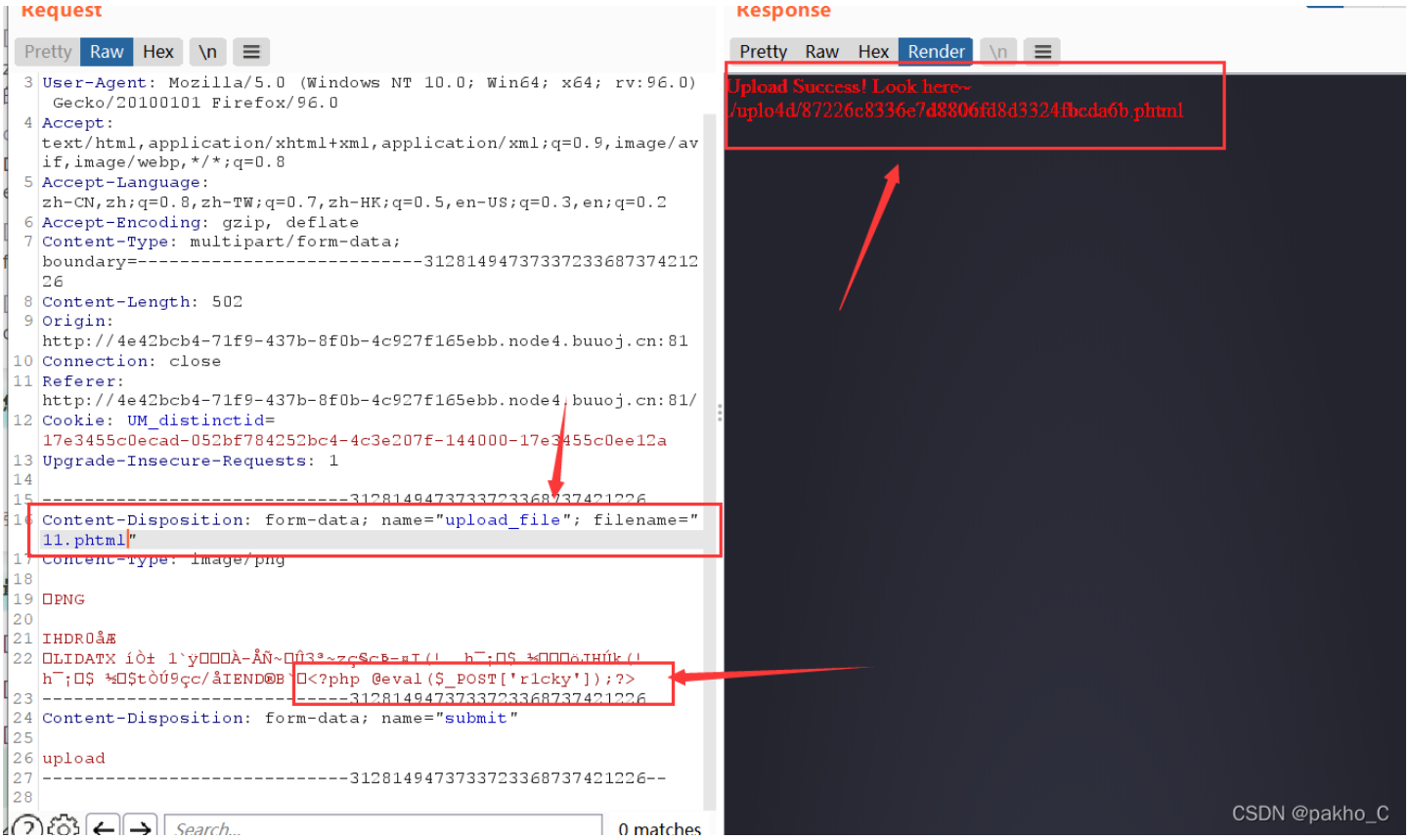

额，做到这里发现好像做错了，使用图片马的话，没有文件包含漏洞的话蚁剑无法解析图片文件，故无法进行连接，查了很多资料也没找到如何连接

换个思路，也许不是白名单验证，黑名单验证的话可以尝试上传图片然后抓包修改后缀进行绕过

参考文件上传漏洞–upload-labs靶场复现（前3关）

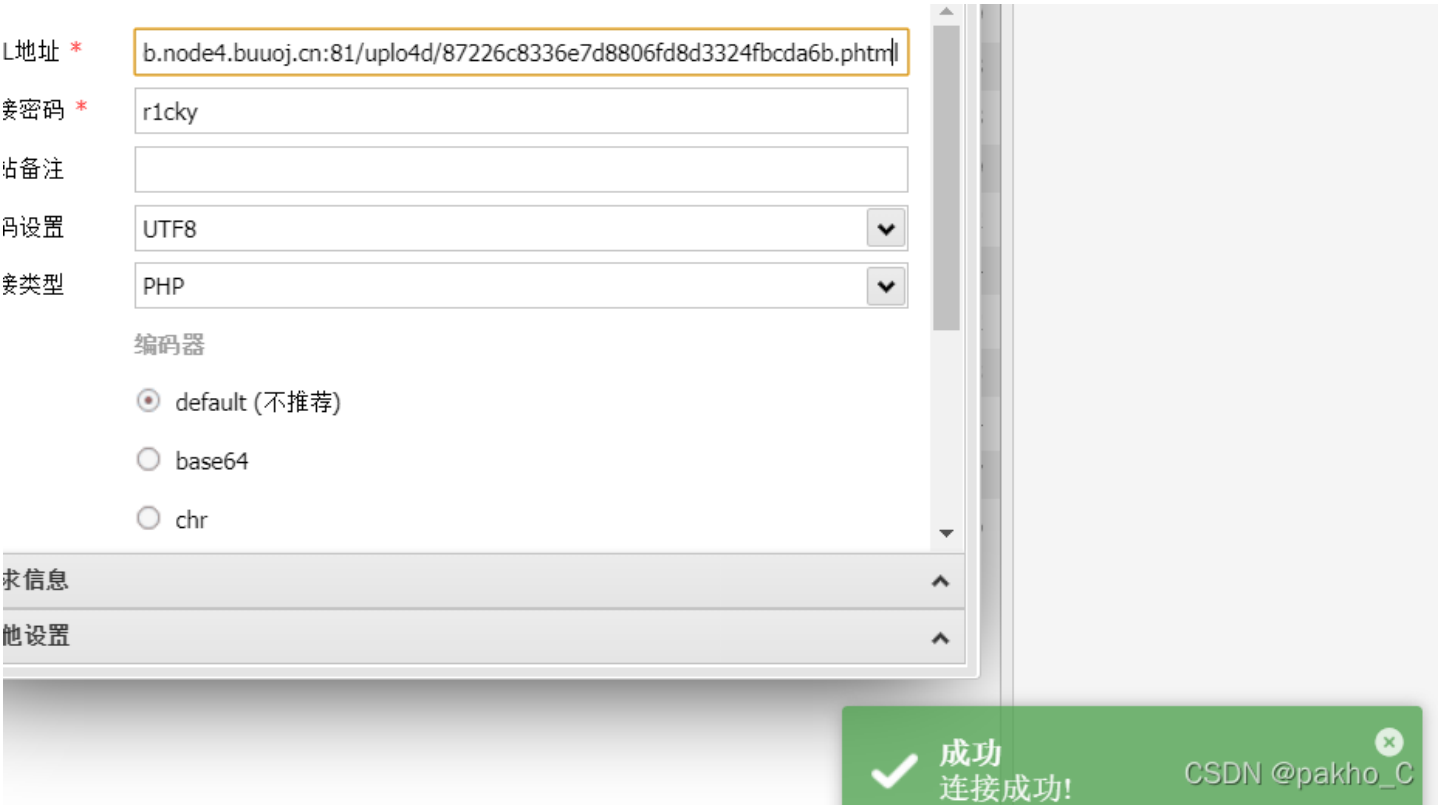
第三关中的绕过以及[极客大挑战 2019]Upload中的做法

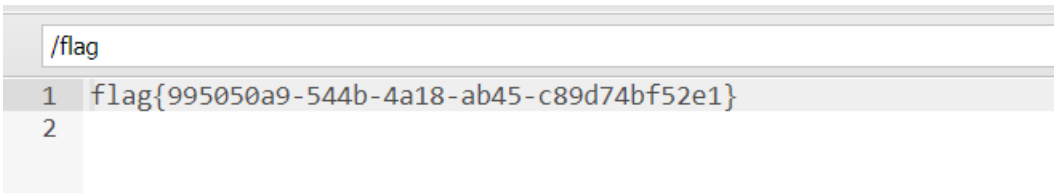
经过尝试.phtml文件可以绕过，说明这是一个黑名单验证，并不是一开始猜想的白名单




ps:这里的一句话木马是我抓包后自己写在图片文件后面的，所以图片文件一定要选小一点的

最后尝试蚁剑进行连接：




依然还是在根目录下找到flag