

2021.3.11 [ACTF2020 新生赛]Upload 1

原创

[weixin_52433547](#) 于 2021-03-11 23:14:10 发布 92 收藏

文章标签：[安全](#)

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/weixin_52433547/article/details/114682450

版权

记录一道文件上传的题目



https://blog.csdn.net/weixin_52433547

进去之后看见这个界面，鼠标移动到灯泡后会提醒你上传文件
我们先试着上传木马，发现限制了只能上传png等格式的文件
我们进行代码审计，发现执行文件上传的代码在这儿

```
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()">
    嘿伙计，你发现它了！
    <input class="input_file" type="file" name="upload_file"/>
    <input class="button" type="submit" name="submit" value="upload"/>
</form>
```

看见onsubmit函数就知道这是个js函数，这个函数限制了上传木马。审查元素删了就行然后上传木马。发现后端还是不让穿php格式的文件。尝试了一下，用了phtml格式，竟然进去了。

Upload Success! Look here~ ./uplo4d/bd914ca4997d34857501cefab0064162.phtml

顺着他给的路径用蚁剑连接，拿到flag