

[ACTF2020 新生赛]Upload 1

原创

祁行 于 2021-03-12 03:58:06 发布 169 收藏

分类专栏: [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/m0_51426816/article/details/114684543

版权



[web](#) 专栏收录该内容

23 篇文章 0 订阅

订阅专栏



在灯泡出发现上传文件, 试了一下只能上传图片
上传图片形式的一句话木马, 抓包修改后缀名为php

```
</div>  
</div>  
nonono~ Bad file
```

改为phtml (还可以尝试PHP, Php, php4, php5)

```
<div style="color:#F00">Upload Success! Look here~  
./uplo4d/74f569c7bc687698e79971a972e36dd6.phtml</div><  
/body>  
</html>
```

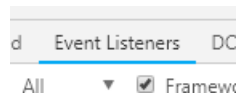
上传成功并得到上传路径, 链接蚁剑在根目录找到flag

```
flag{98e90848-c55e-43cd-bc09-0d3dd11d7b08}
```

看其他WP得知存在前端过滤

```
post" onsubmit="return checkFile()"> == $0
```

可以删除js属性



然后可以直接上传phtml文件