

# BugKu之文件上传测试

原创

D-R0s1 于 2018-07-21 19:44:31 发布 1339 收藏

分类专栏: [CTF WriteUp](#) [文件上传](#) [web](#) 文章标签: [CTF WriteUp](#) [web](#) [文件上传](#) [BurpSuite](#)

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/CliffordR/article/details/81148319>

版权



[CTF WriteUp](#) 同时被 3 个专栏收录

28 篇文章 3 订阅

订阅专栏



[文件上传](#)

2 篇文章 0 订阅

订阅专栏



[web](#)

23 篇文章 2 订阅

订阅专栏

## BugKu文件上传测试

今天在BugKu刷web题的时候, 遇到了一个需要文件上传的题目, 叫做文件上传测试, 这个方法是我之前没有和大家分享过的, 今天和大家分享一下关于文件上传测试这道题目所涉及的有关过程, 我是一个刚入坑的小白, 分享出WriteUp的目的就是和广大刚入门的小白一起进行学习交流, 有误之处还请路过的大牛多多指正。

打开这道题, 题目要求上传一个PHP文件

## 文件上传测试

- 1、请上传PHP文件
- 2、文件上传大小不允许超过1M

浏览... 未选择文件。

Submit

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

我很乖的就找了一个php文件上传了 (php文件可以新建一个记事本改后缀为.php即可) 但是, 上传后发现

非图片文件

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

让上传php却显示不是图片文件，那我们再上传一个图片文件试试

## 非PHP文件

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

上传.jpg后，却显示不是PHP文件。现在我们用BurpSuite来抓包改包试试。使用前一定先进行浏览器的代理。代理后上传文件，

```
POST / HTTP/1.1
Host: 103.238.227.13:10085
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
Referer: http://103.238.227.13:10085/
Content-Type: multipart/form-data; boundary=-----169845912519
Content-Length: 517
Connection: keep-alive
Upgrade-Insecure-Requests: 1

-----169845912519
Content-Disposition: form-data; name="file"; filename="rar000.jpg"
Content-Type: image/jpeg

000d0v0a0n0c0e0d0 0A0r0c0h0i0v0e0 0P0a0s0s0w0o0r0d0 0P0e0c0o0v0e0r0y0 0000o`:00
000 0Z0I0P0/0R0A0R0/0A0C0E0/0A0R0J0 000:0 0E0:0\0c0t0f0\0f0l0a0g0.0r0a0r00
0;`000:0 08070100
0;`000:0 070m0s0 00
0s^Gw00^ (000/00)0:0 0102040,04020800
00*N00000 0:0 08070100
0ASm0Q06R00:0 03080 03070 03010 00
00
0
-----169845912519--
```

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

右击，send to repeater或者是Ctrl + R，

