




BUUCTF: 菜刀666

原创

末初  于 2020-10-02 10:21:34 发布  2826  收藏 3

分类专栏: [CTF_MISC_Writeup](#)

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/mochu777777/article/details/108899933>

版权



[CTF_MISC_Writeup](#) 专栏收录该内容

246 篇文章 45 订阅

订阅专栏

题目地址: <https://buuoj.cn/challenges#%E8%8F%9C%E5%88%80666>

Challenge 615 Solved ×

菜刀666

1

流量分析, 你能找到flag吗注意: 得到的 flag 请包上 flag{} 提交

 0cd3bcfe-bd...

Flag

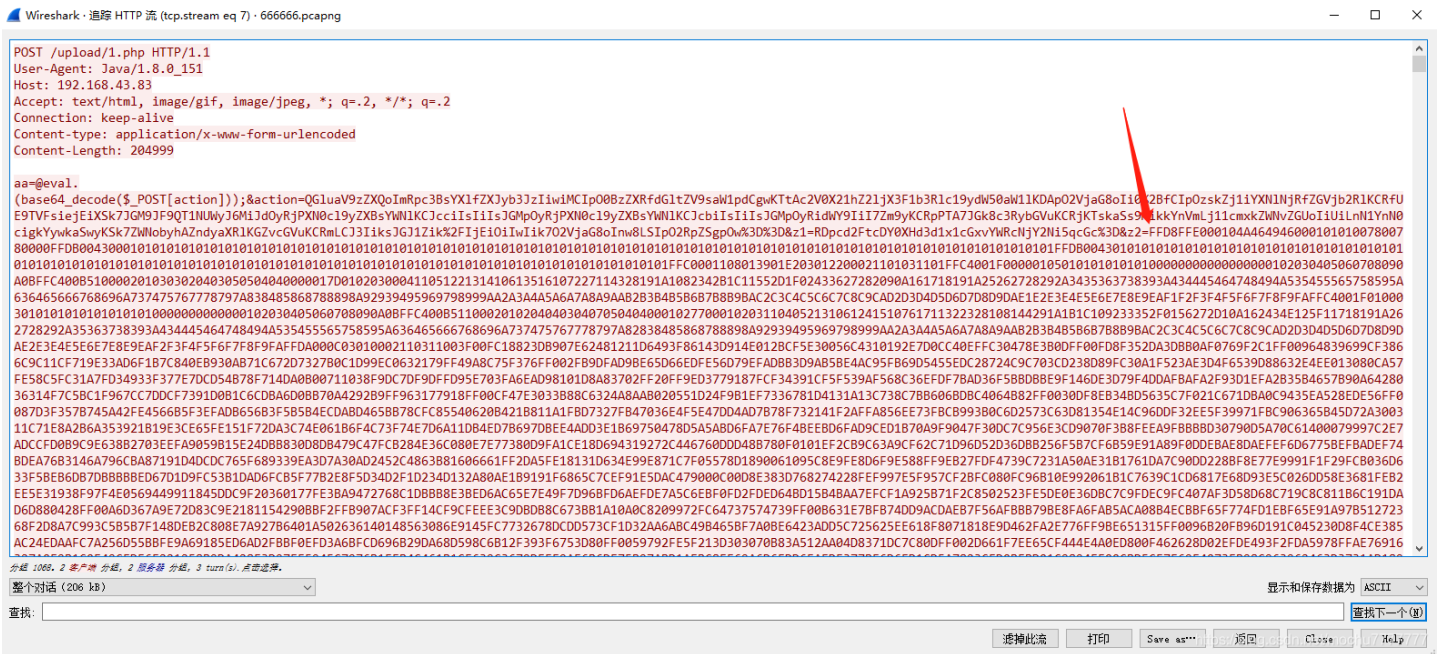
<https://blog.csdn.net/mochu777777>

流量分析

过滤 **POST** 的包

```
http.request.method==POST
```

在 `tcp.stream eq 7` 中发现了大量数据



FF D8 开头 FF D9 结尾，判断为 jpg 图片，将这些十六进制复制出来，以原始文件流写入文件

```
#Author: MoChu7
import struct

a = open("str.txt", "r") #十六进制数据文件
lines = a.read()
res = [lines[i:i+2] for i in range(0, len(lines), 2)]

with open("res.jpg", "wb") as f:
    for i in res:
        s = struct.pack('B', int(i, 16))
        f.write(s)
```

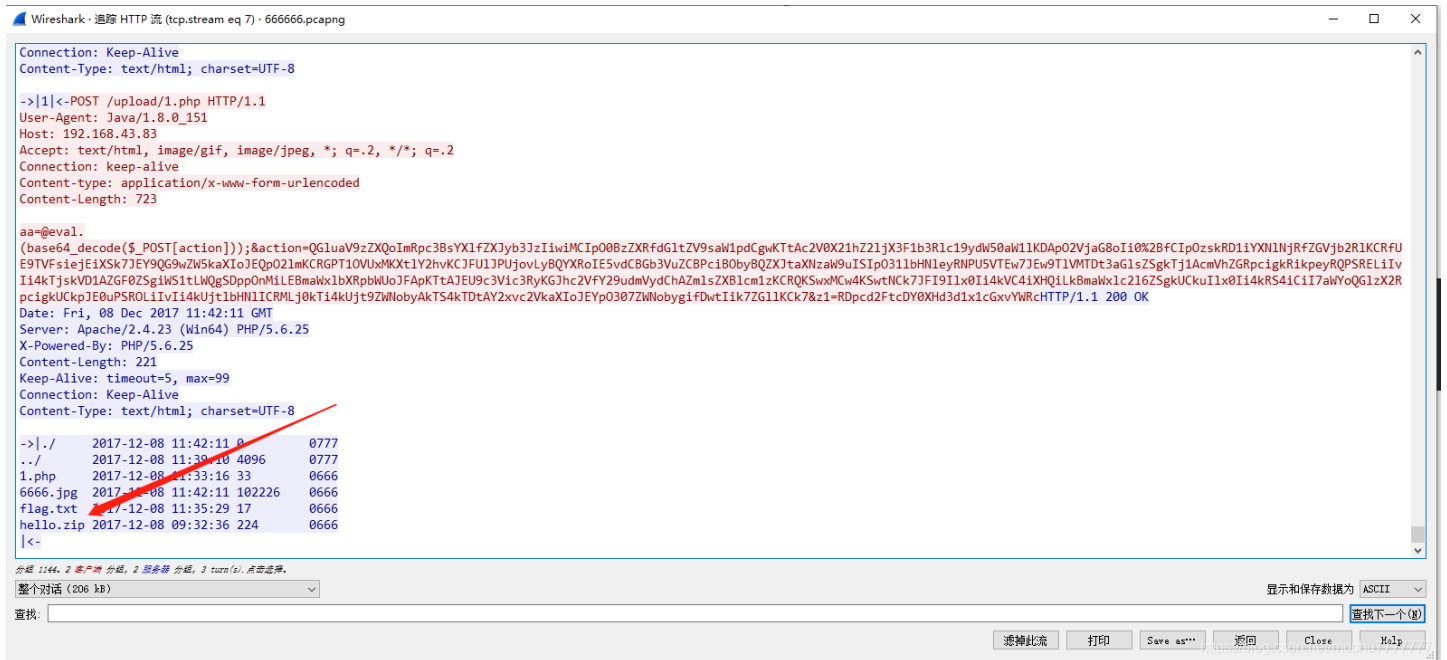


再补一个在网上看到的脚本，感觉更好一点

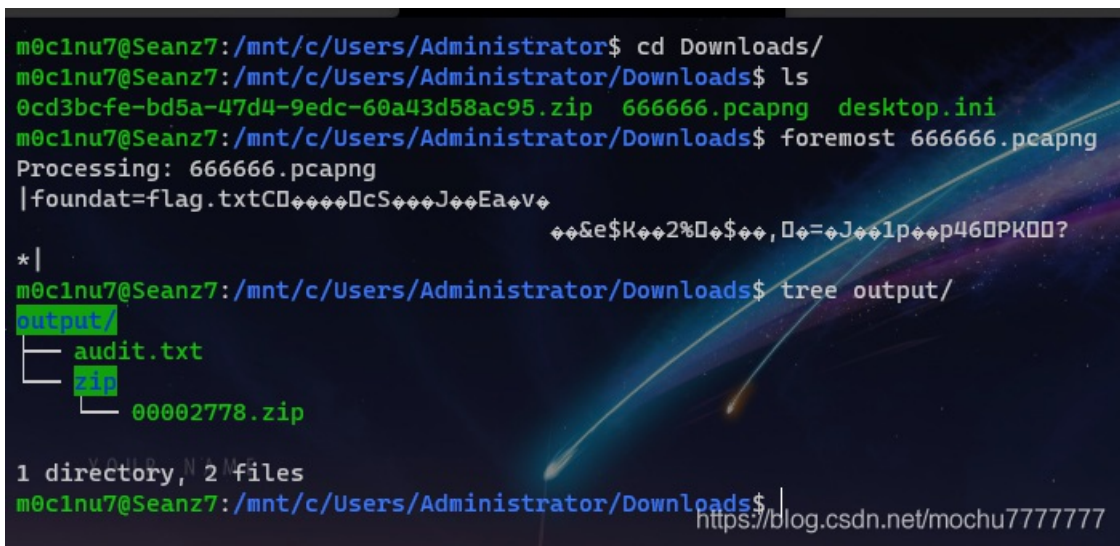
原文地址: https://blog.csdn.net/weixin_44110537/article/details/108350267

```
s='填写16进制数据'
import binascii
out=open('2.jpg', 'wb')
out.write(binascii.unhexlify(s))
out.close()
```

在这个流中还发现了传输了一个 **hello.zip**



foremost 分离流量包，得到一个zip，输入上面图片上的密码



解压得到flag

```
flag{30PwDJ-JP6FzK-koCMAK-VkfWBq-75Un2z}
```