

XCTF-MISC-新手区-base64stego

原创

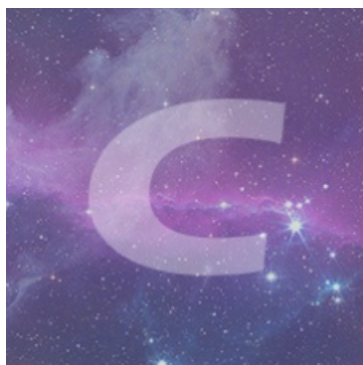
1stPeak 于 2021-06-18 16:34:02 发布 85 收藏

分类专栏: [CTF刷题](#) 文章标签: [XCTF](#)

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_41617034/article/details/118025152

版权



[CTF刷题](#) 专栏收录该内容

87 篇文章 22 订阅

订阅专栏

题目

base64stego

158 最佳Writeup由CTFshow • zEr0_0提供

WP 建议

难度系数: ★★★★★ 5.0

题目来源: olympicCTF

题目描述: 菜狗经过几天的学习, 终于发现了如来十三掌最后一步的精髓

题目场景: 暂无

题目附件: 附件1

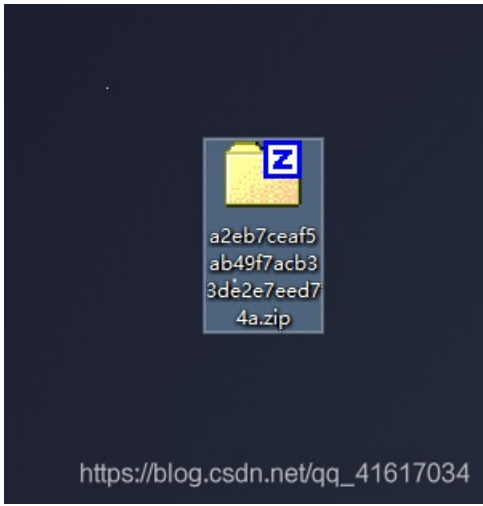
题目已答对

分享wp点赞赚金币哦
马上去写

https://blog.csdn.net/qq_41617034

解题思路

1、下载附件



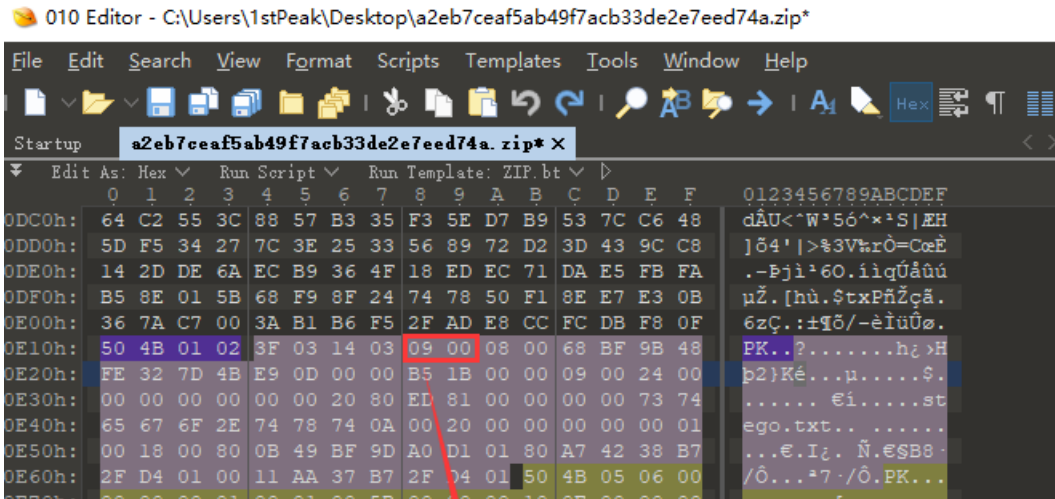
2、查看附件内容



3、直接解压，发现解压失败，存在zip伪加密，那么如何过去stego.txt内容呢

(1) 方法一：

使用010Editor搜索50 4B 01 02，把第九位和第十位改为00并保存，即可成功解压出stego.txt



Template Results - ZIP.bt

Name	Value	Start	Size	Color	C.
struct ZIPFILERECORD record	stego.txt	0h	E10h	Fg: Bg:	
struct ZIPDIRENTRY dirEntry	stego.txt	E10h	5Bh	Fg: Bg:	
struct ZIPENDLOCATOR endLocator		E6Bh	16h	Fg: Bg:	

09第九位, 00第十位, 这里只需要将0改为00即可
<https://blog.csdn.net/qq41617034>

(2) 方法二:

直接在压缩包中打开, 然后复制内容

解题步骤

这是一道base64隐写的题目, 这里用网上的py脚本即可

1、python2脚本

```
# -*- coding: cp936 -*-

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

with open('D:\sw-PyCharmCommunity\PycharmProjects\misc\stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = ''.join(line.split())
        rowb64 = ''.join(stegb64.decode('base64').encode('base64').split())

        offset = abs(b64chars.index(stegb64.replace('=', ''))[-1]) - b64chars.index(rowb64.replace('=', ''))[-1])
        equalnum = stegb64.count('=') #no equalnum no offset

        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)

    print ''.join([chr(int(bin_str[i:i + 8], 2)) for i in xrange(0, len(bin_str), 8)]) #8 位一组
```

```
Base_sixty_four_point_five
Base_sixty_four_point_five
Base_sixty_four_point_five
Base_sixty_four_point_five

D:\sw-PyCharmCommunity\PycharmProjects\misc>
```

2、python3脚本

```
# -*- coding: cp936 -*-

import base64

b64chars = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/'

with open('D:\sw-PyCharmCommunity\PycharmProjects\misc\stego.txt', 'rb') as f:
    bin_str = ''
    for line in f.readlines():
        stegb64 = str(line, "utf-8").strip("\n")
        rowb64 = str(base64.b64encode(base64.b64decode(stegb64)), "utf-8").strip("\n")
        offset = abs(b64chars.index(stegb64.replace('=', ''))[-1]) - b64chars.index(rowb64.replace('=', ''))[-1])
        equalnum = stegb64.count('=') #no equalnum no offset

        if equalnum:
            bin_str += bin(offset)[2:].zfill(equalnum * 2)

    print(''.join([chr(int(bin_str[i:i + 8], 2)) for i in range(0, len(bin_str), 8)])) #8 位一组
```

```
Base_sixty_four_point_five  
PS D:\sw-PyCharmCommunity\PycharmProjects\misc>
```