CUIT CTF WriteUp-BP断点

原创

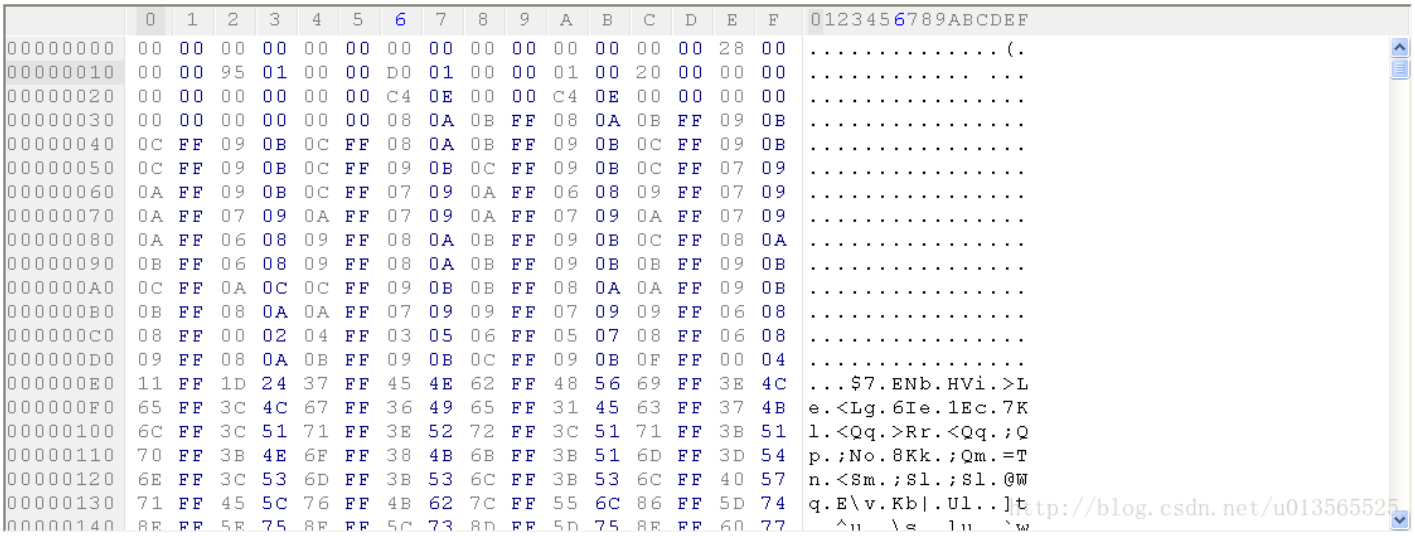
RickGray 于 2014-05-22 15:59:28 发布 1015 收藏
分类专栏： CTF纪实

本文链接：https://blog.csdn.net/u013565525/article/details/26595861

我就不对此题进行任何评价了，在开赛3分钟的时候就发现png了

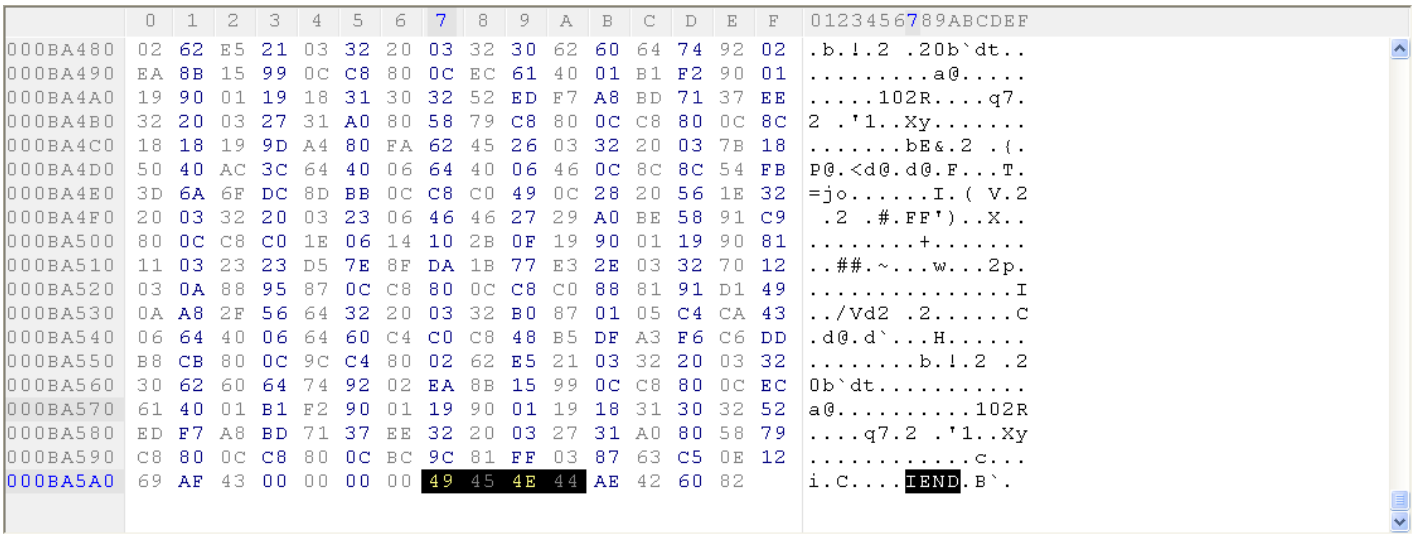
当时由于没想到爆破长宽就没做了，直到第二天早上才搞定，下面说说此题的解题步骤

首先，文件down下来后发现是张无法显示的bm，用winhex或者其他16进制编辑器打开



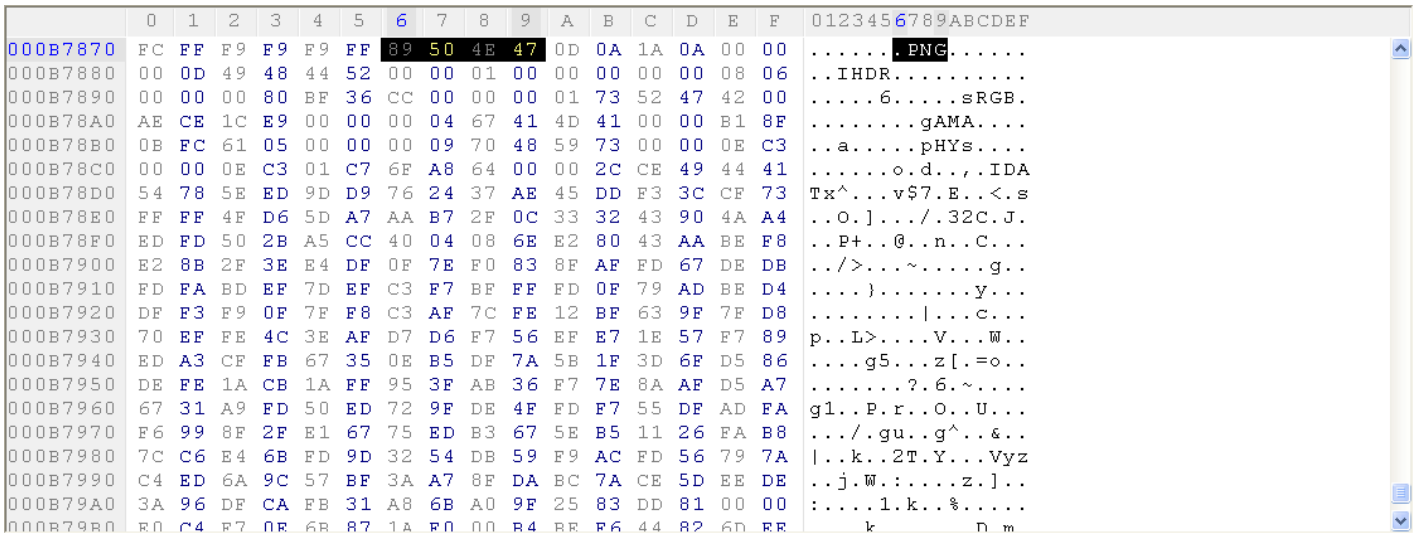
```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
00000000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 00  ..............(.
00000010  00 00 95 01 00 00 D0 01 00 00 01 00 20 00 00 00  ............ ...
00000020  00 00 00 00 00 00 C4 0E 00 00 C4 0E 00 00 00 00  ................
00000030  00 00 00 00 00 00 08 0A 0B FF 08 0A 0B FF 09 0B  ................
00000040  0C FF 09 0B 0C FF 08 0A 0B FF 09 0B 0C FF 09 0B  ................
00000050  0C FF 09 0B 0C FF 09 0B 0C FF 09 0B 0C FF 07 09  ................
00000060  0A FF 09 0B 0C FF 07 09 0A FF 06 08 09 FF 07 09  ................
00000070  0A FF 07 09 0A FF 07 09 0A FF 07 09 0A FF 07 09  ................
00000080  0A FF 06 08 09 FF 08 0A 0B FF 09 0B 0C FF 08 0A  ................
00000090  0B FF 06 08 09 FF 08 0A 0B FF 09 0B 0B FF 09 0B  ................
000000A0  0C FF 0A 0C 0C FF 09 0B 0B FF 08 0A 0A FF 09 0B  ................
000000B0  0B FF 08 0A 0A FF 07 09 09 FF 07 09 09 FF 06 08  ................
000000C0  08 FF 00 02 04 FF 03 05 06 FF 05 07 08 FF 06 08  ................
000000D0  09 FF 08 0A 0B FF 09 0B 0C FF 09 0B 0F FF 00 04  ................
000000E0  11 FF 1D 24 37 FF 45 4E 62 FF 48 56 69 FF 3E 4C  ...$7.ENb.HVi.>L
000000F0  65 FF 3C 4C 67 FF 36 49 65 FF 31 45 63 FF 37 4B  e.<Lg.6Ie.1Ec.7K
00000100  6C FF 3C 51 71 FF 3E 52 72 FF 3C 51 71 FF 3B 51  l.<Qq.>Rr.<Qq.;Q
00000110  70 FF 3B 4E 6F FF 38 4B 6B FF 3B 51 6D FF 3D 54  p.;No.8Kk.;Qm.=T
00000120  6E FF 3C 53 6D FF 3B 53 6C FF 3B 53 6C FF 40 57  n.<Sm.;Sl.;Sl.@W
00000130  71 FF 45 5C 76 FF 4B 62 7C FF 55 6C 86 FF 5D 74  q.E\v.Kb|.Ul..]t
00000140  8E FF 5E 75 8F FF 5C 73 8D FF 5D 75 8E FF 60 77  ..^u..\s..]u..`w
```


搜索半天，在数据尾部发现了IEND



```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
000BA480  02 62 E5 21 03 32 20 03 32 30 62 60 64 74 92 02  .b.!.2 .20b`dt..
000BA490  EA 8B 15 99 0C C8 80 0C EC 61 40 01 B1 F2 90 01  .........a@.....
000BA4A0  19 90 01 19 18 31 30 32 52 ED F7 A8 BD 71 37 EE  .....102R....q7.
000BA4B0  32 20 03 27 31 A0 80 58 79 C8 80 0C C8 80 0C 8C  2 .'1..Xy........
000BA4C0  18 18 19 9D A4 80 FA 62 45 26 03 32 20 03 7B 18  .......bE&.2 .{.
000BA4D0  50 40 AC 3C 64 40 06 64 40 06 46 0C 8C 8C 54 FB  P@.<d@.d@.F...T.
000BA4E0  3D 6A 6F DC 8D BB 0C C8 C0 49 0C 28 20 56 1E 32  =jo......I.( V.2
000BA4F0  20 03 32 20 03 23 06 46 46 27 29 A0 BE 58 91 C9  .2 .#.FF')..X..
000BA500  80 0C C8 C0 1E 06 14 10 2B 0F 19 90 01 19 90 81  ........+.......
000BA510  11 03 23 23 D5 7E 8F DA 1B 77 E3 2E 03 32 70 12  ..##.~...w...2p.
000BA520  03 0A 88 95 87 0C C8 80 0C C8 C0 88 81 91 D1 49  ...............I
000BA530  0A A8 2F 56 64 32 20 03 32 B0 87 01 05 C4 CA 43  ../Vd2 .2......C
000BA540  06 64 40 06 64 60 C4 C0 C8 48 B5 DF A3 F6 C6 DD  .d@.d`...H......
000BA550  B8 CB 80 0C 9C C4 80 02 62 E5 21 03 32 20 03 32  ........b.!.2 .2
000BA560  30 62 60 64 74 92 02 EA 8B 15 99 0C C8 80 0C EC  0b`dt...........
000BA570  61 40 01 B1 F2 90 01 19 90 01 19 18 31 30 32 52  a@..........102R
000BA580  ED F7 A8 BD 71 37 EE 32 20 03 27 31 A0 80 58 79  ....q7.2 .'1..Xy
000BA590  C8 80 0C C8 80 0C BC 9C 81 FF 03 87 63 C5 0E 12  ............c...
000BA5A0  69 AF 43 00 00 00 00 49 45 4E 44 AE 42 60 82     i.C....IEND.B`.
```

对该标记只有PNG图片才有，果断搜了下有没有PNG文件头，发现还真有，直接将PNG整个部分提取出来，保存为aaa.png



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
000B7870 FC FF F9 F9 F9 FF 89 50 4E 47 0D 0A 1A 0A 00 00 ......PNG......
000B7880 00 0D 49 48 44 52 00 00 01 00 00 00 00 00 08 06 ..IHDR..........
000B7890 00 00 00 80 BF 36 CC 00 00 00 01 73 52 47 42 00 .....6.....sRGB.
000B78A0 AE CE 1C E9 00 00 00 04 67 41 4D 41 00 00 B1 8F ........gAMA....
000B78B0 0B FC 61 05 00 00 00 09 70 48 59 73 00 00 0E C3 ..a.....pHYs....
000B78C0 00 00 0E C3 01 C7 6F A8 64 00 00 2C CE 49 44 41 ......o.d..,.IDA
000B78D0 54 78 5E ED 9D D9 76 24 37 AE 45 DD F3 3C CF 73 Tx^...v$7.E..<.s
000B78E0 FF FF 4F D6 5D A7 AA B7 2F 0C 33 32 43 90 4A A4 ..O.].../.32C.J.
000B78F0 ED FD 50 2B A5 CC 40 04 08 6E E2 80 43 AA BE F8 ..P+..@..n..C...
000B7900 E2 8B 2F 3E E4 DF 0F 7E F0 83 8F AF FD 67 DE DB ../>...~.....g..
000B7910 FD FA BD EF 7D EF C3 F7 BF FF FD 0F 79 AD BE D4 ....}.......y...
000B7920 DF F3 F9 0F 7F F8 C3 AF 7C FE 12 BF 63 9F 7F D8 ........|...c...
000B7930 70 EF FE 4C 3E AF D7 D6 F7 56 EF E7 1E 57 F7 89 p..L>....V...W..
000B7940 ED A3 CF FB 67 35 0E B5 DF 7A 5B 1F 3D 6F D5 86 ....g5...z[.=o..
000B7950 DE FE 1A CB 1A FF 95 3F AB 36 F7 7E 8A AF D5 A7 .......?.6.~....
000B7960 67 31 A9 FD 50 ED 72 9F DE 4F FD F7 55 DF AD FA g1..P.r..O..U...
000B7970 F6 99 8F 2F E1 67 75 ED B3 67 5E B5 11 26 FA B8 .../.gu..g^..&..
000B7980 7C C6 E4 6B FD 9D 32 54 DB 59 F9 AC FD 56 79 7A |..k..2T.Y...Vyz
000B7990 C4 ED 6A 9C 57 BF 3A A7 8F DA BC 7A CE 5D EE DE ..j.W.:....z.]..
000B79A0 3A 96 DF CA FB 31 A8 6B A0 9F 25 83 DD 81 00 00 :....1.k..%.....
000B79B0 E0 C4 E7 0E 6B 87 1A E0 00 B4 BE E6 44 82 6D EE     k       D m
```

打开aaa.png发现什么都没有，果断继续16进制编辑

分析和检查了一些东西后，发现它的长宽有问题

然后就意识到可能要调整长宽，又想到一般出题人不会更高CRC（改了就吐血了~！）

So果断写个脚本Crack长宽，代码如下

```
#!/usr/bin/env python
# -*- coding: utf-8 -*-
__author__ = 'RickGray'
import zlib
import struct


crc32key = 0x80BF36CC # target CRC
# 49484452000001000000000000806000000
for i in range(0, 1366):
    width = struct.pack('>i', i)
    for j in range(0, 1366):
        hieght = struct.pack('>i', j)  # pack to 4 bytes with Big-Endian
        # CRC: CD952277
        s = '\x49\x48\x44\x52'  #  IHDR
        s += width  # width 4 bytes
        s += hieght  # hieght 4 bytes
        s += '\x08\x06\x00\x00\x00'

        crc32result = zlib.crc32(s) & 0xffffffff

        if crc32result == crc32key:
            print 'Crack over!'
            print 'Width: ', struct.unpack('>i', width)[0]
            print 'Hieght: ', struct.unpack('>i', hieght)[0]

raw_input('\nFinished!')
```

运行该脚本后，很快就Crack出长宽400×400

更改aaa.png长宽后，果断地弹出了flag：*T7i5Is7h3R3411yK3y_!@#()*

key:T7i5Is7h3R3411yK3y_!@#()

http://blog.csdn.net/u013565525