08067ctf-Misc-SimpleRAR-WriteUp

原创

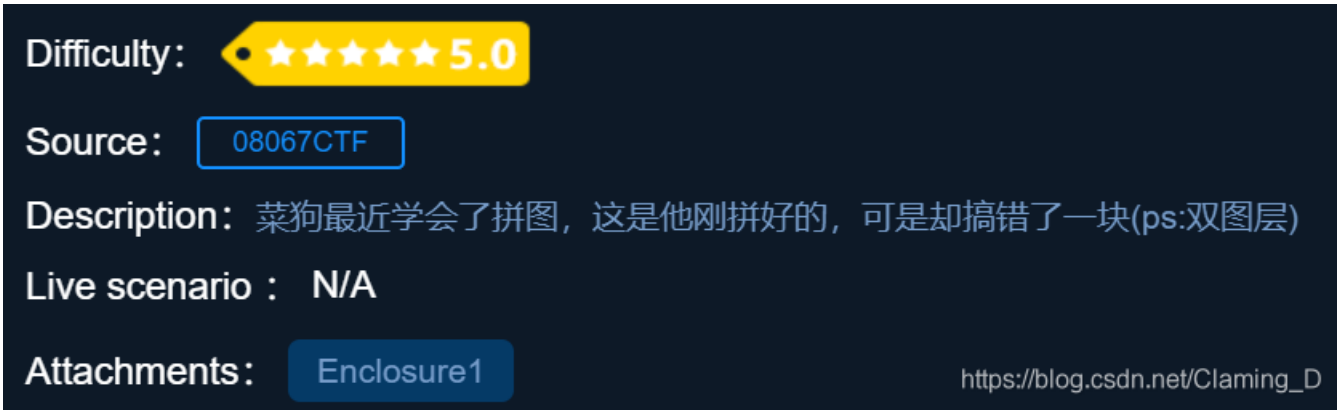
萌萌哒的baola 于 2020-05-23 16:53:04 发布 382 收藏 2

分类专栏： ctf题解

本文链接：https://blog.csdn.net/Claming_D/article/details/106302596

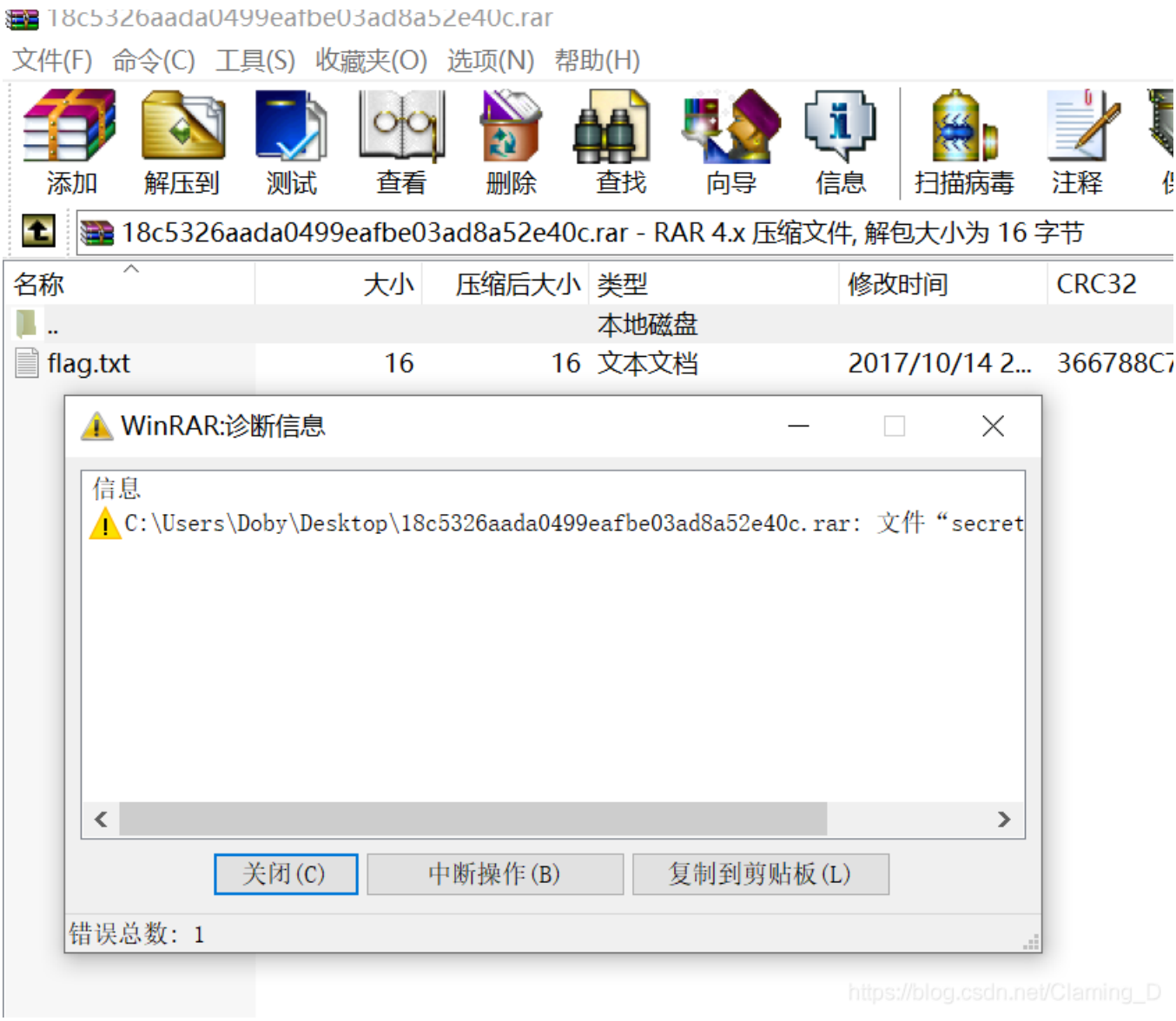
文章目录

SimpleRAR

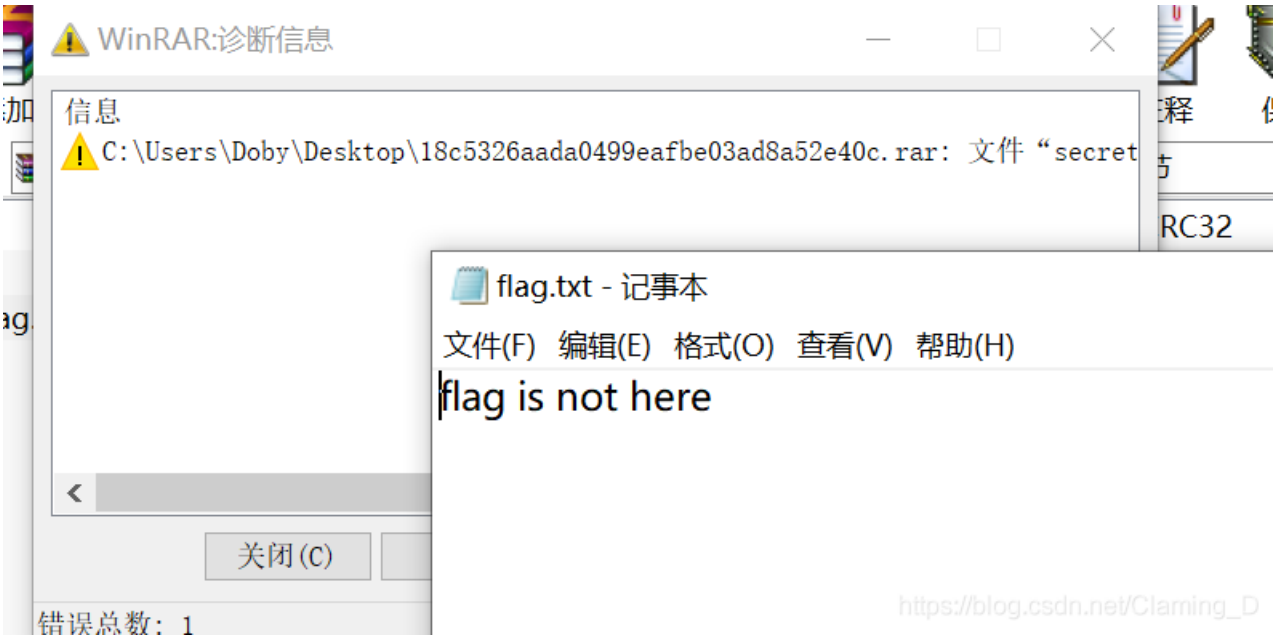


题目分析

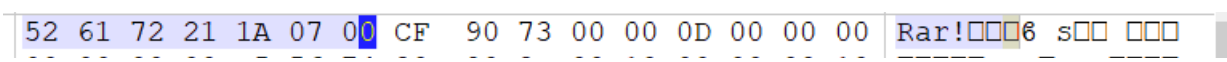
题目给了一个RAR文件，用winrar软件打开，有警告信息。



再此条件下打开flag.txt，里面没有有效信息。

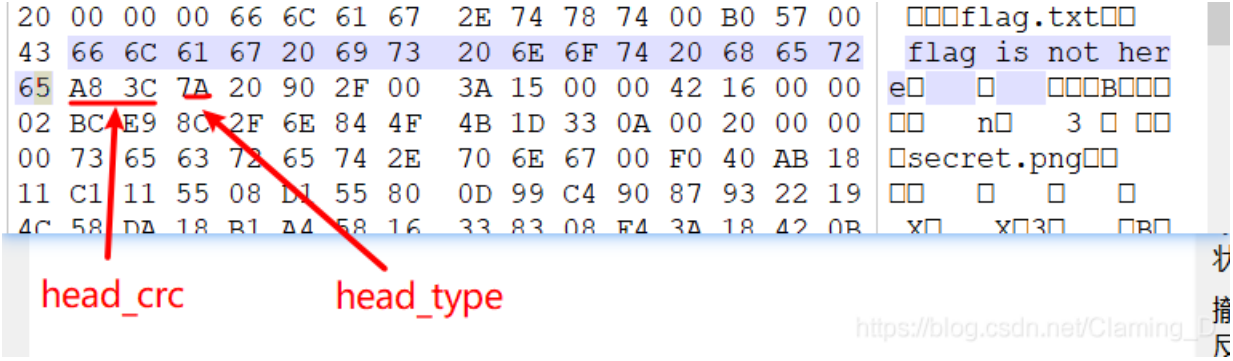


由于警告信息我们可以想到，rar文件可能存在问题，用winhex打开看一下码流

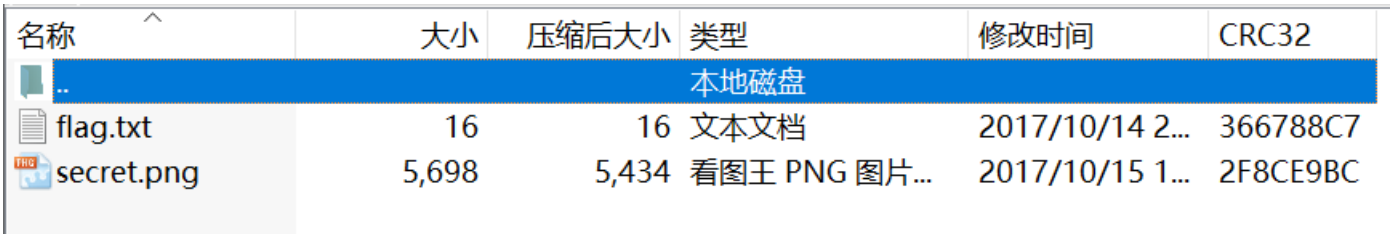


```
00 00 00 00 D5 56 74 20  90 2D 00 10 00 00 00 10
00 00 00 02 C7 88 67 36  6D BB 4E 4B 1D 30 08 00
20 00 00 00 66 6C 61 67  2E 74 78 74 00 B0 57 00
43 66 6C 61 67 20 69 73  20 6E 6F 74 20 68 65 72
65 A8 3C 7A 20 90 2F 00  3A 15 00 00 42 16 00 00
02 BC E9 8C 2F 6E 84 4F  4B 1D 33 0A 00 20 00 00
00 73 65 63 72 65 74 2E  70 6E 67 00 F0 40 AB 18
11 C1 11 55 08 D1 55 80  0D 99 C4 90 87 93 22 19
4C 58 DA 18 B1 A4 58 16  33 83 08 F4 3A 18 42 0B
04 05 85 96 21 AB 1A 43  08 66 EC 61 0F A0 10 21
AB 3D 02 80 B0 10 90 C5  8D A1 1E 84 42 B0 43 29
08 10 DA 0F 23 99 CC F3  9D C4 85 86 67 73 39 DE
47 63 91 DE C4 77 ED A8  DC 46 F4 C5 54 CD 55 6A
AA A3 5F CD 6E 77 3B 8D  EF 7A 99 A9 A9 8F D5 3F
0A AA F9 55 7F 02 9E A2  9C 86 88 CC 59 CC FF 0C
57 34 7B 8B 8F F9 C0 F7  E6 30 E3 25 60 55 58 00
```

文件头和文件尾均正确，我们看到了码流中有png文件标识，但是在我们打开文件时并没有看到这个png文件。rar文件由各种块组成，我猜测可能是png文件所在的文件块出错了，检查一下png文件所在的块，看是否有损坏。png文件所在块的块头在上一个块的结尾，上一个块是txt类型的文件块，txt文件尾在txt内容结束的位置。

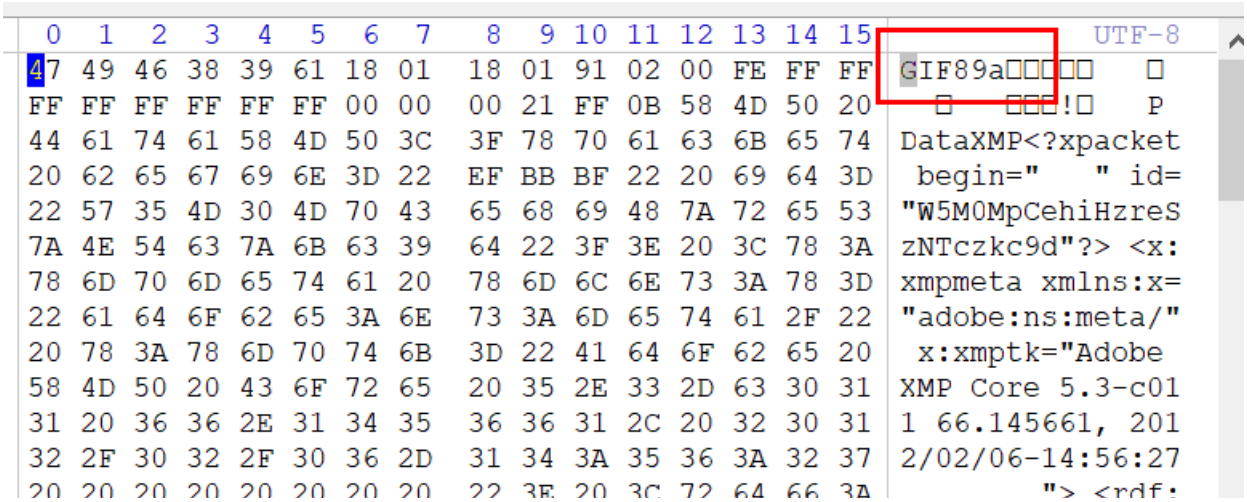


可见head_type的值是错误的，这是一个文件块，所以head_type的值是0x74，我们修改完后，就可以正常打开rar文件



名称	大小	压缩后大小	类型	修改时间	CRC32
..			本地磁盘		
flag.txt	16	16	文本文档	2017/10/14 2...	366788C7
secret.png	5,698	5,434	看图王 PNG 图片...	2017/10/15 1...	2F8CE9BC

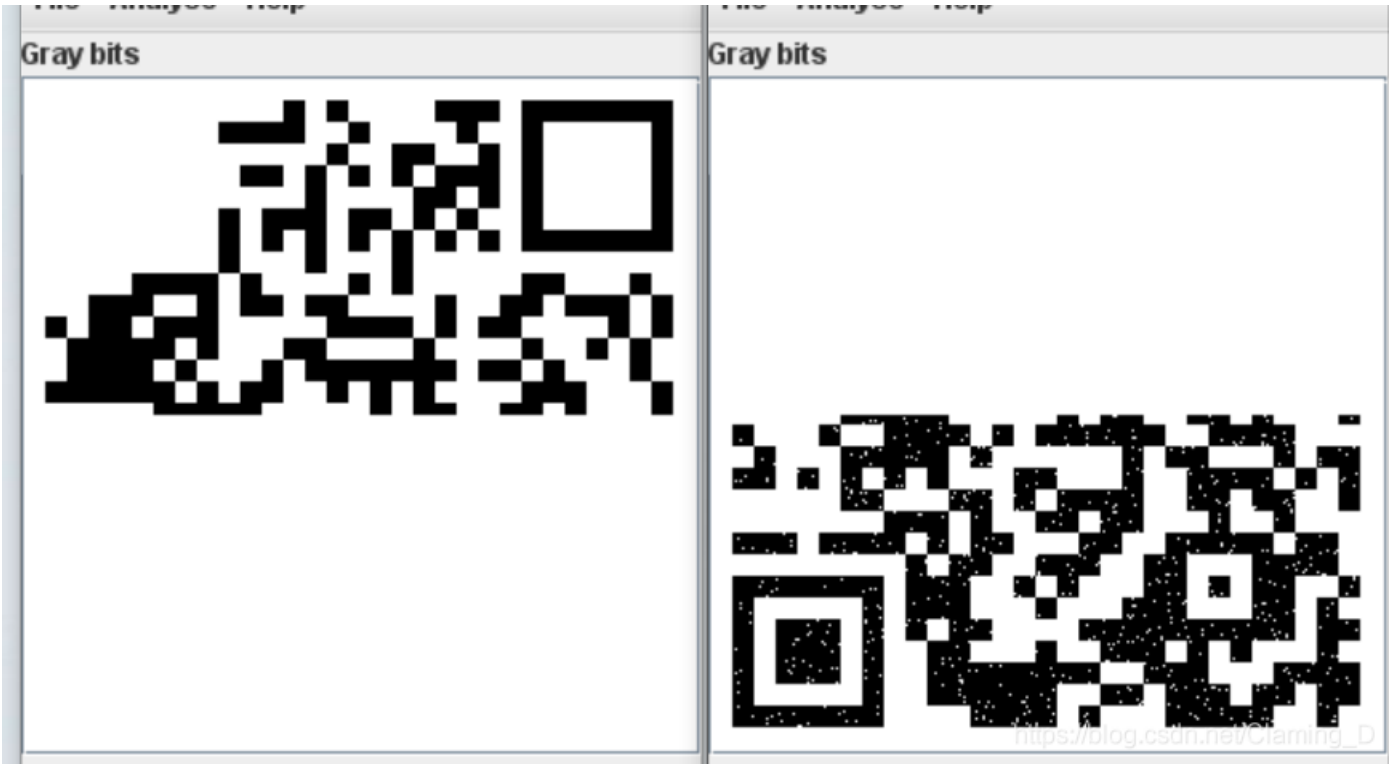
打开这个png文件，全是空白没有可利用信息，用winhex打开看看



```
 0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15          UTF-8
47 49 46 38 39 61 18 01  18 01 91 02 00 FE FF FF  GIF89a
FF FF FF FF FF FF 00 00  00 21 FF 0B 58 4D 50 20  !  XMP
44 61 74 61 58 4D 50 3C  3F 78 70 61 63 6B 65 74  DataXMP<?xpacket
20 62 65 67 69 6E 3D 22  EF BB BF 22 20 69 64 3D   begin="  " id=
22 57 35 4D 30 4D 70 43  65 68 69 48 7A 72 65 53  "W5M0MpCehiHzreS
7A 4E 54 63 7A 6B 63 39  64 22 3F 3E 20 3C 78 3A  zNTczkc9d"?> <x:
78 6D 70 6D 65 74 61 20  78 6D 6C 6E 73 3A 78 3D  xmpmeta xmlns:x=
22 61 64 6F 62 65 3A 6E  73 3A 6D 65 74 61 2F 22  "adobe:ns:meta/"
20 78 3A 78 6D 70 74 6B  3D 22 41 64 6F 62 65 20   x:xmptk="Adobe
58 4D 50 20 43 6F 72 65  20 35 2E 33 2D 63 30 31  XMP Core 5.3-c01
31 20 36 36 2E 31 34 35  36 36 31 2C 20 32 30 31  1 66.145661, 201
32 2F 30 32 2F 30 36 2D  31 34 3A 35 36 3A 32 37  2/02/06-14:56:27
20 20 20 20 20 20 20 20  22 3E 20 3C 72 64 66 3A          "> <rdf:
```

```
52 44 46 20 78 6D 6C 6E  73 3A 72 64 66 3D 22 68  RDF xmlns:rdf="h
74 74 70 3A 2F 2F 77 77  77 2E 77 33 2E 6F 72 67  ttp://www.w3.org
2F 31 39 39 39 2F 30 32  2F 32 32 2D 72 64 66 2D  /1999/02/22-rdf-
73 79 6E 74 61 78 2D 6E  73 23 22 3E 20 3C 72 64  syntax-ns#"> <rd
```

可以看到这是个gif文件，于是修改文件扩展为.gif。gif内容也是空白，于是用stegsolve查看，在灰色位（gray bits）看到了半个二维码，题目中提示双图层，可以用ps打开看一下图层，我们发现有两个图层，将两个空白图层导出为png格式。用stegsolve查看，在灰度位中看到两个残缺的二维码。



用ps将二维码合并，合并后发现这个二维码的位置探测图形有残缺，这里我用Photoshop将这个二维码的位置探测额图形补充完整，得到如下所示的二维码

> 位置探测图形：由三个黑白相间的大正方形嵌套组成，分别位于二维码左上角、右上角、左下角，目的是为了确定二维码的大小和位置。

扫描二维码得到

总结

了解RAR、png、gif的文件结构，会分析码流。
了解图层的的概念。
二维码的位置探测图形要会补全。
会使用stegsolve

参考资料

二维码详解
百度百科-图层
RAR文件格式分析

工具下载

链接：https://pan.baidu.com/s/1QrApFK720tVcBvY9J83lQQ
提取码：w3mp