

BUGKU misc--细心的大象--writeup

原创

SankyOu 于 2017-08-14 16:03:10 发布 3725 收藏

文章标签: [BUGKU misc ctf](#)

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/SankyOu/article/details/77162806>

版权

题目打开

题目 6 Solves

细心的大象

100

链接: <https://pan.baidu.com/s/1i5ehlnj> 密码: gprr

Key SUBMIT

<http://blog.csdn.net/SankyOu>

下载下来后是一张jpg图片, 用010editor查看搜索jpg文件尾FFD9发现后面有Rar!标志, 想必图片最后有个rar压缩包。

```
61:8870h: F1 9C BE DE 00 CE 48 AF A4 7F 65 8F F9 14 7C 1F fice%B.ÎH̄m.e.ù.j.
61:8880h: FF 00 64 F6 C3 FF 00 45 8A F2 2F DB C7 FE 44 6B ŷ.dôÃÿ.Ešô/ÛÇpDk
61:8890h: 5F FA EF 17 FE 86 D5 C2 B3 9C C3 11 9D F2 D5 A8 úi.p+ôÃ'œÃ..ôô~
61:88A0h: DA ED F3 3D 4A 78 5A 3C AA 56 D6 DF A9 FF D9 52 Ūiô=JxZ<*VÔB@ÿWR
61:88B0h: 61 72 21 1A 07 00 CF 90 73 00 00 0D 00 00 00 00 rar!...î.s.....
61:88C0h: 00 00 00 86 AB 74 24 94 32 00 60 3F 00 00 0B 45 ...t&t$"2.>?...E
61:88D0h: 00 00 02 DE 05 A8 4E 56 B3 C7 4A 1D 33 05 00 20 ...B."NV'ÇJ.3..
61:88E0h: 20 00 00 32 2E 70 6E 67 79 6C DB 54 79 3C 3D 4A ...2.pngylÛTy<=J
61:88F0h: 00 B0 DA 9F 6E 72 DF 0A 39 31 60 2A DD E1 EA BD .°ÛÿnrB.91`*ÿáé%
```

将包括Rar!在内的后面所有16进制拷贝, 保存成rar文件之后, 解压时发现需要密码, 因为没有很好的爆破rar压缩包的工具, 而且按理密码应该会藏在某个地方, 于是再回到原文件尝试寻找密码.....

在前面的FFD9标志后发现很多明文字符串,

```
6720h: 3E 29 22 86 55 22 35 32 38 D8 19 49 3C E3 38 C0 >)" +U"5280.I<ã8ã
6730h: E3 9A 8E 66 60 8C 5D 3C E6 0F 81 2F 01 87 72 0A äšžf'€]<æ../.tr.
6740h: E3 D3 A7 1E 95 29 EA 44 65 73 FF D9 FF E1 0B B0 äôs.*)âDesÿÜÿá.°
6750h: 68 74 74 70 3A 2F 2F 6E 73 2E 61 64 6F 62 65 2E http://ns.adobe.
6760h: 63 6F 6D 2F 78 61 70 2F 31 2E 30 2F 00 3C 3F 78 com/xap/1.0/.<?x
6770h: 70 61 63 6B 65 74 20 62 65 67 69 6E 3D 27 EF BB packet begin='i»
6780h: BF 27 20 69 64 3D 27 57 35 4D 30 4D 70 43 65 6 z' id='W5MOMpCeh
6790h: 69 48 7A 72 65 53 7A 4E 54 63 7A 6B 63 39 64 27 iHzreSzNTczkc9d'
67A0h: 3F 3E 0D 0A 3C 78 3A 78 6D 70 6D 65 74 61 20 78 ?>..<x:xmpmeta x
67B0h: 6D 6C 6E 73 3A 78 3D 22 61 64 6F 62 65 3A 6E 73 mlns:x="adobe:ns
67C0h: 3A 6D 65 74 61 2F 22 3E 3C 72 64 66 3A 52 44 46 :meta/"><rdf:RDF
67D0h: 20 78 6D 6C 6E 73 3A 72 64 66 3D 22 68 74 74 70 xmlns:rdf="http
67E0h: 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67 2F 31 39 ://www.w3.org/19
```

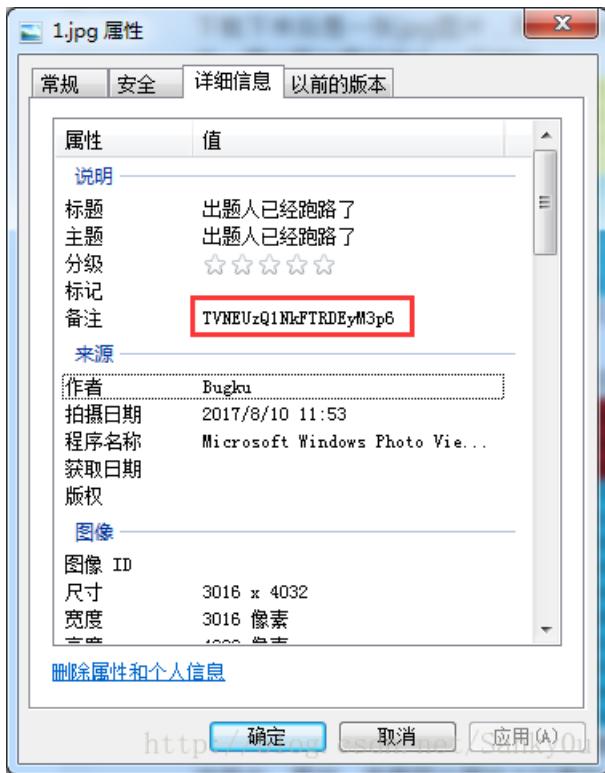
开始不知道什么意思, 搜索了一番知道是图片信息, 类似于下面的解释,

我知道exif是拍摄信息，iptc是关键字、版权信息。

某张照片的xmp信息

```
<?xpacket begin='? id='W5M0MpCehiHzreSzNTczkc9d'?>
<x:xmpmeta xmlns:x='adobe:ns:meta/' x:xmpTk='XMP toolkit 3.0-28, framework 1.6'>
<rdf:RDF xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#' xmlns:iX='http://ns.adobe.com/iX/1.0/'>
<rdf:description rdf:about='uuid:fdd7dc92-d11d-11d8-9d5f-f1a9741e31b0'
xmlns:exif='http://ns.adobe.com/exif/1.0/'>
<exif:ExposureTime>1/250</exif:ExposureTime>
<exif:FNumber>80/10</exif:FNumber>
<exif:ExifVersion>0220</exif:ExifVersion>
<exif:DateTimeOriginal>2004-06-21T17:46:31+08:00</exif:DateTimeOriginal>
<exif:DateTimeDigitized>2004-06-21T17:46:31+08:00</exif:DateTimeDigitized>
<exif:CompressedBitsPerPixel>3/1</exif:CompressedBitsPerPixel>
```

于是想到了图片隐写可能隐在图片信息中，果然，查看图片属性之后看到下面信息。



之后就简单了，备注里面的是base64编码后的压缩包密码，压缩包解压得到一张png图片，后面就和隐写2的那题一样了，修改png图片高度并修改CRC校验值，之后就可以看到图片里的flag。

说明：隐写2那题的做法在我的[上一篇博客](#)有提到。