BUGKU misc--细心的大象--writeup

原创

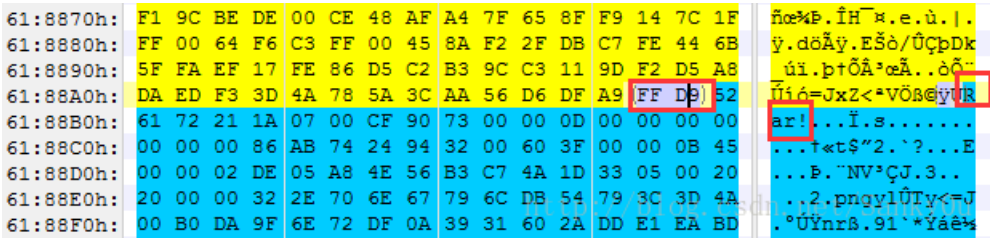
Sanky0u 于 2017-08-14 16:03:10 发布 3725 收藏

文章标签： BUGKU misc ctf

本文链接：https://blog.csdn.net/Sanky0u/article/details/77162806

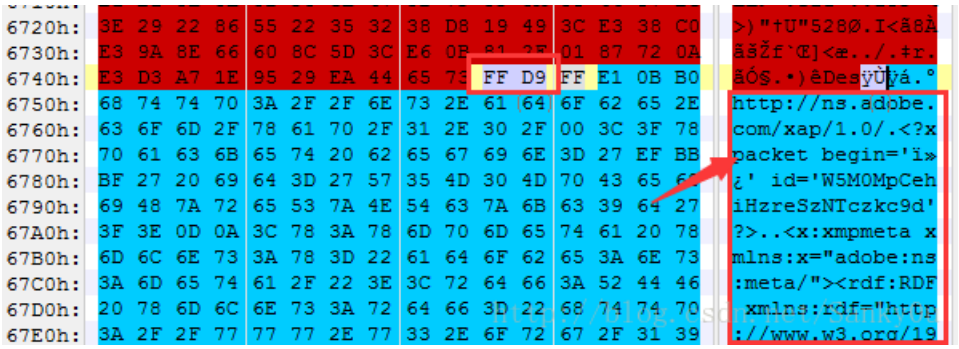
题目打开

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。



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，



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，

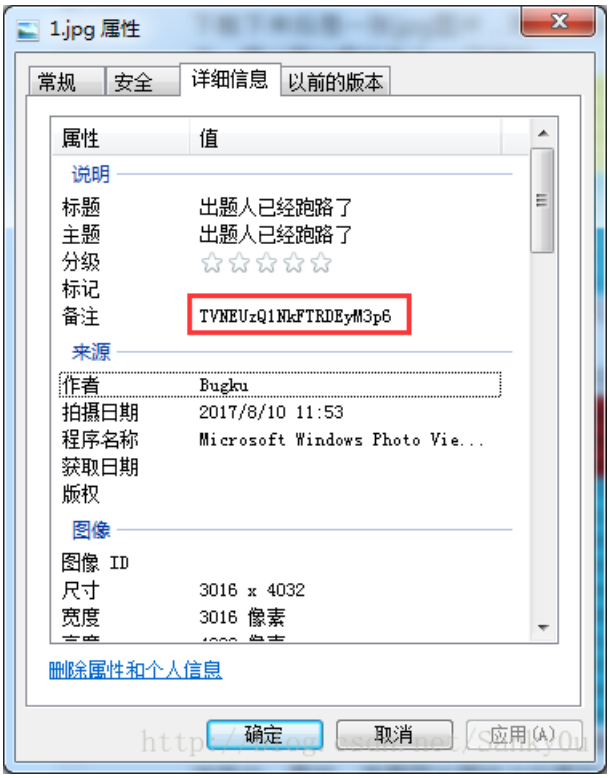
我知道exif是拍摄信息，iptc是关键字、版权信息。

某张照片的xmp信息

```
<?xpacket begin='锘? 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。