

MISC-bugku一个普通的压缩包

原创

[Alikas](#) 于 2019-04-18 22:25:03 发布 1636 收藏 3

分类专栏: [MISC](#) 文章标签: [MISC writeup bugku](#)

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/q83182034/article/details/89389702>

版权



[MISC 专栏收录该内容](#)

1 篇文章 0 订阅

订阅专栏

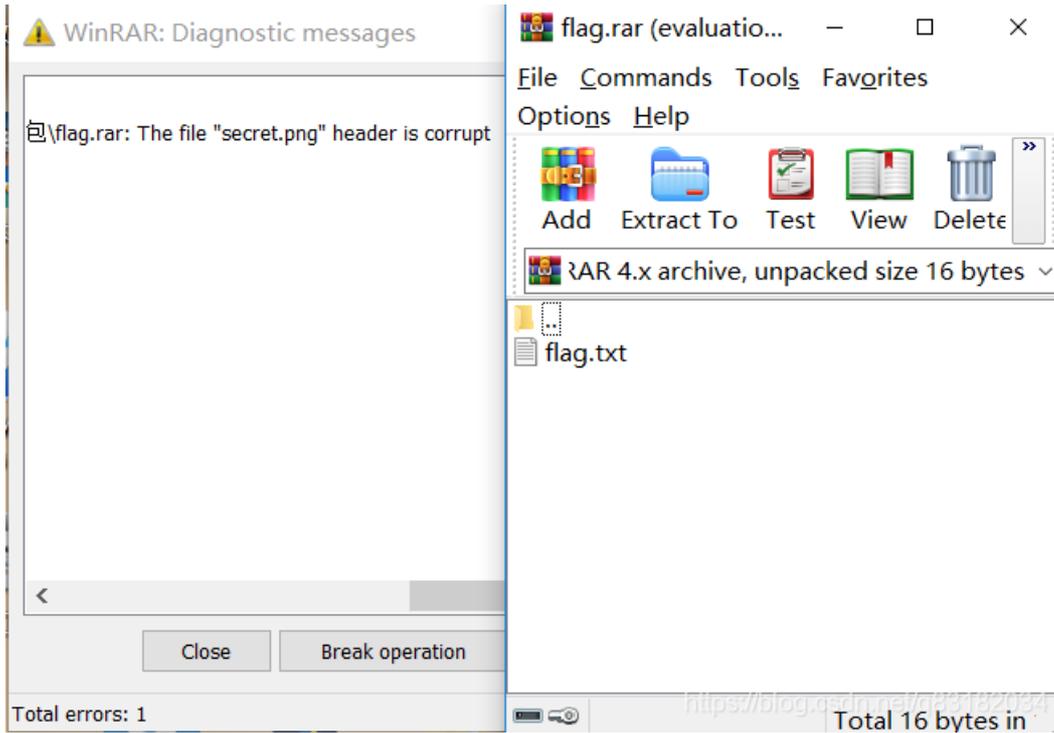
Alikas-0x0A

题目: [MISC-bugku一个普通的压缩包](#)

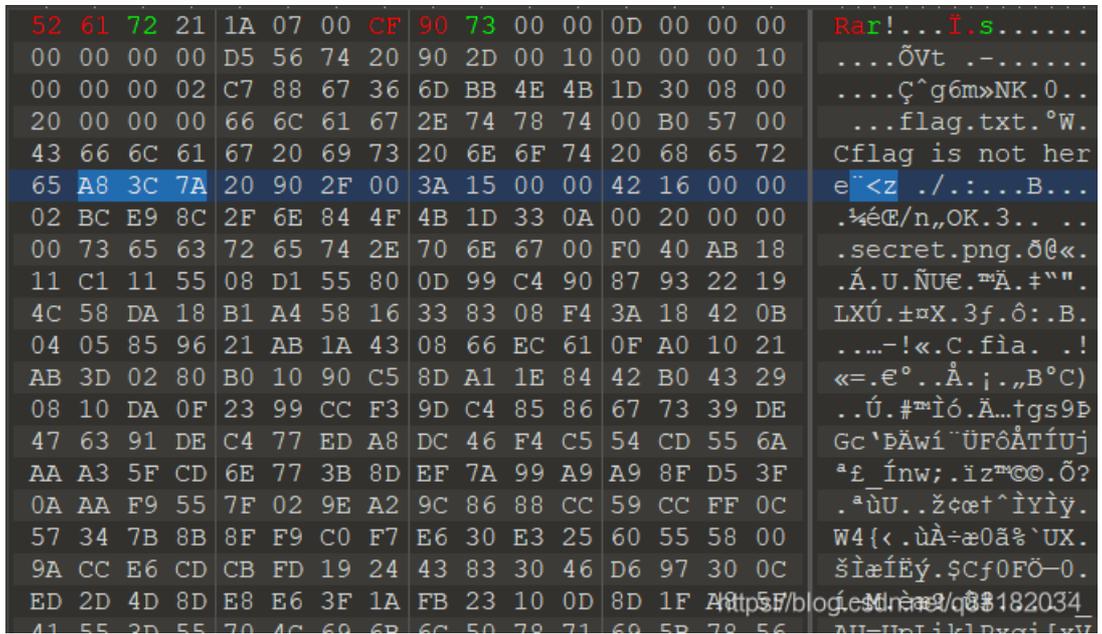
这是一道在Xp0intCTF的题, 名为“一个普通的压缩包”(一看就不普通好嘛! (ノ'-'') (ノ'-'') BugkuCTF里也有收录, 下面写写心路历程.....

先下文件包得到zip.zip, 直接拖进010editor中, 看文件的头尾结构是否有问题, 根据文件头判断这是个zip压缩的文件, 改后缀名zip, 直接解压得到名为“一个普通的压缩包”的文件夹。

打开，得到一个名为flag.rar的压缩包，直接打开，就出事儿了，报错说secret.png文件头损坏。打开flag.txt后.....嗯，flag应该藏在secret.png里。尝试rar修复工具无果后，决定用010editor手动修复。



拉进010editor，检查rar文件头，没问题，那就是文件头损坏咯。检查文件头，发现0x74位置被修改为0x7A，故修改还原，检查计算CRC32，就是A83C那就不用改咯。（知道这么修改的原因在文末参考文件里0.0）返回打开flag.rar可以看见secret.png已经出来啦！

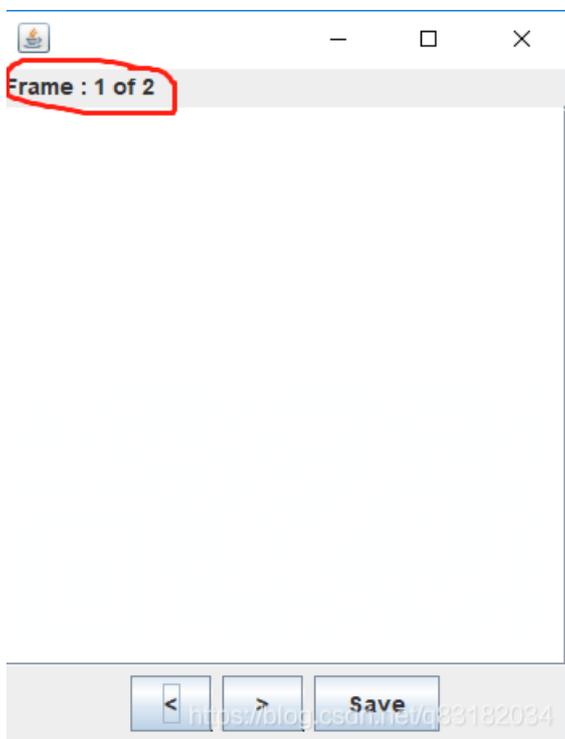


你以为这样就完了，没想到一打开白花花一片 ((°Д°) ㄟ(ㄟ ㄟ)，拉进010editor，发现应该是个gif文件，修改后缀，依旧白花花....

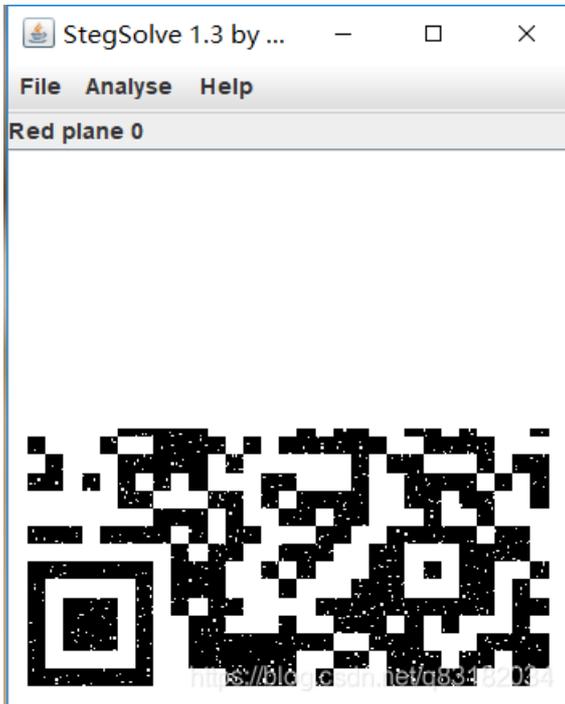
这时候就要动用stegsolve（一个好工具，强烈推荐！），一波检查，发现R通道含有半个二维码。



查看图片帧数，发现是两帧。



用ps分离图层，再用stegsolve检查一波两图层，得到另一半。



缺少一个定位点，用另半张里的通过ps补足，再ps合并，扫码，flag既出！<(^~^)>自豪



总结：
misc的依旧是脑洞题，这道题考察的有点像压缩包的伪装加密（做这道题之前就没做过...也不知哪里来的爆肝精神...）对压缩包文件结构要有一定的了解，还要做过一些隐写题，再次安利stegsolve！做图片隐写真的好用！