

# BugKu CTF(杂项篇MISC)—赛博朋克

原创

网络安全研究所 于 2021-02-02 11:13:36 发布 1324 收藏 6

文章标签: [乱码](#) [css](#) [html](#) [微软](#) [md5](#)

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/zjqxzhj/article/details/113578023>

版权

CTF

BugKu CTF

(杂项篇MISC)

攻与防



赛博朋克

描述: flag{}

下载之后是一个压缩包, 包含一个txt文本文件。



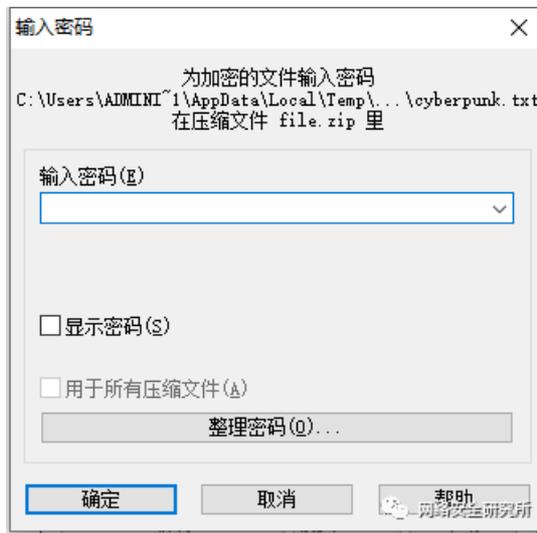
一、工具

十六进制工具 010 editor

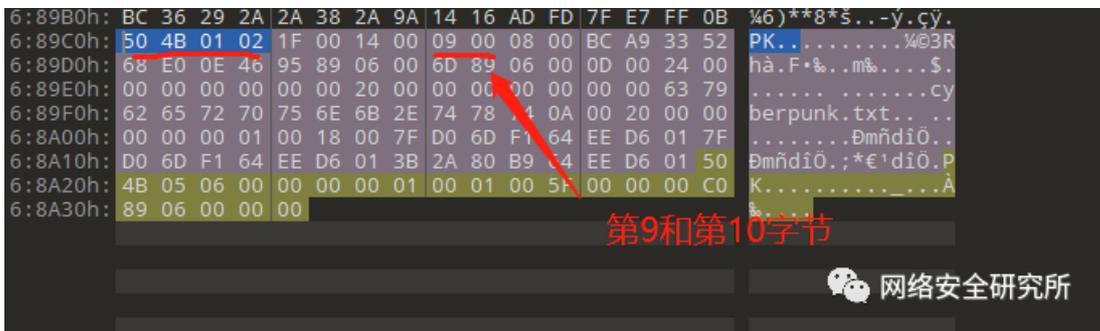
图片分析工具 Stegsolve

二、解题思路

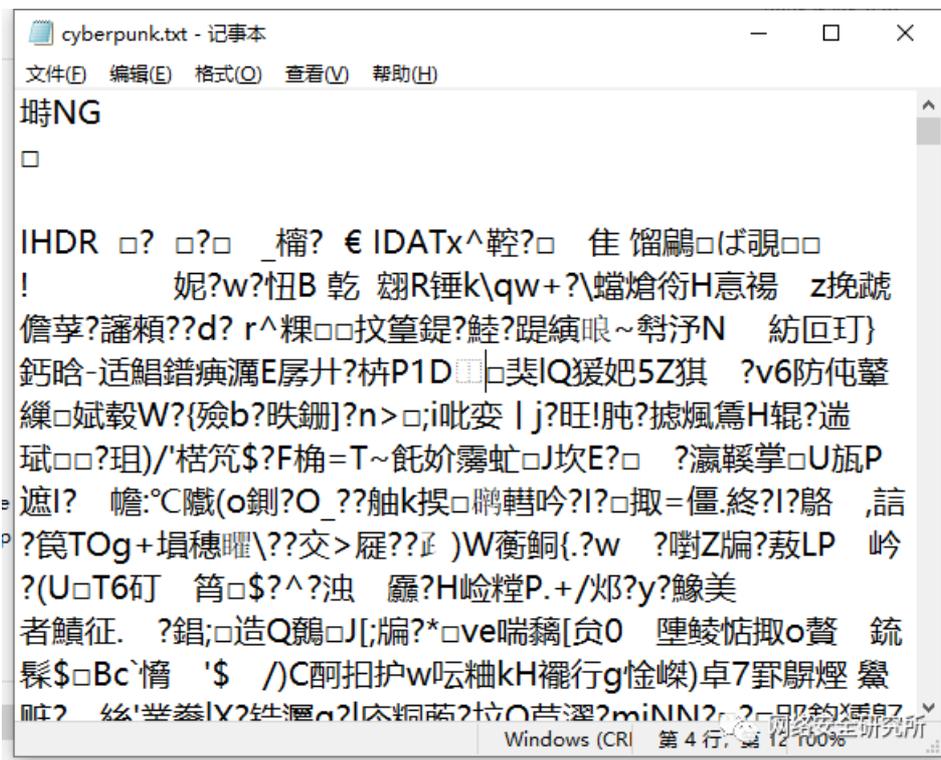
1.先尝试把压缩包解压, 提示需要密码。看看压缩包属性也没有发现特殊字段。



2.考虑有没有可能是zip压缩包的伪加密了。用010 editor编辑器打开看一看。找到从504B0102字节，从50开始算，第9和第10个字节改为0000



3.压缩包可以正常解压了。确实是伪加密。但是打开之后是一堆乱码。发现头部有个NG，猜测可能是png图片。



4.用010 editor编辑器打开看看，前面讲过89504E47是PNG文件头标识。这应该是一张图片被改后缀了。因此将txt后缀改为png。

```

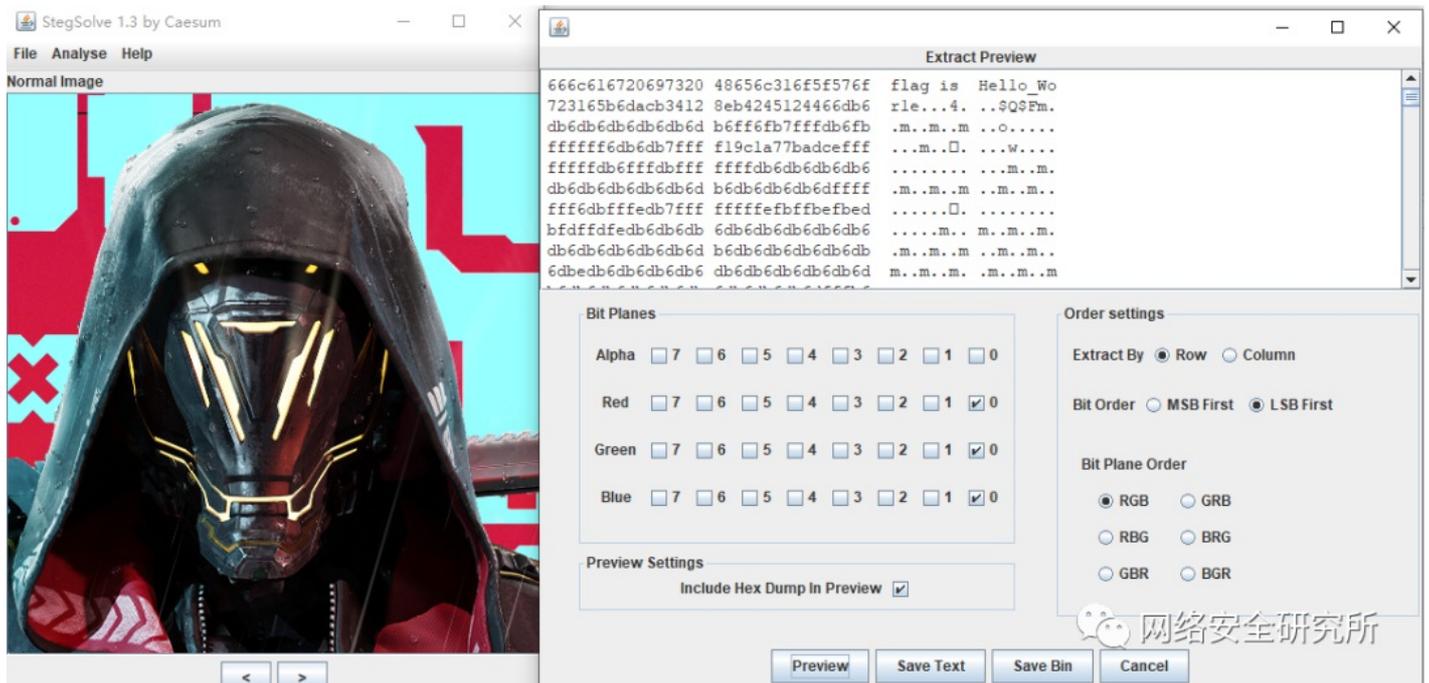
起始页  file.zip  cyberpunk.txt x
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0000h: 89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 PNG.....IHDR
0010h: 00 00 01 B3 00 00 01 CC 08 06 00 00 00 5F 99 46 ...³...ÿ...™F
0020h: 93 00 00 80 00 49 44 41 54 78 5E EC 9D F5 7F 14 "...€.IDATx^i.õ..
0030h: D7 FB F6 BF 7F C1 F3 FA 40 12 A4 D0 D2 96 16 0F xûõ¿.Áóú@.µÐÛ-..
0040h: 09 21 09 C4 DD 90 04 77 B7 04 E2 EE 1E 42 20 81 .!.Áÿ..w.âi.B .
0050h: 78 02 C1 9D 52 B4 38 6B 5C 71 77 2B EE 2D 5C CF x.Á.R'k\qw+i-\Ï
0060h: 7D 9F CD D0 65 48 90 96 B6 40 F9 E1 7A CD EC CC }YÏþEh.-¶@üázíÏ
0070h: 99 D9 D9 DD B3 E7 3D D7 7D EE 73 E6 FF B2 01 64 "UÛÝ³ç=x}isæÿ².d
0080h: BF 00 72 5E BC 40 0E 14 92 5E F3 F2 E5 7E DE 2E ç.r^%@.öóóóóóóó
0090h: F6 49 FB 15 DB 79 BF 74 AC F2 7E 85 78 9B 54 4E öIÛ.Ûÿ;t-öóóóóóóó
00A0h: F9 FC 7F BC 8F D8 CF E7 E0 7D E2 7D EA CF 2D CA üü.%.ØIçã}â}ëI-É

```

5. 打开看到一张图片。用010打开之后未看到报错信息，没有CRC错误之类的。



6. 考虑图片隐写，用Stegsolve工具看一看吧。最常见的就是LSB隐写，RGB模式。设置完之后往上翻，发现最上面就是flag了。



### 3.总结

本题需要掌握010 editor编辑器，zip压缩包文件头和伪加密方式，图片隐写查看器Stegsolve，LSB隐写等。

常用文件的文件头如下(16进制):

JPEG (jpg), 文件头: FFD8FFE1

PNG (png), 文件头: 89504E47

GIF (gif), 文件头: 47494638

TIFF (tif), 文件头: 49492A00

CAD (dwg), 文件头: 41433130

Adobe Photoshop (psd), 文件头: 38425053

Rich Text Format (rtf), 文件头: 7B5C727466

MS Word/Excel (xls.or.doc), 文件头: D0CF11E0

ZIP Archive (zip), 文件头: 504B0304

RAR Archive (rar), 文件头: 52617221

**END**

扫码关注

网络安全研究所

更多精彩等着你

