

Writeup of BlueDon CTF's MISC-1:杂项全家桶

原创

C0ss4ck 于 2017-10-30 21:23:50 发布 2024 收藏 1

分类专栏: [MISC_of_CTF](#) 文章标签: [MISC CTF BlueDon](#)

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/cossack9989/article/details/78397527>

版权



[MISC_of_CTF](#) 专栏收录该内容

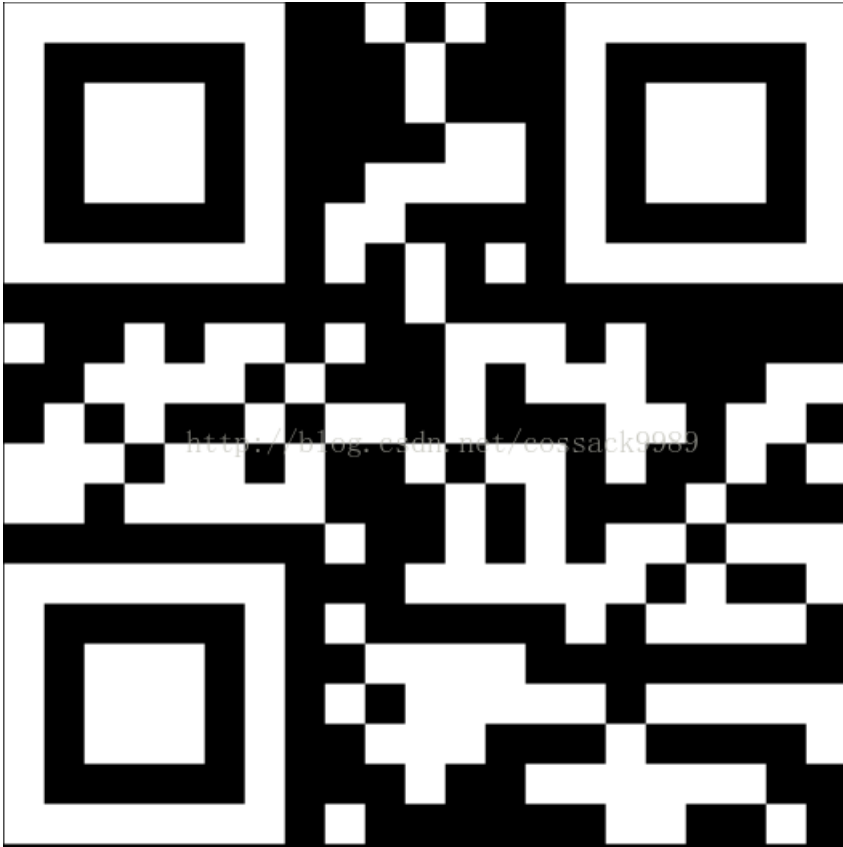
3 篇文章 0 订阅

订阅专栏

突然发现bdctf的初赛竟然还有一轮, 拿起电脑顺手干了一题~。

Step1:

下载附件后解压得一个打不开的png文件, 发现文件头被损坏, 修正后打开得下图



Step2:

很明显需要反色一下, 用stegosolve的colour inversion (Xor) 进行反色, 扫码得到一串当铺密码“工井大人夫王”译得485376。这个时候本来以为是在png里面藏了个加密压缩包什么的, 一番搜索之后并没有发现啥……陷入沉思。

Step3:

再打开010editor, 发现png文件后面跟着一个rar, 解压得一个mp3文件, 用audacity一番操作之后并没有发现什么有价值的信息, 于是用命令行操作MP3stego,

```
Windows PowerShell
PS D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego> D:\MP3Stego_1_1_18\MP3Stego\Decode.exe -X -P music.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
USAGE : D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego\Decode.exe [-X][-A][-s sb] inputBS [outPCM [outhidden]]
OPTIONS : -X          extract hidden data
          -P <text>  passphrase used for embedding
          -A          write an AIFF output PCM sound file
          -s <sb>   resynth only up to this sb (debugging only)
          inputBS    input bit stream of encoded audio
          outPCM     output PCM sound file (dflt inputBS+.aif|.pcm)
          outhidden  output hidden text file (dflt inputBS+.txt)
PS D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego> D:\MP3Stego_1_1_18\MP3Stego\Decode.exe -X music.mp3
MP3StegoEncoder 1.1.17
See README file for copyright info
Input file = 'music.mp3'  output file = 'music.mp3.pcm'
Will attempt to extract hidden information. Output: music.mp3.txt
Enter a passphrase: *****
Confirm your passphrase: *****
the bit stream file music.mp3 is a BINARY file
HDR: s=FFF, id=1, l=3, ep=off, br=9, sf=0, pd=1, pr=0, m=0, js=0, c=0, o=0, e=0
alg.=MPEG-1, layer=III, tot bitrate=128, sfrq=44.1
mode=stereo, sblim=32, jsbd=32, ch=2
[Frame 7949]Avg slots/frame = 417.907; b/smp = 2.90; br = 127.984 kbps
Decoding of "music.mp3" is finished
The decoded PCM output file name is "music.mp3.pcm"
PS D:\MP3Stego_1_1_18\MP3Stego_1_1_18\MP3Stego>
```

得到music.mp3.txt (decode文本)，获得字符串fx4qx0hj_4_cg{Wvf}，显然是凯撒密码，列出所有位移结果后得到flag，即bdctf{4_Sm4rt_b0y}