BDCTF2017-初赛第一阶段writeup

原创

Pz_mstr 于 2017-10-14 16:29:34 发布 1359 收藏

文章标签： bdctf ctf 蓝盾

本文链接：https://blog.csdn.net/qq_35544379/article/details/78235074

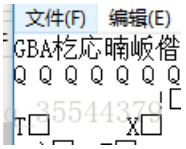
0x00 前言

由于某些不可描述的原因暂时停赛了，现在分享一下题目writeup，不按顺序写

0x01 正文

childhood

下载题目后，打开有个压缩包，历经各种方法都搞不开，只能爆破出结果了
密码bdctf2017
压缩包中两个文件：file，data
猜测一个文件可执行，另一个文件为可执行文件的数据，因此将file文件拖入winhex分析



发现是gba文件，改文件后缀，使用gba打开，ok成功打开文件

因此修改data文件为file.sav
重新打开文件发现flag

贝S16连环锁猪套

提示：图片中有提示
下载文件后扔winhex分析
发现rar文件头

```
0003CC0  8B 8E BC BE 5F F8 F0 93  FE B9 D1 45 00 7A 47 87  ‹Ž¼¾_øð“þ¹ÑE zG‡
0003CD0  3F D5 DE 7F D7 BC 75 A3  A0 CC E3 C3 BA 77 CC DF  ?ÕÞ ×¼u£ ÌãÃºwÌß
0003CE0  F1 EC 9D FD A8 A2 80 3F  FF D9 52 61 72 21 1A 07  ñì ý¨¢€?ÿÙRar!
0003CF0  00 CF 90 73 00 00 0D 00  00 00 00 00 00 00 4A 62   Ï s           Jb
0003D00  74 24 96 55 00 A0 00 00  00 90 00 00 00 02 37 22  t$–U          7"
0003D10  04 06 2B 7A AB 4A 1D 33  28 00 20 00 00 00 D5 E6    +z«J 3(     Õæ
```

改名字进行解压需要密码，联想到题目提示说图片，因此看图片找到字符串war2，输入后成功解压
出现这样的密码串
62746374667B647l6F3l326D786B6l7364667D
观察发现，这个很像是ascii码十六进制值，尝试后得到flag

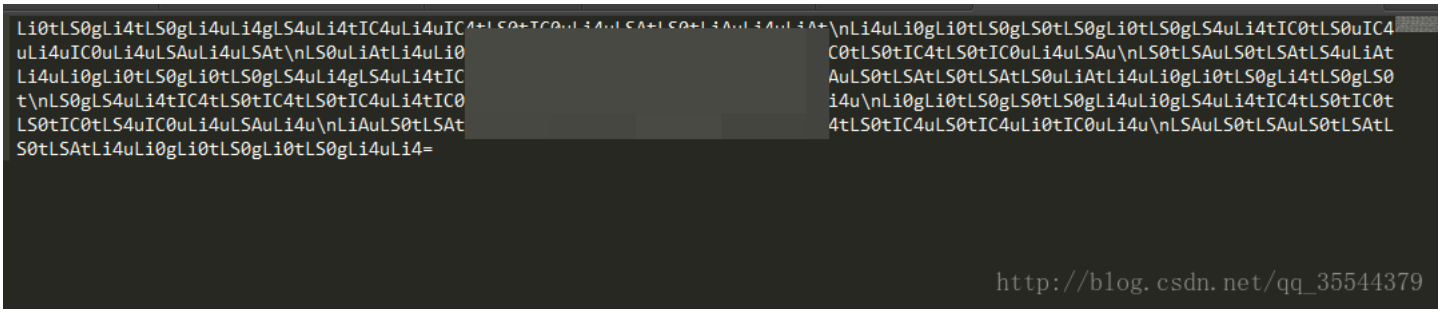
```
btctf{d          if}
```

贝斯的一家

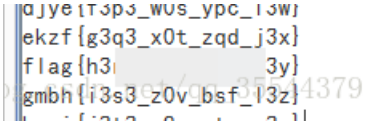
```
UjFrelJFMVJXbGRIUlRORVQwNHlRMGRaTTBSTlVWcFVS                VUzFKU1ZVZEpXbFJKVGxwVVIxa3lWRXRTVWxkSVJWcFVSMDVMUjBkVk0wUkhUVnBZU
jBrelZGTk9TMGRIVFRSVVRWS1NWMGxaTTBSS1RqSkY=
```

简单明了贝斯全家桶即出flag

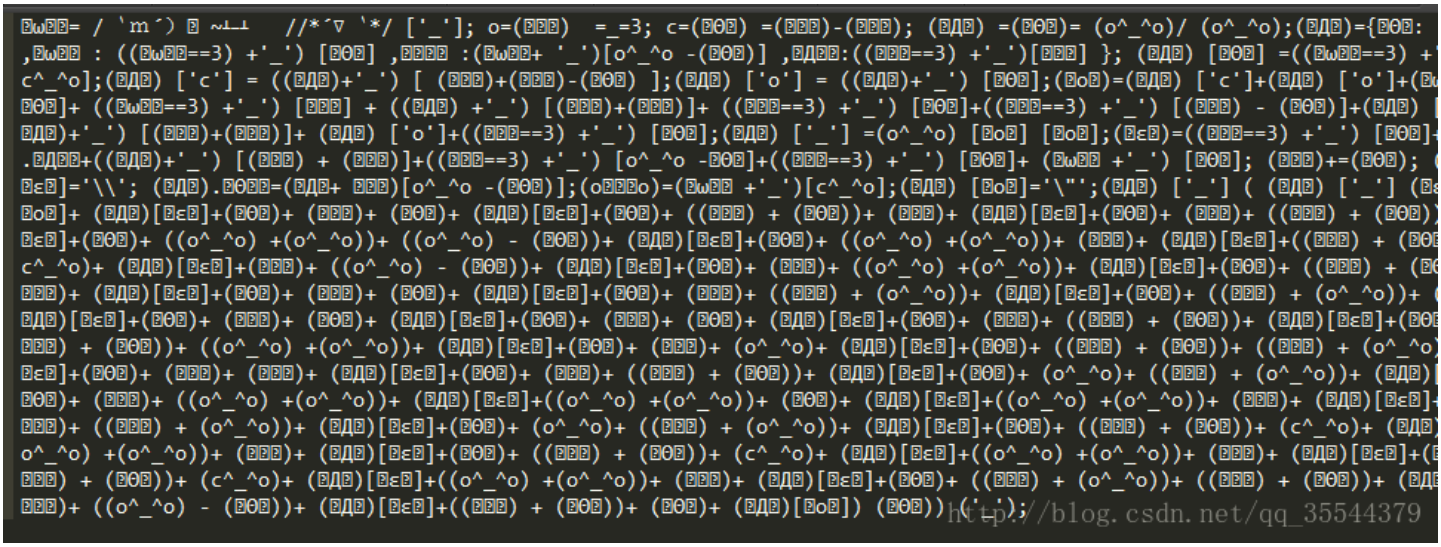
你猜我像啥



1.发现\n手动换行处理
2.发现最后=号，每一行base64处理
3.发现莫斯密码，摩斯密码解密处理
4.解密出ascii码值，转为对应字符
5.对应字符为
}3_e_0_euxxxxxnhl33{ns（中间的xxxxx为掩盖字符，不是真实的字符，以便大家动手复现，而不是原样照抄）
6.发现{}的位置不太正确，翻转试试
7.获得看起来正确一些的位置，先栅栏一下
8.xxxx{xxxxxxxxxxxxx}，这种形式，使用凯撒密码
9.出结果



颜文字



别想了，控制台运行吧

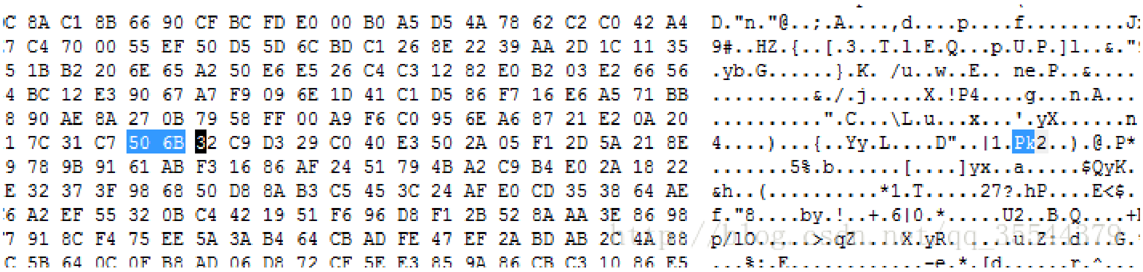
这是什么加密

不好意思。。。这题所有参赛人员暂未解出，我也不会，等待更新

狗的疑惑

这道可以说是假web题了
下载音频，下载图片
将这张经典的狗图片放进为winhex看看

发现PK头，修改为zip，解压得出密码



将该密码应用到MP3Stego中，得到flag

两道简单的逆向题

不演示太多了，
第一道提取apk的dex文件，然后将dex转jar，反汇编看源码
第二道一个套路

web2

据说还有这道题，但是没见到就挂了