

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](#)

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/qq_35544379/article/details/78235074

版权

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

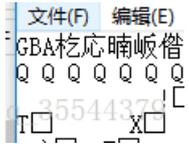
childhood

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

```

003C80 00 6A 51 45 00 78 1F C8 0F E9 27 DF E8 F1 27 E8 | jQe x x u`zOn`p
003CC0 8B 8E BC BE 5F F8 F0 93 FE B9 D1 45 00 7A 47 87 | <Z4%_a8`p^ÑE zG#
003CD0 3F D5 DE 7F D7 BC 75 A3 A0 CC E3 C3 BA 77 CC DF | ?ÖE *4uE iãÃ°wİß
003CE0 F1 EC 9D FD A8 A2 80 3F FF D9 52 61 72 21 1A 07 | ñi ý`cE?ÿÜRar!
003CF0 00 CF 90 73 00 00 0D 00 00 00 00 00 00 00 4A 62 | i s Jb
003D00 74 24 96 55 00 A0 00 00 00 90 00 00 00 02 37 22 | t$-U 7"
003D10 04 06 2B 7A AB 4A 1D 33 28 00 20 00 00 00 D5 E6 | +z«J 3( Öæ

```

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

62746374667B647I6F3I326D786B6I7364667D

观察发现，这个很像是ascii码十六进制值，尝试后得到flag

```

22e-2/9
) btctf{d if}
3 .....C.....
4 .....35544379.....

```

贝斯的一家

```

UjFre1JFMVJXbGRIUIRORVQwNH1RMGRaTTBST1VwcFVS VUzFKU1ZVZEpxBfJKVGxwVVIxa31WRXRTVwxkSVJWcFVSMVMUjBkVk0wUkhUVnBZU
jBre1ZGtK9TMGRIVFRSVVRWS1NwMGxaTTBSS1RqSkY=

```

http://blog.csdn.net/qq_35544379

简单明了贝斯全家桶即出flag

你猜我像啥

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

```

C 8A C1 8B 66 90 CF BC FD E0 00 B0 A5 D5 4A 78 62 C2 C0 42 A4 D."n."@...;A....,d....p....f.....J:
7 C4 70 00 55 EF 50 D5 5D 6C BD C1 26 8E 22 39 AA 2D 1C 11 35 9#..HZ.{...[.3..T.l.E.Q...p.U.P.]l..&."!
5 1B B2 20 6E 65 A2 50 E6 E5 26 C4 C3 12 82 E0 B2 03 E2 66 56 .yb.G.....}.K. /u..w..E.. ne.P...&....
4 BC 12 E3 90 67 A7 F9 09 6E 1D 41 C1 D5 86 F7 16 E6 A5 71 BB .....&.../.j.....X.!P4....g...n.A...
8 90 AE 8A 27 0B 79 58 FF 00 A9 F6 C0 95 6E A6 87 21 E2 0A 20 .....".C...L.u...x...'.yX.....n
1 7C 31 C7 50 6B 02 C9 D3 29 C0 40 E3 50 2A 05 F1 2D 5A 21 8E 4....)...{..Yy.L....D"...|1.Pk2...).@.P*
9 78 9B 91 61 AB F3 16 86 AF 24 51 79 4B A2 C9 B4 E0 2A 18 22 .....5%.b.....[....]yx..a.....$QyK.
E 32 37 3F 98 68 50 D8 8A B3 C5 45 3C 24 AF E0 CD 35 38 64 AE sh..(.....*1.T.....27?.hP....E<$.
6 A2 EF 55 32 0B C4 42 19 51 F6 96 D8 F1 2B 52 8A AA 3E 86 98 f."8....by.!...+6|0.*.....U2..B.Q....+|
7 91 8C F4 75 EE 5A 3A B4 64 CB AD FE 47 EF 2A BD AB 2C 4A 88 /p/100q...(>:q2!.nXlyRqj...AuZz!d!7!G.
C 5B 64 0C 0F B8 AD 06 D8 72 CF 5E E3 85 9A 86 CB C3 10 86 E5 ...%:.E.....-e*.[d.....r.0...

```

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