Writeup of MOCTF

原创

MozhuCY 于 2018-02-01 21:39:17 发布 1438 收藏
分类专栏： CTF入门

RE:

0x00:SOEASY

逆向的签到题，扔进IDA搜索字符串，本来想定位下主函数，结果直接看到了flag。

0x01:跳跳跳

打开dump.exe发现居然是掷色子的游戏..很明显爆破，OD载入找到关键跳，直接吧jnz改成je...或者从开头直接跳到最后hhhhhhhhh，得到一串base64，解之得到flag。

0x02:听小姐姐的话此题官方并没放出..

0x03:暗恋的苦恼

得到一个jiamiqi.exe 密文和密匙，IDA定位到函数，发现加密器将明文和密匙的每一位放到了加密函数里，密匙长度如果比明文短，会再次从密匙头开始传进加密函数，函数中可以看到，空格是不会被加密的，加密函数的逻辑很清晰，先吧对应位的字符toupper(),将大写后明文相对‘A’的距离加到密匙位上然后返回,直接爆破好了..(懒得想逆运算..下面是加密函数和脚本

```
l='QWDRILDWNTW'
key='ILOVEMOCTFI'
flag=''
for i in range(len(l)):
    for plain in range(65,91):
        a=plain-65
        if a+ord(key[i])>90:
            a-=25
        if a+ord(key[i])==ord(l[i]):
            flag+=chr(plain)
print flag
```

```
char __cdecl sub_401170(char plaintext, char key)
{
  char result; // al@2
  char v3; // [sp+Ch] [bp-48h]@1
  int i; // [sp+4Ch] [bp-8h]@3
  int v5; // [sp+50h] [bp-4h]@3
  char v6; // [sp+5Ch] [bp+8h]@1
  char v7; // [sp+60h] [bp+Ch]@1

  memset(&v3, 0xCCu, 0x48u);
  v6 = toupper(plaintext);
  v7 = toupper(key);
  if ( v6 == 32 )
  {
    result = v6;
  }
  else
  {
    v5 = v6 - 65;
    for ( i = 0; i < v5; ++i )
      ++v7;
    if ( v7 > 90 )
      result = v7 - 25;
    else
      result = v7;
  }
  return result;
}
```

CRYPTO:

0x00:就是这个feel!!:明显摩斯电码，解码得flag

0x01:数据库密码,想了好久hhh “**D8EA7326QE6EC5916ACCDX6E0VC9D264C63”**的到这样一串字符串，长度为**35**，数字超过了**base32**的范围,后来发现,长度**35**正好有**3**个非**16**进制字符，除去解**MD5**,得**flag**

0x02:题目名字很明确，rot解下所给字符串就好了

0x03:奇怪汉字,典型当铺密码，解码后10进制转ASKII

0x04:base族谱,解码后得到诡异字符串，栅栏后凯萨列举解密

MISC:

0x00-…… 杂项的题目很基础,010,stegslove,熟识一些文件头，当然也有爆破等操作,就留给大家自己探索吧。

WEB的话..因为是二进制方向没有做太多,不过了解最基本的抓包看PHP源码，还是可以做出前6道题的。