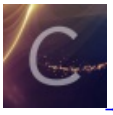
实验吧CTFreverse题目证明自己吧writeup

原创

iqiqiya 于 2018-09-11 19:57:40 发布 1161 收藏 2
分类专栏： 我的逆向之路 我的CTF之路 ------实验吧CTF 我的CTF进阶之路 文章标签： 实验吧CTFreverse题目证明自己吧题解 证明自己吧 writeup

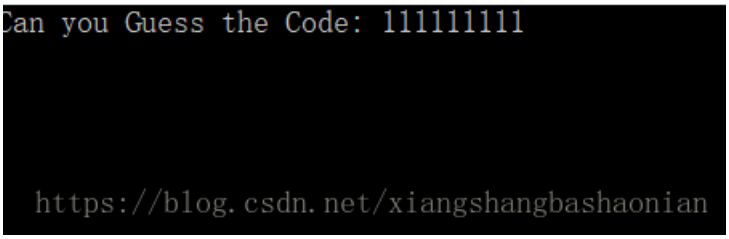

我的逆向之路 同时被 3 个专栏收录
108 篇文章 10 订阅
订阅专栏


我的CTF之路
92 篇文章 5 订阅
订阅专栏


------实验吧CTF
6 篇文章 0 订阅
订阅专栏

题目地址： http://ctf5.shiyanbar.com/crackme/

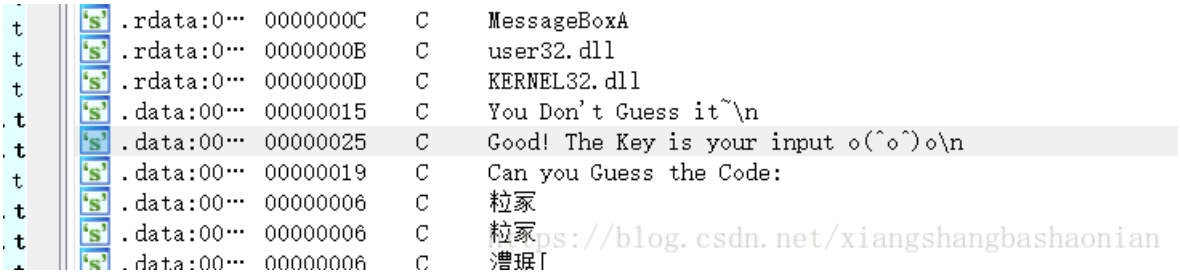
先运行下



发现输入错误就会闪退

没有加壳

载入IDA 搜索字符串



```
.data:00407045                 align 4
.data:00407048 aGoodTheKeyIsYo db 'Good! The Key is your input o(^o^)o',0Ah,0
.data:00407048                                         ; DATA XREF: _main+2B↑o
.data:0040706D                 align 10h
.data:00407070 aCanYouGuessThe db 'Can you Guess the Code: ',0
.data:00407070                                         ; DATA XREF: _main+6↑o
.data:00407089                 align 4
.data:0040708C dword_40708C    dd 48195768h            ; DATA XREF: sub_401060+3↑r
.data:00407090 dword_407090    dd 78586E50h            ; DATA XREF: sub_401060+8↑r
```

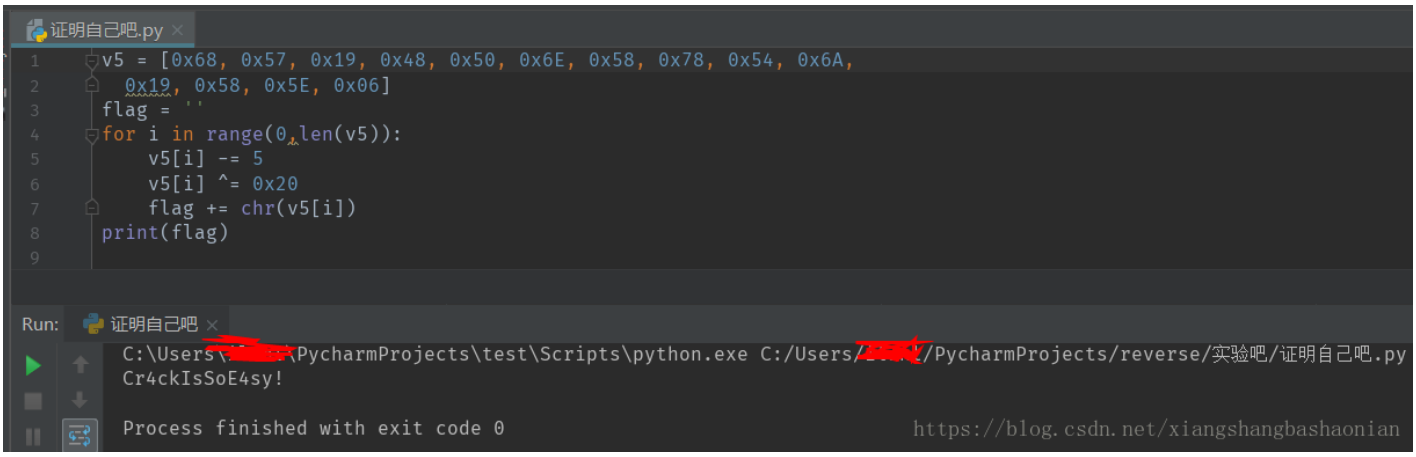

IDA View-A | Pseudocode-B | Pseudocode-A | Strings window | Hex View-1 | Structures | Enums

```
1  int __cdecl main(int argc, const char **argv, const char **envp)
2  {
3    int v4; // [esp+0h] [ebp-7D0h]
4
5    sub_4011BA(aCanYouGuessThe, v4);
6    gets(&v4);                                  // 获得输入
7    if ( sub_401060(&v4) )                      // 我们的input经过函数sub_401060()的处理返回值为1  那就正确
8      sub_4011BA(aGoodTheKeyIsYo, v4);
9    else
10     sub_4011BA(aYouDonTGuessIt, v4);
11   return 0;
12 }
```



```
signed int __cdecl sub_401060(const char *input)

{

  unsigned int i; // edx

  unsigned int j; // edx

  int v3; // edx

  int v5; // [esp+Ch] [ebp-10h]

  int v6; // [esp+10h] [ebp-Ch]

  int v7; // [esp+14h] [ebp-8h]

  __int16 v8; // [esp+18h] [ebp-4h]

  char v9; // [esp+1Ah] [ebp-2h]



  v5 = dword_40708C;

  v6 = dword_407090;

  v8 = word_407098;

  v9 = byte_40709A;

  v7 = dword_407094;

  if ( strlen(input) == strlen(&v5) )           // 如果我们输入的长度=v5的长度

  {
```

```
    i = 0;
    if ( strlen(input) != 0 )                   // 如果len(input) != 0 且i<len(input)
    {
      do
        input[i++] ^= 0x20u;                    // 与0x20u异或
      while ( i < strlen(input) );
    }
    j = 0;
    if ( strlen(&v5) != 0 )                     // 对v5进行-5
    {
      do
        *(&v5 + j++) -= 5;
      while ( j < strlen(&v5) );                // 那我们只需要倒过来操作  先-5  再与0x20异或即可得到flag
    }
    v3 = 0;
    if ( strlen(&v5) == 0 )
      return 1;
    while ( *(&v5 + v3 + input - &v5) == *(&v5 + v3) )
    {
      if ( ++v3 >= strlen(&v5) )
        return 1;
    }
  }
  return 0;
}
```



得到flag：Cr4ckIsSoE4sy!