XCTF IgniteMe

原创

酸酸菜鱼 于 2020-08-15 22:35:52 发布 58 收藏
分类专栏： CTF

1.通过搜索字符串，确定函数sub_4011C0是关键函数，再者里边有個小的计算的函数sub_4013C0

贴上代码

```
bool __cdecl sub_4011C0(char *input)
{
  size_t v2; // eax
  signed int v3; // [esp+50h] [ebp-B0h]
  char v4[32]; // [esp+54h] [ebp-ACh]
  int v5; // [esp+74h] [ebp-8Ch]
  int v6; // [esp+78h] [ebp-88h]
  size_t i; // [esp+7Ch] [ebp-84h]
  char input1[128]; // [esp+80h] [ebp-80h]

  if ( strlen(input) <= 4 )
    return 0;
  i = 4;
  v6 = 0;
  while ( i < strlen(input) - 1 )
    input1[v6++] = input[i++];
  input1[v6] = 0;
  v5 = 0;
  v3 = 0;
  memset(v4, 0, 0x20u);                         // v4
  for ( i = 0; ; ++i )
  {
    v2 = strlen(input1);
    if ( i >= v2 )
      break;
    if ( input1[i] >= 97 && input1[i] <= 122 )
    {
      input1[i] -= 32;
      v3 = 1;
    }
    if ( !v3 && input1[i] >= 65 && input1[i] <= 90 )
      input1[i] += 32;
    v4[i] = byte_4420B0[i] ^ sub_4013C0(input1[i]);
    v3 = 0;
  }
  return strcmp("GONDPHyGjPEKruv{{pj]X@rF", v4) == 0;
}


int __cdecl sub_4013C0(int a1)
{
  return (a1 ^ 0x55) + 72;
}
```

算法代码如下

```
"""
正向思路:
        1.把小写转换为大写
        2.進行sub_4013C0函数里的计算 (a1 ^ 0x55) + 72
        3.逐位异或字符串数組 byte_4420B0，但不是每一位都会用到，得出结果
逆向思路:
        1.逐位异或数組
        2.进行 -72 ^0x55 计算
        3.转为小写

        4.可以使用爆破。

"""

import string
str_list = [0x0D, 0x13, 0x17, 0x11, 0x02, 0x01, 0x20, 0x1D, 0x0C,
            0x02, 0x19, 0x2F, 0x17, 0x2B, 0x24, 0x1F, 0x1E, 0x16,
            0x09, 0x0F, 0x15, 0x27, 0x13, 0x26, 0x0A, 0x2F, 0x1E,
            0x1A, 0x2D, 0x0C, 0x22, 0x04]
flag = []
Str = [ord(s) for s in "GONDPHyGjPEKruv{{pj]X@rF"]
print(len(str_list))
print(len("GONDPHyGjPEKruv{{pj]X@rF"))

# 爆破
def exp():
    for i in range(24):  # len(str_list)
        for f in string.printable:
            ff = (ord(f) ^ 0x55) + 72
            ff = str_list[i] ^ ff
            if ff == Str[i]:
                flag.append(f)
    print("".join(flag).lower())

# 逆向
def rev():
    for i in range(len(Str)):
        s = Str[i] ^ str_list[i]
        s = (s - 72) ^ 0x55
        flag.append(chr(s))
    print("".join(flag).lower())


rev()
```