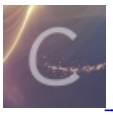
2021 羊城杯&网刃杯 re wp

原创

yaoxixixi 于 2021-09-12 19:35:43 发布 153 收藏

分类专栏： re 文章标签： c语言



@TOC

Resmc

Smc动调即可，找到加密函数，恢复栈帧，即可看到加密函数，变异的base64

```
#include<stdio.h>
#include<string.h>
unsigned char a[100]={"H>oQn6aqLr{DH6odhdm0dMe`MBo?lRglHtGPOdobDlknejmGI|ghDb<4"};
unsigned char s[100]={  0xE4, 0xC4, 0xE7, 0xC7, 0xE6, 0xC6, 0xE1, 0xC1, 0xE0, 0xC0,
  0xE3, 0xC3, 0xE2, 0xC2, 0xED, 0xCD, 0xEC, 0xCC, 0xEF, 0xCF,
  0xEE, 0xCE, 0xE9, 0xC9, 0xE8, 0xC8, 0xEB, 0xCB, 0xEA, 0xCA,
  0xF5, 0xD5, 0xF4, 0xD4, 0xF7, 0xD7, 0xF6, 0xD6, 0xF1, 0xD1,
  0xF0, 0xD0, 0xF3, 0xD3, 0xF2, 0xD2, 0xFD, 0xDD, 0xFC, 0xDC,
  0xFF, 0xDF, 0x95, 0x9C, 0x9D, 0x92, 0x93, 0x90, 0x91, 0x96,
  0x97, 0x94, 0x8A, 0x8E};
char q[100]={"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"};
int p[100];
int main(){
 //int n=strlen(a);
 //printf("%d ",n);
 for(int i=0;i<56;i+=4){
  a[i]^=0xa6;
  a[i+1]^=0xa3;
  a[i+2]^=0xa9;
  a[i+3]^=0xac;
 }

 for(int i=0;i<56;i++){
  //printf("%x ",a[i]);
  for(int j=0;j<64;j++){
   if(a[i]==s[j]){
    printf("%d ",j);
    p[i]=j;
   }
  }
 }
 for(int i=0;i<56;i++){
  printf("%c",q[p[i]]);
 }

 return 0;
}
```

找到对应的顺序后，用base64解密即可

reverse1

key长度64位 sm3加密

爆破可以拿到key，然后输入后文件自动加密即可拿到flag

```
if ( &Src[strlen(Src) + 1] - &Src[1] == 16 )
{
  for ( i = 0; i < 16; ++i )
  {
    sub_1B33A0(Src, i + 1, v14);
    for ( j = 0; j < 16; ++j )
      sub_1B1180(&Buffer[2 * j], "%02x", v14[j]);
    v4 = strcmp(&a6b8575c6092240[36 * i], Buffer);
    if ( v4 )
      v9 = v4 < 0 ? -1 : 1;
    else
      LOBYTE(v9) = 0;
    v7 = v9;
  }
```



```
from gmssl import sm3, func
from Crypto.Util.number import *
if __name__ == '__main__':
        #key = long_to_bytes(0x32)
        #print(key)
        for i in range(33,127):
                key2=long_to_bytes(i)
                key = b'wel30m_t0_sm3!!!'+key2
                y = sm3.sm3_hash(func.bytes_to_list(key))
                print(y,chr(i))
```

2048小游戏

2048小游戏

玩2048 成功后有判断

```
42  }
43  if ( v19[21] > 0 )
44  {
45    v2 = sub_F35F0(std::cout, "(GAME OVER)");
46    std::ostream::operator<<(v2);
47    v10 = v19[19];
48    v3 = sub_F35F0(std::cout, "SCORE:");
49    v4 = std::ostream::operator<<(v3, v10, sub_F3960);
50    std::ostream::operator<<(v4);
51    if ( sub_F2770(v19) == 0x1A8CD )
52    {
```


Patch判断后 就可以到加密环节

把16格格的总和数作为参数参与加密 满足这个式子等于0x1a8cd即可拿到总和数

```
3  int result; // eax
4
5  return ((((((1.5
6             - (((this[19] * 0.5) * COERCE_FLOAT(0x5F3759D8 - (COERCE_INT(this[19]) >> 1)))
7               * COERCE_FLOAT(0x5F3759D8 - (COERCE_INT(this[19]) >> 1))))
8            * COERCE_FLOAT(0x5F3759D8 - (COERCE_INT(this[19]) >> 1)))
9           * 10000000.0)
10         * 10.0)
11        + 5.0)
12       / 10.0);
13}
```

直接解密，发现数据太大，弄不出来
可以动调解密，这个式子是一个线性关系，夹逼即可
Patch掉动调和这里

```
14  result = unknown_libname_5(0, 3);
15  for ( var13A0 = 0; var13A0 < a2; ++var13A0 )
16  {
17    do
18    {
19      this[16] = sub_F35C0(var10, var1398);
20      this[17] = sub_F35C0(var10, var1398);
21    }
22    while ( this[4 * this[16] + this[17]] );
23    this[4 * this[16] + this[17]] = 2434;
24    result = var13A0 + 1;
25  }
26  return result;
27}
```


不断尝试，8448成功过掉判断
后面的两个简单的加密 前四位和剩下的，动调可以拿到flag