babyre

发表于 2021-01-04 分类于 Challenge， 2019， SCTF， Reverse
Challenge | 2019 | SCTF | Reverse | babyre

点击此处获得更好的阅读体验

解题思路

有几个简单的花指令。主逻辑很清晰，三部分password。
第一部分为555的迷宫，wasd上下左右，xy在z轴方向上下移动。

```
***** *..** *..** ***** *****
***** ****. *..** ***** **..*
****. ****. ..#*. ***** *...*
****. ***** .***. ***** ..*.*
**s.. ***** .***. .**.. .**.*
```

直接看出路径来：ddwwxxssxaxwwaasasyywwdd

第二部分就是base64c2N0Zl85MTAy第三部分为一个简单的对称加密，直接逆回来:

```
#include"stdio.h"
#include"string.h"
#define ROL(x, r)  (((x) << (r)) | ((x) >> (32 - (r))))
#define ROR(x, r)  (((x) >> (r)) | ((x) << (32 - (r))))
unsigned int a[288] = {0x0D6, 0x90, 0x0E9, 0x0FE, 0x0CC, 0x0E1, 0x3D, 0x0B7, 0x16, 0x0B6, 0x14, 0x0C2, 0x28, 0x0FB, 0x2C, 0x5, 0x2B, 0x67, 0x9A, 0x76, 0x2A, 0x0BE, 0x4, 0:
unsigned int foo2(unsigned int a1)
{
    unsigned v1;
    unsigned char byte[4];
    byte[0] = a1&0xff;
    byte[1] = (a1>>8)&0xff;
    byte[2] = (a1>>16)&0xff;
    byte[3] = (a1>>24)&0xff;
    v1 = (a[byte[0]])|(a[byte[1]]<<8)|(a[byte[2]]<<16)|(a[byte[3]]<<24);
    return ROL(v1,12)^ROL(v1,8)^ROR(v1,2)^ROR(v1,6);
}
unsigned int foo(unsigned int a1, unsigned int a2, unsigned int a3, unsigned int a4)
{
    return a1 ^ foo2(a2^a3^a4);
}
int main()
{
    unsigned int tmp[30] = {0};
    unsigned int cipher[4] = {0xBE040680, 0xC5AF7647, 0x9FCC401F, 0xD8BF92EF};
    memcpy(tmp+26,cipher,16);
    for(int i = 25;i>=0;i--)
        tmp[i] = foo(tmp[i+4],tmp[i+1],tmp[i+2],tmp[i+3]);
    tmp[4] = 0;
    printf("%sn",(char *)tmp);
    return 0;
}
// fl4g_is_s0_ugly!
```

FLAG

```
sctf{ddwwxxssxaxwwaasasyywwdd-c2N0Zl85MTAy(fl4g_is_s0_ugly!)}
```

- ***本文作者：*** *CTFHub*
- ***本文链接：*** *https://writeup.ctfhub.com/Challenge/2019/SCTF/Reverse/bKTLpJ6572XS2DSHnXoLxT.html*
- ***版权声明：*** *本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！*

 # Challenge # Reverse # 2019 # SCTF
two_heap
Crackme