

第一题:

在0x40117D处存在产卵花核全、修剂为mop 后重新打开即历页编译 main-o逐数。 Sub-401005(a.b.) 等价子 Read (buffer, Size)

输入长度为小的串,与byte-427A30倒序异实后,

逐飞与 byte-427A40 比较,相同则获取 flag.

引: for (i=0; i<15; i++)

flag[i] + byte - 427A30[14-i] = byte - 427A40[i]

754 flag[i] = byte-427A30[14-i] byte-427A40[i]

flag: More Then Friends/

第二版:

在伪代码第18行出现附零并常,因此争 精咖重要部分以。定在异常处理函数中.

观察汇编代码.在0x4011B6-0x4011C7处为3~产量 SEH 链表操作.其中插入的函数为插入 siub-401c9年,

数 sub-401005. 抗防 sub-401020.

进入 Sub-401020, 经典径3年

aci] = 4\* (aci1&3) | ((aci)&0xc) >>>) | aci7&0xf0.

现际2位 取3.47至 取高4位 取高4位 不多以至 不多以至 不移以至 不移以至 不移以

即这个操作是多换。acin的低1、2bit和23.4biti强 多换后与byte-429430、比较。

剧比, 支接 byte-429430俄12、345it 即得到fleg. 簡唱到flag="Security Is Puzzle", 但输入 要求长度/18. (后面只取前16字串) 放输 OH 输入flag后 随便打两个字母即可。

第三题:

输入一串度 > 5的 15 多母串,取前 4位 进行某种加密后,得到一串16进制串,推测加密应该是哈奇函数。又摘要数度为1286;t,即排除、SHA2,可能为 SHA-1 或 MDI

在 sib-401420函数中, 是对4个量进行初始化, 分别值为 Ox67452301, Oxefcdab89, 0x98 badcfe, Ox10325476

繁拾 mds/宴前

\$ub-401500 返回3 size+0x38-size名0x40+8,其字是填充后明文的长度。对济单位为512bit,在加密函数中的循环轮数的长度:64 byte,完全符合 mds 加密。

因为明文就45节,直接爆破即可.

爆出明文:100%.

输入长度要求 >5, 就在月~月后随便到一个小等牙母即可. (如: love u).

20

## 第4起:

输入一串大写字型,对基在钻代码第33行进行如下操作:

input[j] = L7+9\*(input[j]·'A'))% >6 \*/A'
附見的活射溶液。 a=9.6=7.

弱文已给出,存在 0x429A30处.

解基础设置. (im message [i7 = (cipnerti1-7)\*97)
flag: "HANGON" (mod 26)

第上题:

输入8字节(64bit) 数据进行某种加密.

最一开始调用sub-40100F函数, 跨入3V4变量, V4中存的等符串为"Take Easty", 精训为密制,进入后,发现程序流程与DES 密钥扩展流程-3处;

sub-401046 => PC1 置换 sub-401014 => ShiftLeft sub-40100A => PC2 置换、 子家钢存在 unk-42009c 中.

市 Sub\_401200 函数隔程也与DES加密流程



一致,因此确认加密为DES加密。 定文、密钥已给出,解密即可。

神仙 flag: itiseasy.
18