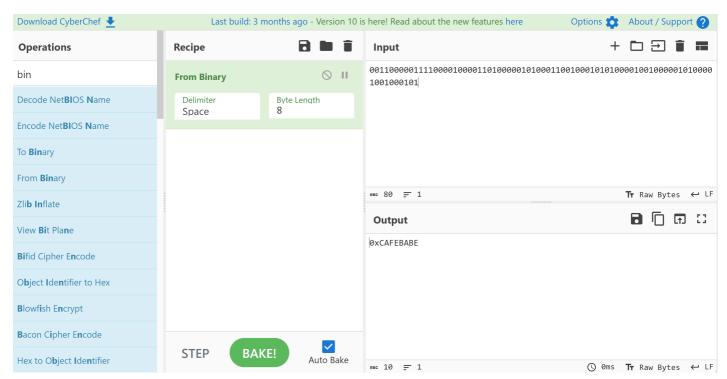
Reverse

数字筑基

根据程序要求,我们需要将如下内容转换为其十六进制形式。这里用到这个工具

在线工具

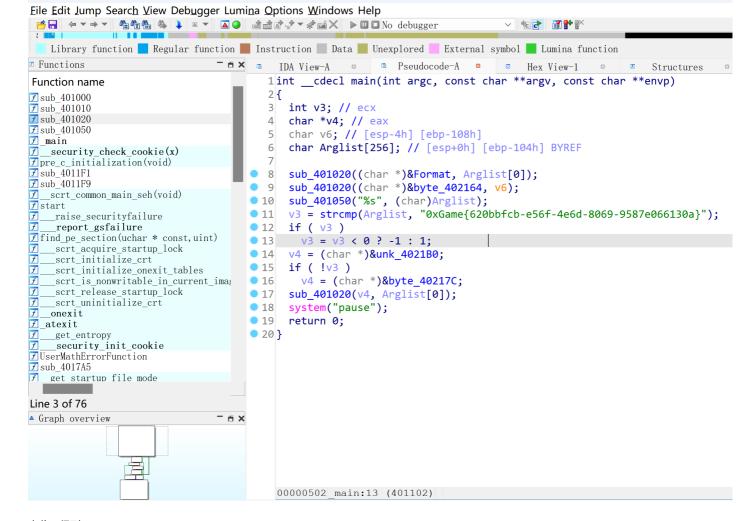
可能你需要能访问谷歌才可以打开这个工具。



利用该工具拿到十六进制的字符串,输入程序,即可拿到flag。(题目描述的16进制形式可能存在歧义。最终输入应该是ASCII字符串(如30=='0'))

代码金丹

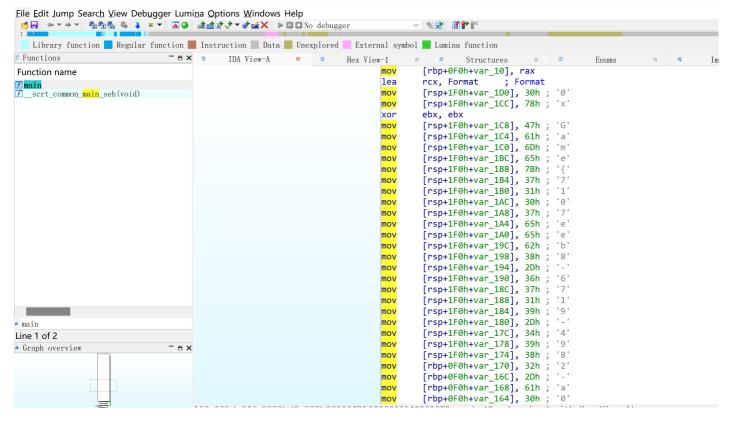
拿到程序后,我们可以用IDA打开,F5反编译main函数后,可以看到如下内容



由此,得到flag

网络元婴

拿到程序后,仿照第三题用IDA打开,F5反编译main函数后,可以看到如下内容。



由此,可以将每一位拼接,从而获得flag,也可以动态调试,复制最终拼接好的flag。

虚拟化神

拿到程序,运行发现是重启验证(输入注册码后不直接解锁功能,需要下次启动软件才会生效)。

观察可以发现,程序在验证完毕、重启之前会在同目录下创建config.txt。

根据其内容发现输入错误为0(false),将其改为1(true),再次运行程序,即可获得flag。

```
<u>File Edit Jump Search View Debugger Lumina Options Windows Help</u>
 Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
                                 - □ × □ IDA View-A
                                                         ■ Pseudocode-A
■ 
                                                                                        Hex View-1
                                                                                                         A
                                                                                                               Structures
                                                 v3[13] ^= a0xgame[(v4 + 12) % 6];
                                        • 41
Function name
                                                 v3[14] ^= a0xgame[(v4 + 13) % 6];
                                        42

J sub_140001000
                                                 v3[15] ^= a0xgame[(v4 + 14) % 6];
f sub_140001010
f sub_140001020
                                        43
                                        44
                                                 v3[16] ^= a0xgame[(v4 + 15) % 6];
f sub_140001070
f sub_1400010D0
f main
                                        45
                                                 v3 += 22;
                                                 *(v3 - 5) ^= a0xgame[(v4 + 16) % 6];
*(v3 - 4) ^= a0xgame[(v4 + 17) % 6];
                                        9 46
                                        47
   _security_check_cookie
pre_c_initialization(void)
post_pgo_initialization(void)
                                        48
                                                 v6 = v4 + 19;
                                        49
                                                 *(v3 - 3) ^= a0xgame[(v4 + 18) % 6];
| Fe_cpp_initialization(void) | scrt_common_main_seh(void) | start | raise_securityfailure | report_gsfailure
                                        9 50
                                                 v4 += 22i64;
                                       51
                                                 *(v3 - 2) ^= a0xgame[v6 % 6];
                                        52
                                                 --v5;

    __report_gsfailure
    __capture_previous_context
                                          53 }
54
                                              while (v5);
                                              fopen_s(&Stream, "config.txt", "r");
                                        55
                                              if ( Stream && (fgets(Buffer, 2, Stream), fclose(Stream), atoi(Buffer) == 1) )
   _scrt_is_nonwritable_in_current_image
                                         57
                                              {
                                                 sub_140001070("你已经解锁了神的秘密。\n");
                                        9 58
                                        9 59
                                                 sub_140001070("%s\n", (const char *)v10);

f atexit
                                         60
                                              }
 sub_140001C50
                                         61
                                              else

■ UserMathErrorFunction

                                          62
                                              {
fcharNode::raw length(void)
                                                 sub_140001070(asc_1400032E0);
                                        63
f get startup file mode
                                       64
                                                 sub 1400010D0("%s");
                                        65
                                                 if ( !strcmp(v15, (const char *)v10) )
Line 6 of 76
                                         66
                                                 {
▲ Graph overview
                                        67
                                                   fopen_s(&Stream, "config.txt", "w");
                                        68
                                                   sub_140001020(Stream, "%d");
                                        69
                                                   fclose(Stream);
                                                   sub_140001070(asc_1400032F8);
                                        70
                                            000005D0 main:53 (1400011D0)
```

当然,我们IDA分析一下也能发现,程序会解密出内置的flag,然后和输入进行比较,所以动态调试也可以拿到flag。

赛博天尊

拿到程序, 丢入IDA分析, 可以看到如下结果

```
ile Edit Jump Search View Debugger Lumina Options Windows Help
 ☆ □ ← ▼ → ▼ 衛衛艦 毎 ↓ ■ ▼ ▲ ● 講述はずず▼孝ᡤ× ▶ □ □ No debugger
                                                                                                         Library function Regular function Instruction Data Unexplored External symbol Lumina function
                              - 5 × □ IDA View-A □
 Functions
                                                            ■Pseudocode-A □
                                                                                  ■ Hex View-1 ■ Structures ■ Enums ■
                                             __int64 v10; // [rsp+58h] [rbp-130h] BYREF
__int64 v11; // [rsp+60h] [rbp-128h] BYREF
                                         9
Eunction name
__security_check_cookie
pre_c_initialization(void)
post_pgo_initialization(void)
                                        10
                                        11
                                             char Buffer[256]; // [rsp+70h] [rbp-118h] BYREF
pre_cpp_initialization(void)
                                        12
                                              sub_140001020((char *)&Format, argv, envp);
sub_140001080("%s", Buffer);
                                      13
__crp_intralization(void)
__scrt_common_main_seh(void)
_start
__raise_securityfailure
__report_gsfailure
                                      14
                                      15
                                              v3 = -1i64:
                                        16
                                              do
__report_gstature
capture_previous_context
__scrt_acquire_startup_lock
__scrt_initialize_crt
__scrt_initialize_onexit_tabl
__scrt_is_nonwritable_in_curr
                                      17
                                      18
                                              while ( Buffer[v3] );
                                              if ( v3 != 44
                                      19
20
                                                 || Buffer[43] != 125
                                        21
                                                 | (sub_1400010E0(Buffer, "0xGame{%161lx-%161lx-%161lx-%161lx}", &v7, &v8, &v9, &v10, &v11),
                                                 7 * v9 + 5 * (v8 + v11) + 2 * (v10 + 4 * v7) != 0x12021DE669FC2i64)
|| (v4 = v9 + v10 + 2 * v10 + 2 * (v11 + v7), v8 + 2 * v4 + v4 != 0x159BFFC17D045i64)
|| v10 + v9 + v11 + 2 * v9 + 2 * (v9 + v11 + 2 * v9) + 2 * (v8 + 4 * v7) != 0xACE320D12501i64
                                        22
                                        23
                                        24
                                                 | v8 + 2 * (v7 + v11 + v9 + 2 * v10) != 0x733FFEB3A4FAi64
                                        25
                                                             "恭喜!你已解锁赛博天尊的力量。
                                        26
get_star.up_.
sub_140001A50
                                                       v8 + 7 * v11 + 8 * (v9 + v10) + 5 * v7 != 0x1935EBA54EB28i64) )
                                        27
sub_140001A60
                                        28
_guard_check_icall_nop
__scrt_initialize_default_loc
                                      29
                                                v5 = "很遗憾,修仙之路漫漫其修远兮,继续努力吧。\n";
                                        30
  scrt
         is_user_matherr_presen
sub_140001A90
sub_140001A98
                                      9 31
                                              sub_140001020(v5);
                                      32
                                              system("pause");
sub 140001AA0
                                      33
                                              return 0;
                                      34 }
                                           000006B5 main: 27 (1400012B5)
ine 32 of 76
```

可以发现输入的flag按-分割,转换成整数后需要满足特定方程,提取出方程后求解即可。

运行如上脚本即可得到flag。