攻防世界逆向入门maze详解

原创

暮归纪 于 2022-01-24 22:12:44 发布 282 收藏

文章标签： c语言 开发语言 后端

本文链接：https://blog.csdn.net/weixin_52865102/article/details/122676013

题目用到的两个宏定义，百度意思都差不多，dword是双字32位，在本题是取64位的高32位的值

ida反汇编后分析，关键地方我都加了注释，需要仔细去读，我自己也是看了一个半小时

```
#define HIDWORD(x)  (*((_DWORD*)&(x)+1))
#define SHIDWORD(x)  (*((int32*)&(x)+1))
```

```
__int64 __fastcall main(__int64 a1, char **a2, char **a3)
{
  const char *v3; // rsi
  signed __int64 v4; // rbx
  signed int v5; // eax
  char v6; // bp
  char v7; // al
  const char *v8; // rdi
  __int64 v10; // [rsp+0h] [rbp-28h]

  v10 = 0LL;
  puts("Input flag:");
  scanf("%s", &s1, 0LL);
  if ( strlen(&s1) != 24 || (v3 = "nctf{", strncmp(&s1, "nctf{", 5uLL)) || *(&byte_6010BF + 24) != 125 )// // in
put:s1
                                                // // len(s1) = 24
                                                // // v3 = nctf{
                                                // // s1[0-4] = nctf{
                                                // // s1[23] = chr(125)->}
  {
LABEL_22:
    puts("Wrong flag!");
    exit(-1);
  }
  v4 = 5LL;                                     // v4 = 5
                                                //
  if ( strlen(&s1) - 1 > 5 )
  {
    while ( 1 )
    {
      v5 = *(&s1 + v4);                         // v5 = s1[v4](s1[5],s1[6]....s1[22])
      v6 = 0;
      if ( v5 > 'N' )
      {
        v5 = (unsigned __int8)v5;
        if ( (unsigned __int8)v5 == 'O' )
        {
          v7 = sub_400650((char *)&v10 + 4, v3);// v10高32位-1，O向左走
          goto LABEL_14;
        }
```

```
        }
        if ( v5 == 'o' )
        {
          v7 = sub_400660((char *)&v10 + 4, v3);// v10高32位+1，o向右走
          goto LABEL_14;
        }
      }
      else
      {
        v5 = (unsigned __int8)v5;
        if ( (unsigned __int8)v5 == '.' )       // v10低32位-1,.向上走
        {
          v7 = sub_400670(&v10, v3);
          goto LABEL_14;
        }
        if ( v5 == '0' )
        {
          v7 = sub_400680((int *)&v10);         //  v10低32位+1，0向下走
LABEL_14:
          v6 = v7;
          goto LABEL_15;
        }
      }
LABEL_15:
      v3 = (const char *)HIDWORD(v10);
      if ( !(unsigned __int8)sub_400690((__int64)asc_601060, SHIDWORD(v10), v10) )// asc_601060[v10低32位的值(行)*8+v10高32位的值(列)],
                                                // 可以化成列数为8的二维数组，这样两个值对应行和列，
                                                // 对应的字符只能是' '或'#'
        goto LABEL_22;
      if ( ++v4 >= strlen(&s1) - 1 )            // 这里看出用v5进行遍历
      {
        if ( v6 )                               // 这里应该是判断遍历完后就退出，v6=v7是char型不为''，所以这个if语句一定为真
          break;
LABEL_20:
        v8 = "Wrong flag!";
        goto LABEL_21;
      }
    }
  }
  if ( asc_601060[8 * (signed int)v10 + SHIDWORD(v10)] != '#' )// 走完18步后'#'为终点
    goto LABEL_20;
  v8 = "Congratulations!";
LABEL_21:
  puts(v8);
  return 0LL;
}
```

一顿眼花缭乱后拿到flag

```
  ******
*    *  *
*** * **
**  * **
*  *#  *
** *** *
**     *
********
nctf{o0oo000000oooo..00}
```