攻防世界 maze

原创

大瑞大 于 2020-11-26 12:48:54 发布 72 收藏 1

题目

```
v9 = 0LL;
puts("Input flag:");
scanf("%s", &input, 0LL);
if ( strlen(&input) != 24 || strncmp(&input, "nctf{", 5uLL) || *(&byte_6010BF + 24) != '}' )// nctf{18个字符}
{
LABEL_22:
  puts("Wrong flag!");
  exit(-1);
}
i = 5LL;
if ( strlen(&input) - 1 > 5 )
{
  while ( 1 )
  {
    char_ = *(&input + i);
    v5 = 0;
    if ( char_ > 'N' )                          // 如果该字符是Oo
    {
      char_ = (unsigned __int8)char_;
      if ( (unsigned __int8)char_ == '0' )
      {
        v6 = sub_400650((_DWORD *)&v9 + 1);     // 数组-1
        goto LABEL_14;
      }
      if ( char_ == 'o' )                       // char
      {
        v6 = sub_400660((int *)&v9 + 1);        // 数位+1
```


步骤

1、首先根据正常思路看，nctf{..}然后判断字符串，找到flag
2、根据不断分析，各种LABEL得跳转，最终得到结果，目的是到这

```
if ( asc_601060[8 * (signed int)v9 + SHIDWORD(v9)] != '#' )
  goto LABEL_20;
v7 = "Congratulations!";
```

3、查看字符串明白，只要最后能到#就行了

```
asc_601060      db '  *******   *  **** * ****  * ***  *#  *** *** ***     *********',(
```

4、查看题解，迷宫类型题：

```
    if ( !(unsigned __int8)sub_400690((__int64)asc_601060, SHIDWORD(v9), v9) )// 迷宫碰撞检测，如果撞到了，输出wrong
      goto LABEL_22;
```

碰撞检测函数

```
# -*-coding = utf-8 -*-
string = '  *******   *  **** * ****  * ***  *#  *** *** ***     *********'

for i in range(0, len(string), 8):
    for j in range(8):
        if string[i+j] == '*':
            print('1', end='')
        elif string[i+j] == ' ':
            print('0', end='')
```

```
        else:
            print('#', end='')
    print('')
```


司：237 字符数：1,747 图片：14 大小：1.1 MB

最终分析得

```
if ( strlen(&input) - 1 > 5 )
{
  while ( 1 )
  {
    char_ = *(&input + i);
    v5 = 0;
    if ( char_ > 'N' )                          // 如果该字符是Oo
    {
      char_ = (unsigned __int8)char_;
      if ( (unsigned __int8)char_ == 'O' )      // 低8位
      {
        v6 = sub_400650((_DWORD *)&v9 + 1);     // 高8位 -1 左
        goto LABEL_14;
      }
      if ( char_ == 'o' )                       // char
      {
        v6 = sub_400660((int *)&v9 + 1);        // 高8位 +1 右
        goto LABEL_14;
      }
    }
    else                                        // 如果该字符是.0
    {
      char_ = (unsigned __int8)char_;
      if ( (unsigned __int8)char_ == '.' )
      {
        v6 = sub_400670(&v9);                   // 低8位 -1 上
        goto LABEL_14;
      }
      if ( char_ == '0' )
      {
        v6 = sub_400680((int *)&v9);            // 低8位+1 下
LABEL_14:
```


总结

nctf{o0oo00O000oooo…OO}