【华山杯】逆向300_WriteUp

原创

Angel枫丨灬红叶 于 2015-11-02 13:06:58 发布 1111 收藏

分类专栏： CTF

本文链接：https://blog.csdn.net/yuanyunfeng3/article/details/49550259

简单对其静态分析一下。

主函数：

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
  char *v3; // esi@1
  char direct; // bl@2
  int offset; // eax@2
  int result; // eax@13
  int v7; // [sp+8h] [bp-30h]@2
  int v8; // [sp+Ch] [bp-2Ch]@2
  char v9; // [sp+10h] [bp-28h]@1
  char v10; // [sp+36h] [bp-2h]@1

  v3 = &v9;
  printf("input your sn:");
  scanf("%s", &v9);
  v10 = 0;
  if ( v9 )                                     // / 如果有输入，则进入判断
  {
    do
    {
      direct = v3[1];                           // 形式为操作数+方向
                                                //
      offset = *v3 - 48;
      v3 += 2;
      if ( !sub_401000(offset, (int)&v8, (int)&v7) )// 带入操作数，返回坐标
        break;
      switch ( direct )
      {
        case 49:
          sub_4010A0(v8, v7);
          break;
        case 50:
          sub_4010E0(v8, v7);
          break;
        case 51:
          sub_401130(v8, v7);
          break;
        default:
```

```
            if ( direct != 52 )
              goto LABEL_12;
            sub_401180(v8, v7);
            break;
        }
      }
      while ( *v3 );                            // 循环直到字符串结束
                                                //
    }
LABEL_12:
    if ( sub_4011D0() )
    {
      printf("Σ(っ °Д °;)っ\ngood job!");
      result = 0;
    }
    else
    {
      printf("(ノ °Д°)ノ ︵ ┻━┻\ntry again!");
      result = 0;
    }
    return result;
}
```

向上方向：（其他方向就不贴了。

```
char *__cdecl sub_4010A0(int a1, int a2)
{
  int i; // eax@1

  for ( i = a2 - 1; i >= 0; --i )
  {
    if ( *(&cmp1[9 * a1] + i) )
      break;
  }
  if ( i == -1 )
    *(&cmp1[8 * a1] + a1 + a2) = 1;             // // 向上直到该分组结束，如果不碰到1，则个位数为2的值会更新为
  return sub_401060(a1, a2, a1, i + 1);         // swap操作
}
```

个位数为2值的坐标：

```
x  a  b
1  2  5
2  2  6
3  3  1
4  3  5
5  5  3
6  6  6
7  7  1
8  7  4
```

xy为一组
x 来取a,b的值
y 来确定使用哪个方法

x 取值有8种
y 取值有4种

总计32种情况。(爆破貌似不现实。。

碰到1的地方与1前一个位置进行互换操作。

只要把以上8个位置的置为个位数不为2的就可以了。

搜索一下，才发现题目的的意思，原来是圆球补墙

构造一副地图。

```
1 1 0 1 1 1 0 1 1
1 0 0 0 0 0 0 0 1
1 0 0 0 0 i 2 0 1
1 3 0 0 0 4 0 0 1
0 0 0 0 0 0 0 0 0
1 0 0 5 0 0 0 0 1
0 0 0 0 0 0 6 0 0
1 7 0 0 8 0 0 0 1
1 1 0 1 1 1 1 0 1
```

1向左，2向右，3向上，4向下。可以开始玩游戏了。。

还好游戏不是很难，要是难了，凭我的智商肯定是做不出来的orz

```
flag:818344141141442362737154515352323 4
```