

Maze

@2022/11/07

初见

本体一开始没什么头绪，后来注意到名字，联系到之前在ctfwiki上看到的文章

迷宫问题

迷宫问题

迷宫问题有以下特点:

- 在内存中布置一张"地图"
- 将用户输入限制在少数几个字符范围内.
- 一般只有一个迷宫入口和一个迷宫出口

瞬间知道怎么写了

查壳



upx加壳了，直接-d脱去即可

静态分析

拖入IDA，找到main函数，F5反编译

```
{
    strcpy(v14, "*#####");
    strcpy(&v14[11], "**#####");
    strcpy(v15, "#*#####");
    strcpy(&v15[11], "***#####");
    strcpy(v16, "*##**##**");
    strcpy(&v16[11], "**##**##**");
    strcpy(v17, "#*#####");
    strcpy(&v17[11], "#*#####");
    strcpy(v18, "***#####");
    strcpy(&v18[11], "###*****");
    v8 = 0;
}
```

得到迷宫，走出即可

