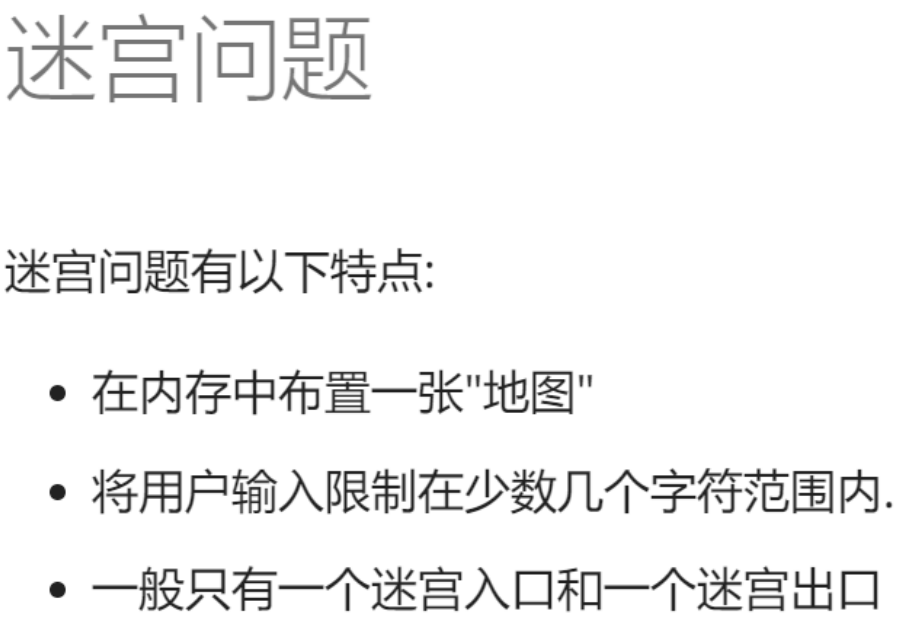
Maze

@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**
>
> 
>
>
> 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