maze

ctf比赛中经典的迷宫题目,此题把难度升级了一点而已,把地图变大了,而且upx压缩了一下,详细的wp可参考https://www.cnblogs.com/blackicelisa/p/12263625.html



放进exeinfope, 32位exe, upx加壳了, upx.exe -d game.exe指令脱壳



用ida打开,发现是maze题目(这不废话么,题目都讲了),找到地图

找到地图变量位置

```
## dompratulation db 'Congratulation!!! flag = MUCSCIF{(md5 of best input)}',0
358
                         ; DATA XREF: _main+1943^o
           align 10h
38F
390 asc_48A090
           390
           aE5
           align 4
                    # # # #
                         3F8 asc 48A0F8
           db '# # #
)F8
                         : DATA XRFF: main+7D10
           db ' # # # # # # # # # # # # # # ",0
3F8
           align 10h
15D
L60 asc_48A160
           DATA XREF:
L60
                                _main+B3↑o
           160
105
           align 4
LC8 asc 48A1C8
           db '# # # ### ###
                       DATA XREF: _main+E91o
LC8
           db' # # # # # # # # # # # # ',0
22D
           align 10h
230 asc_48A230
           230
                         DATA XREE:
                                main+11F↑o
           db ' # # # # # # # # # # # # # # " '.0
230
295
           align 4
```

然后按alt+L键方便选取,选取数据完成后按shift+E导出数据,导出完后发现会有\x00\x00\x00\x00, 这不刚好方便用软件替换吗(善用替换功能,防止手残了),替换后用广搜算法一搜就出来了

```
1 #include <cstdio>
2 #include <iostream>
3 #include <cstring>
4 using namespace std;
5 int main()
6 {
   char map[101][101] = {
    8
 "# # #
         #
          # # # #
               # # # # # # # # # # # # # # #
     # # # # # # # # # # # # # # # # # # ".
 ##
10
    11
    "# # # ### ###
            #
              ### # # # # # # # #
                        # # # # # ###
 # ### # # # # # # # # # # # # #
                # # #
                    # ".
    12
 "# # # #
         ##### # ###
                #
                  # #
                     #
                      # ### # # # # #
    14
 "# # #
15
         ### # #
             # ### # ### # ###
                        # #
                              #
               # # # # # # # ",
 ## # ##### # # # # # # # # #
```

```
17
 ##########".
 19
# ##### # ###### # # # ##### ".
 # # # # # ### ### # # # # ######### ".
 23
# # ### # # #
   # # ### # # # # ".
 # # ### # ####### # ### # # # ",
 # # ### # ### # ######## # ### # ##### ### ".
 ### # # # # # # # # # # # ### ### ",
 # ### # # ### # # # # # ### ### ",
 _ # ### # # ### # # # ### ### ### # # ### ### ",
 ### ## ###### #### ### # ".
```

```
###########".
###########".
#### # # # # # # # # #### ### # ### # ",
##########".
"# # #
  ##### # # # # # # # # # # # # # # #
################",
53
# ### # # ### # # # # # # # # # # "
54
```

```
#########".
 ############".
 # # # # # ###### # ###
 70
"# ### # # # # # #
   ##### # ### # # # # # # # # #
# # # # # # # # ### # # # # # # # # ### ##",
 73
   ### ",
 74
### # # # # # # # # # # # # # #
   ##".
```

```
### #
"# # # # # # #
      ### # ### #
 "#I
   ### # ### ### # # # # # # # # # ##### #
### # # #
 "# # # ### # # #####
### ##### # # # # # # ### # # # # ",
 # # # # #
  ### ### # # # # # # ### ",
 "# ### # # # ### #
       ### #
94
# # # # # # # # ###
```

```
# ### # # # # # # # # # # # # # # ###".
   # # # # # # # # # # # # # # # ".
   ##########################
    103
                       ###
 104
 106
 ### # # # # # #### # # # # # # # # "};
108
int board_x = 100, board_y = 100, sx = 77, sy = 1, tx = 2, t
y = 99;
110 bool book[100][100];
111 memset(book, 0, sizeof(book));
struct node
113
  int x, y;
114
115
   int f;
116
  } q[10001];
  q[0].x = sx, q[0].y = sy, q[0].f = -1;
117
  // int queue[10001] = {0};
118
  book[sx][sy] = true;
119
120
  int head = 0, tail = 1;
 //queue[head]
121
  while (head < tail)</pre>
122
123
124
  const static int next[4][2] = \{\{0, 1\}, \{1, 0\}, \{0, -1\},
```

```
\{-1, 0\}\};
            struct node temp;
125
            int flag = 0;
126
            for (int i = 0; i < 4; i++)
127
128
129
                 temp.x = q[head].x + next[i][0];
                 temp.y = q[head].y + next[i][1];
130
                 if (temp.x < 0 \mid | temp.x >= board_x \mid | temp.y < 0 \mid |
131
    temp.y >= board_y || map[temp.x][temp.y] == '#' || book[temp.x][
    temp.y])
132
                     continue;
                 book[temp.x][temp.y] = true;
133
134
                temp.f = head;
                 q[tail] = temp;
135
136
                 tail++;
137
138
                 if (temp.x == tx && temp.y == ty)
                 {
139
                     flag = 1;
140
141
                     break;
142
                 }
143
            }
144
            if (flag)
                 break:
145
146
            head++;
        }
147
148
        struct node t = q[tail - 1];
        int step[10001] = \{0\}, cnt = 0;
149
        while (t.f != -1)
150
151
        {
            step[cnt++] = t.f;
152
153
            t = q[t.f];
154
        }
155
        for (int i = cnt - 1; i >= 0; i--)
156
        {
157
            if (q[step[i]].x == q[step[i + 1]].x)
            {
158
                 if (q[step[i]].y < q[step[i + 1]].y)</pre>
159
                     cout << "A";
160
161
                 else
```

```
162
                     cout << "D";
            }
163
164
            else
165
            {
                if (q[step[i]].x < q[step[i + 1]].x)</pre>
166
                    cout << "W";
167
168
                else
169
                    cout << "S";
170
            }
171
        }
172
      return 0;
173 }
```

解出路径为:

Congratulation!!! flag = MOCSCTF{(md5 32 lowercase of best input)}

flag为MOCSCTF{ca0366ebf47cae250a8995a2cab459bf}