## 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,详细的wp可参考https://www.cnblogs.com/blackicelisa/p/12263625.html



放进exeinfope, 32位exe, 用ida打开, 发现是maze题目(这不废话么, 题目都讲了), 找到地图

```
strcpy(&v7[8177], " # ");
"# # ### # # # # ";
"# # ### # # ### ";
strcpy(\&v7[8581], "##"); \\ qmemcpy(\&v7[8485], \&asc\_48C2B0[-(\&v7[8484] - \&v7[8485])], 4*(((\&v7[8484] - \&v7[8485] + 101) \& 0xFFFFFFFC) >> 2)); \\ \end{cases}
*(_DWORD *)&v7[8585] = *(_DWORD *)"# ### # # # # ####
             "# # # # # ##### ":
strcpy(&v7[8783], "###");
qmemcpy(&v7[8689], &asc_48C380[-(&v7[8686] - &v7[8689])], 4 * (((&v7[8686] - &v7[8689] + 101) & 0xFFFFFFFC) >> 2));
strcpy(&v7[8884], " ");
```

## 找到地图变量位置

```
158 alongratulation db 'Congratulation!!! flag = MUCSCIF{(md5 of best input)}',0
                        ; DATA XREF: _main+1943^o
190
           db '#############################,0
190
∂F5
           align 4
)F8 asc_48A0F8
          db '# # #
                   # # # #
                         ####################
           db ' # # # # # # # # # # # # # # # ",0
)F8
           align 10h
15D
          L60 asc_48A160
                         DATA XREE: main+B31o
160
          L60
           align 4
LC8 asc_48A1C8
          LC8
                         ; DATA XREF: _main+E9↑o
           db' # # # # # # # # # # # # ",0
LC8
22D
           align 10h
          230 asc 48A230
                        ; DATA XREF: _main+11F↑o
           db' # # # # # # # # # # # # # # " ',0
```

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 {
7 char map[101][101] = {
 ##
 ##################
 #########################
 14
 17
 #########".
###
 # ##### # ### #### # # ##### ".
 # # # # # ### ### # # # # #### #### ".
```

```
"# # # ### # # # # # # # # # # # # #
             # # ### #
# # ### # # #
     # # ### # # # # ",
  # # # # ### # ####### # ## # # ",
  # # ### # ### # ######## # ### # #### ### ".
  # ### # # # # # # # # # # ### ### ",
  # ##### # ### # # # # # # # ### # #### ### ".
  # ### # # ### # # # # # ### # ### ### ",
  # ### # # ### # # # # ### ### ### # # ### ".
  "# # # #####
      ##### # ### # # # # # # # # # # # # #
# # #
 ## ####### #### ### # ",
  "## ####################
# # # # # # # # # # # # # # # # ".
  #### # # # # # # # #### ### # ### # ",
```

```
#########".
 _ ### # # # # # # # ### # # # ### # # # ".
 48
"# # #
   ##### # # # # # # # # # #
# ##### # # # # # # # # # # # # # "
 _ # ##### # # # # # # # # # # # # # ### ##".
 ##### ### ######",
 # ### # # ### # # # # # # # # # # # # "
 54
"# ################################
############,
 ##########################
```

```
## # # # # # # # # ## # ### # ### # ",
 "# # # # # # # # ### # #
       # # # ### #
           # # ###
# # # # # ###### # ###
 ## ### # # # # ######## # ### ####### ###".
 # # # # # # # ### # # # # # # # #
       ### ##".
 # # # # # # # # ### # # # # # # # # ### ### ##",
  ### "
74
 ### # # # # # # # # # # # # # #
        ##",
 "# # # # # # # ### # #### # # # # #
         # # # # # ##
#########".
 "# # # # # # #
          ### # ### #
```

```
"#I
      ### # ### ### # # # # # # # # # ##### #
### # # #
  "# # # ### # # # ####
_ ### ##### # # # # # # ### # # # # " ,
  ### ### # # # # # # ### ",
# # # # #
  "# ### # # # ### #
              ### #
# ### # # # # # # # # # # # # # # #### ",
  # # # # # # # # ###
  # ### # # # # # # # # # # # # # # # ###".
  # # # # # # # # # # # # # # "
  100
"# # ##### # # ### # # ### # # ### # ### #
########################
  102
"## ####################
  # # ### # ### # # # # # # # # # # # ".
```

```
105
        # ### #
  107
        ### # # # # # # # # # # # # # # # # "}:
108
      int board_x = 100, board_y = 100, sx = 77, sy = 1, tx = 2, t
109
  y = 99;
110
      bool book[100][100];
     memset(book, 0, sizeof(book));
111
112
     struct node
113
     {
114
        int x, y;
115
        int f;
     } q[10001];
116
      q[0].x = sx, q[0].y = sy, q[0].f = -1;
117
118
     // int queue[10001] = \{0\};
119
      book[sx][sy] = true;
120
     int head = 0, tail = 1;
121
     //queue[head]
122
     while (head < tail)</pre>
123
        const static int next[4][2] = \{\{0, 1\}, \{1, 0\}, \{0, -1\},
124
  \{-1, 0\}\};
125
         struct node temp;
        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
131
            if (temp.x < 0 \mid | temp.x >= board_x \mid | temp.y < 0 \mid |
   temp.y >= board_y || map[temp.x][temp.y] == '#' || book[temp.x][
  temp.y])
132
               continue;
133
            book[temp.x][temp.y] = true;
            temp.f = head;
134
            q[tail] = temp;
135
136
            tail++;
```

```
137
138
                if (temp.x == tx \&\& temp.y == ty)
139
                {
140
                    flag = 1;
141
                    break;
142
                }
143
            }
144
            if (flag)
145
                break;
146
            head++;
147
        }
148
        struct node t = q[tail - 1];
149
        int step[10001] = \{0\}, cnt = 0;
        while (t.f != -1)
150
151
        {
152
            step[cnt++] = t.f;
153
            t = q[t.f];
154
        }
155
        for (int i = cnt - 1; i >= 0; i--)
156
        {
            if (q[step[i]].x == q[step[i + 1]].x)
157
158
            {
                if (q[step[i]].y < q[step[i + 1]].y)</pre>
159
160
                    cout << "A";
161
                else
162
                    cout << "D";
163
            }
            else
164
            {
165
166
                if (q[step[i]].x < q[step[i + 1]].x)
                    cout << "W";
167
168
                else
169
                    cout << "S";
170
            }
171
        }
172
       return 0;
173 }
```