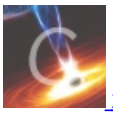
xctf easy_Maze

原创

lcer. 于 2021-03-09 16:57:00 发布 40 收藏

分类专栏： xctf-wp 文章标签： wp

本文链接：https://blog.csdn.net/weixin_43655690/article/details/114589218



这是一道迷宫题。

```
  memset(v7, 0, 0xC0uLL);
  v8 = 0;
  memset(v5, 0, 0xC0uLL);
  v6 = 0;
  Step_0((int (*)[7])v9, 7, (int (*)[7])v7);
  Step_1((int (*)[7])v7, 7, (int (*)[7])v5);
  v3 = std::operator<<<std::char_traits<char>>(&_bss_start, "Please help me out!");
  std::ostream::operator<<(v3, &std::endl<char,std::char_traits<char>>);
  Step_2((int (*)[7])v5);
  system("pause");
  return 0;
}
```

经过step_1，2是创建迷宫，step_3是走迷宫。进入step_3后发现：

```
17  while ( v8 <= 29 && (*a1)[7 * v10 + v9] == 1 )
18  {
19    std::operator>><char,std::char_traits<char>>(&std::cin, &v7);
20    v1 = v8++;
21    v6[v1] = v7;
22    if ( v7 == 'd' )
23    {
24      ++v9;
25    }
26    else if ( v7 > 'd' )
27    {
28      if ( v7 == 115 )
29      {
30        ++v10;
31      }
32      else
33      {
34        if ( v7 != 'w' )
35          goto LABEL_14;
36        --v10;
37      }
38    }
39    else if ( v7 == 'a' )
40    {
41      --v9;
42    }
43    else
44    {
45LABEL_14:
46      v2 = std::operator<<<std::char_traits<char>>(&_bss_start, "include illegal words.");
47      std::ostream::operator<<(v2, &std::endl<char,std::char_traits<char>>);
48    }
49  }
```

使用了w、a、s、d表示上下左右，我们输入这四个字母对应正确的迷宫路径就是flag，那么得到迷宫就是关键了，我们可以直接在step_3设断点、调试时查看step_1、2运行后的迷宫。

```
07FFE6919C400  01 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  ................
07FFE6919C410  01 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00  ................
07FFE6919C420  00 00 00 00 01 00 00 00  01 00 00 00 00 00 00 00  ................
07FFE6919C430  00 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00  ................
07FFE6919C440  01 00 00 00 00 00 00 00  01 00 00 00 01 00 00 00  ................
07FFE6919C450  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
07FFE6919C460  01 00 00 00 01 00 00 00  00 00 00 00 00 00 00 00  ................
07FFE6919C470  01 00 00 00 01 00 00 00  01 00 00 00 01 00 00 00  ................
```

然后写脚本得到迷宫

```
maze=[
    1,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   1,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   1,   0,   0,   0,   1,   0,
    0,   0,   0,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   1,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   1,   0,   0,   0,   0,   0,
    0,   0,   1,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   0,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   1,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   1,   0,   0,   0,   0,   0,
    0,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    1,   0,   0,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   0,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   1,   0,   0,   0,   1,   0,
    0,   0,   1,   0,   0,   0,   1,   0,   0,   0,
    1,   0,   0,   0,   1,   0,   0,   0,   0,   0,
    0,   0,   1,   0,   0,   0,   0,   0,   0,   0,
    0,   0,   0,   0,   0,   0,   0,   0]
maze1 = ''
for i in range(len(maze)):
    if (i%4 == 0):
        maze1 += str(maze[i])
    if ((i+1)%28==0):
        maze1 += '\n'
print(maze1)
```

```
1001111
1011001
1110111
0001100
1111000
1000111
1111101
000
>>>
```

```
Please help me out!
ssddwdwdddssaasasaaassddddwdds
Congratulations!
Thanks! Give you a flag: UNCTF{ssddwdwdddssaasasaaassddddwdds}
sh: pause: command not found
```

得到flag：UNCTF{ssddwdwdddssaasasaaassddddwdds}