

极客巅峰2020 virus

原创

酸酸菜鱼 于 2021-01-16 18:40:47 发布 83 收藏

分类专栏: [CTF](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/lhk124/article/details/112719086>

版权



[CTF 专栏收录该内容](#)

41 篇文章 1 订阅

订阅专栏

迷宫题

题目逻辑:

- 1.以4个 - 分割了5段内容。xxx-xxx-xxx-xxx-xxx 第一段为进入迷宫的顺序, 之后的段为迷宫的行走路线
- 2.根据题目的内容, 可以判断出进入迷宫的顺序。直接确定顺序和flag

题目详情如下

```
int __cdecl main(int argc, const char **argv, const char **envp)
{
    int v3; // eax
    _DWORD v5[10]; // [esp+14h] [ebp-4Ch]
    _DWORD v6[4]; // [esp+3Ch] [ebp-24h]
    int v7; // [esp+4Ch] [ebp-14h]
    size_t v8; // [esp+50h] [ebp-10h]
    int v9; // [esp+54h] [ebp-Ch]
    int i; // [esp+58h] [ebp-8h]
    int v11; // [esp+5Ch] [ebp-4h]

    __main();
    puts("There is a long way to defeat it.");
    scanf("%s", flag);
    v9 = strlen(flag);
    v6[0] = 0;
    v6[1] = 0;
    v6[2] = 0;
    v6[3] = 0;
    v7 = 0;
    v11 = 0;
    v8 = 0;
    for ( i = 0; i < v9; ++i ) // 该循环包括:
                                // 1.确定 - 的索引
                                // 2.限制v5(迷宫进入顺序的值)为0-9
    {
        if ( flag[i] == '-' )
        {
            v3 = v11++; // v11会+1
            v6[v3] = i; // 将每个索引保存到v6
        }
    }
}
```

```

}
if ( !v11 ) // 当v11不为0时，即第1次遇到v11时，获得v5的值
{
    v5[i] = flag[i] - 48;
    if ( (int)v5[i] > 9 || (int)v5[i] < 0 ) // 限制范围在0-9 这里其实就是字符串的‘0’-‘9’
        return 0;
}
}
if ( v11 != 4 ) // 要有4个‘-’
    return 0;
v7 = v9;
for ( i = 1; i <= v11; ++i )
{
    v8 = v6[i] - v6[i - 1] - 1; // 计算4个-之间的距离，就是走迷宫的步数
                                // 根据这个step里的次序和步数，我们直接确定迷宫的次序，是4312
    if ( step[i] != v8 ) // 0x13 0x19 0x1A 0x1C
        return 0;
    strncpy(&road[200 * i], &flag[v6[i - 1] + 1], v8);
}
for ( i = 0; i <= 3; ++i ) // 确定flag，里边有swad的方向以及d为中点，.为路线的说明
{
    if ( check_flag((int)&global_map + 200 * v5[i], v5[i], &road[200 * i + 200]) )
    {
        puts("How about try again?");
        return 0;
    }
    if ( i == 3 )
        printf("Great! We will defeat it!!! your flag is flag{%s}", flag);
}
return 0;
}

```

搜索字符串得到迷宫图，根据迷宫图：

```
||||| | | | |
|||||
|||||
||s.....||
|||||.||
||d|||||.||
|.|||||.||
|.|||||.||
|.....|
||||| | | | | |
|||||
|||||
||s||||||d|
|..|||||.||
||..|||||.||
|||.|||||.||
|||||.||||
|||||.||||
|||||.||||
|||||.||||
|||||.||||
|||||.||||
||.....d||
|||||
|||||
|||||
|||||
|||.....|
|||.|||||.||
|||.|||||.||
|||.|||||.||
|||.|||||.||
||s||||||d|
|||||
```

得到 flag{4312-wwwwwdddddsssss-aaaaaaaassssssddddd-dddddsssssaaaaaaa-www-
sdsdsdsdsddwdwdwdwdwd}