前言

这个系列的文章会带领大家从零开始完成一个完整的游戏辅助的设计，整个过程包括所需要游戏数据的查找分析，和代码编写。最后会带大家完成一个具有自动打怪，自动选择技能，自动吃药，自动任务的游戏辅助，并且整个游戏辅助的代码可以作为一套框架套用到任何一个游戏上面。

学习目标

完成一个具有自动打怪，自动选择技能，自动吃药，自动任务的游戏辅助

游戏选择

对于一个新手来说，选择一个适合入门的游戏至关重要。个人认为需要考虑下面几个因素：

1. 游戏反调试和检测相对弱
2. 封号问题不严重
3. 更新不频繁
4. 不需要上外网

如果不排除掉上述的几个干扰因素，那么在找数据技巧不成熟和代码不熟练的情况需要在其他方面花费很高的时间成本，更有可能被劝退。

这里我选择的是下面的这款游戏，下载链接：

```
https://cq.web.sdo.com/web4/guide/default.aspx
```

64位的传奇永恒，这个游戏现在玩的人已经很少，基本没有了商业化的价值，而且里面的游戏数据都很全，数组，二叉树，链表，基本都会遇到，并且不容易封号，更新也比较稳定，数据结构基本不怎么变。唯一的缺点是需要用到驱动调试器。

前置知识

在看本系列文章之前，各位需要下面的基础知识：

1. C/C++语言基础
2. 汇编语言
3. MFC界面框架
4. Windows编程基础
5. dll注入和hook技术原理
6. 软件调试的基本知识

环境准备

1. VS2017
2. x64dbg调试器
3. CE搜索工具
4. 任意一个过保护的驱动调试器
5. 传奇永恒游戏客户端

游戏数据准备

一般来说一款游戏的全套数据通常包含下面几个部分：

1. 人物属性
2. 周围遍历
3. 背包遍历
4. 技能遍历
5. 任务遍历
6. 控件遍历
7. 明文发包

以编写自动化脚本为目的，过程中需要用到的数据就是游戏所需要的全套数据。其他的数据等需要用到的再进行查找。吐槽一下市面上所谓的游戏逆向教程，号称是一个游戏找齐了两三百个功能，基本都是在水时长，具体到底有多少干货就不得而知了。

下一篇文章我们就以自动打怪为目标，开始所需要的相关数据。