郝老师，我用你的账号登进游戏了，但是不能点击酒店，要完成主线任务后才能点击。。。

我做了很久的主线任务，都还没有做到使酒店出现的任务。。。

所以我没有看到“点酒店信息查询”！

另外我调查了一下网页游戏外挂制作，发现需要与我现在制作游戏完全不同的技术。

## 技术基础

### 1、熟练的C语言知识

　　目前的外挂大部分都是用BC或者是vc写的，拥有熟练的C语言知识是写外挂的基本条件。

### 2、具有很强的汇编基础

　　一般游戏都不可能有原代码的，必须靠反汇编或者跟踪的办法来探索其中的机理，所以有强的汇编基础也是必不可少的条件。

　　3、熟练掌握跟踪和调试的工具

　　有了上面2个条件后，掌握一些工具也是很有必要的跟踪的工具，softice当然是不二之选，至于反汇编的工具，我推荐用IDA PRO这个工具反汇编出来的代码结构清晰，非常好读。

## 基本技术问题

### 1、修改进程的执行代码

　　要修改进程的执行代码，要先取得进程的ID,如果是由外挂程序启动，返回值里就有进程ID,如果不是的话，

　　需要用findwindow找到窗口句柄，再用GetWindowProcessID取得进程ID,取得进程ID以后，就可以用

　　writeprocessmemory来修改进程的执行代码了，使程序按照我们的意愿来执行，石器外挂里的不遇敌、寸步遇敌

　　就是用这样的方法来实现的

### 2、截获外挂发送和接收的封包

　　除了通过修改代码来实现的功能以外，很多的功能都是通过修改封包来实现的，要修改封包，首先要能截获它。

　　第一步是要跟踪出发和收的位置，至于怎么跟踪，我以后会提到，找到位置以后，有2个办法，一是在那个位置加一

　　个jmp语句，跳到你的处理函数位置，处理完后，再跳回来，这种方法要求比较高，需要处理好很多事情，另一种办法

　　是往那个位置写条能造成例外的指令，比如int 3,然后用DebugActiveProcess调试游戏进程，这样每当游戏执行到那个

　　位置的时候，就会停下来，到外挂程序里面去，等外挂程序处理完以后，用ContinueDebugEvent 继续运行程序。

## 技术分析

### 1 模拟键盘或鼠标的响应

### 2截获消息

### 3拦截socket包

### 4截获api

## 结论

开发外挂很难。