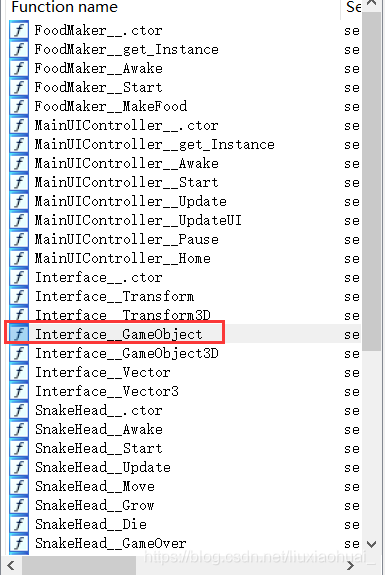
不得不说这个游戏做的还是蛮精致的，我就这么玩玩了我半个小时。

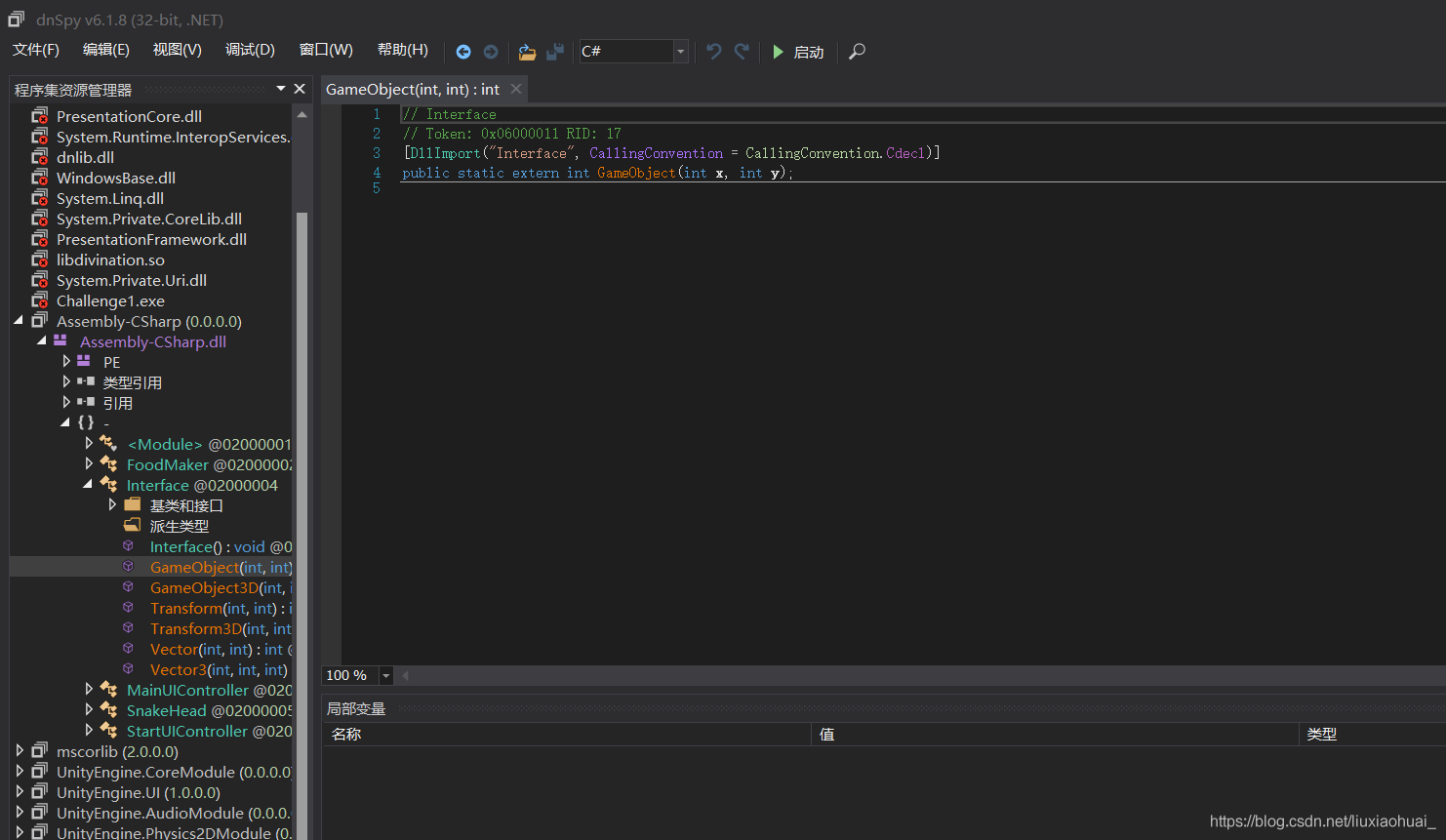


该游戏是用unity编写的，那么在文件中找到Assembly-CSharp.dll（\Snake\Snake\_Data\Manage\Assembly-CSharp.dll这个路径）拖进dnspy就能对该游戏框架的反汇编了。

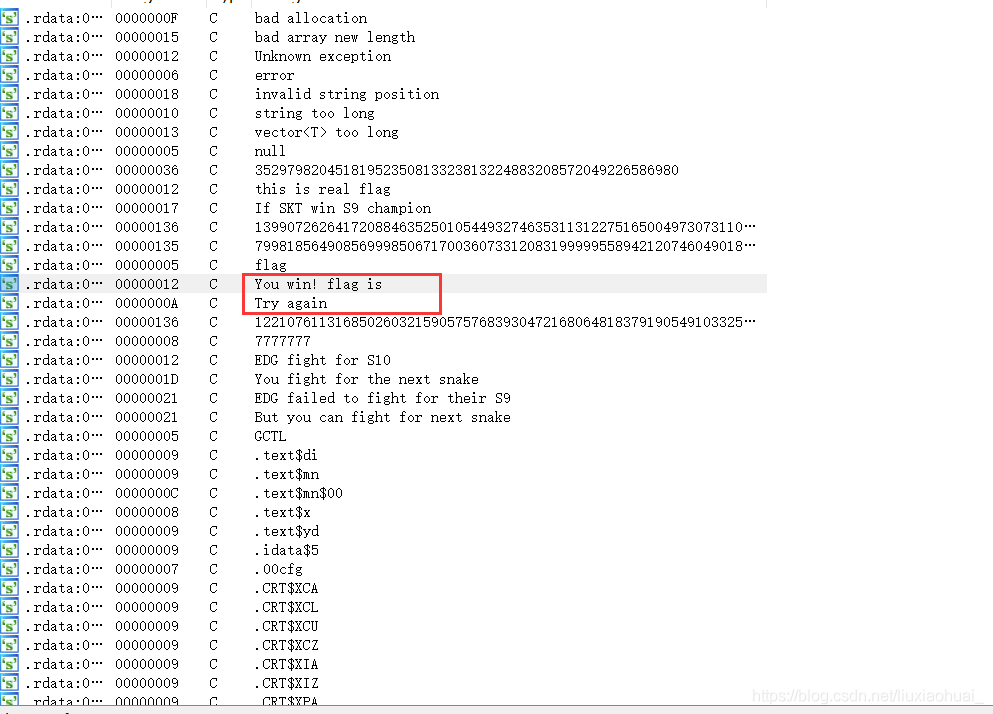
我们把它拖入ida中，就可以很清楚的看到文件中的函数调用情况



而这个GameObject函数就是这个游戏的主函数。再回到dnspy中，找到Interface下的GameObject函数



在游戏文件中找到interface.dll把它拖入ida64中，按shitf+f12查看字符串



发现了flag提示跟进去查看伪代码

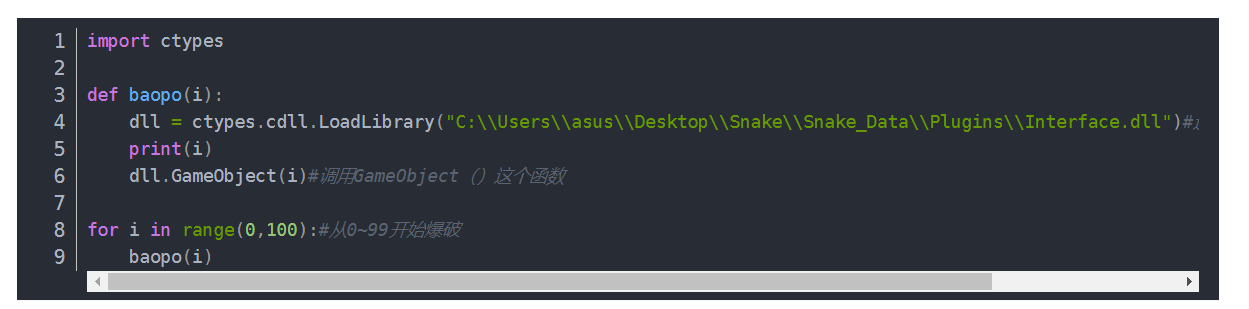


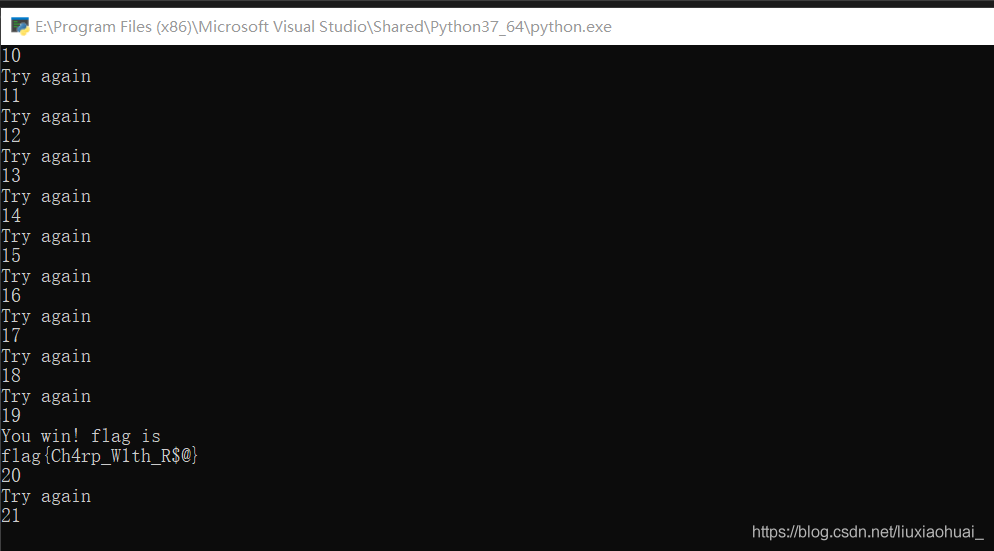
观察这个函数发现这个函数只有一个形参a1

并且接下来的函数操作都是在0<=a1<=99这个范围内进行的。



所以我们接下来直接上脚本爆破它：





得到flag{Ch4rp\_W1th\_R$@}

(ps:这个爆破需要一定的时间我等了接近30分钟才爆破出来！！！)

————————————————

原文链接：https://blog.csdn.net/liuxiaohuai\_/article/details/111595325