西普学院 writeup 逆向工程 该题不简单

原创

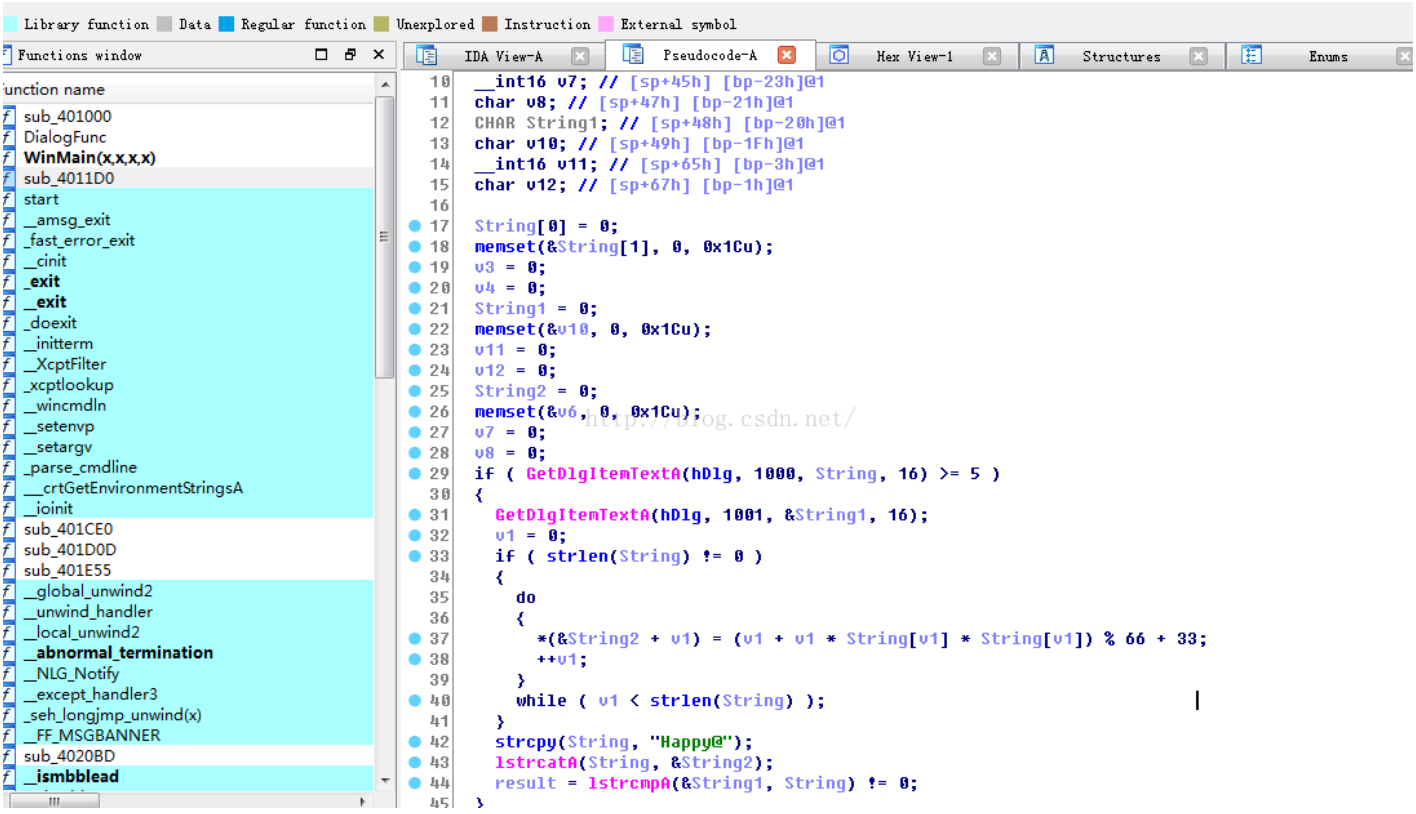
tiaotiaolong99234 于 2015-08-14 16:05:39 发布 1353 收藏
分类专栏： ctf 文章标签： writeup ctf 西普学院

跳跳龙

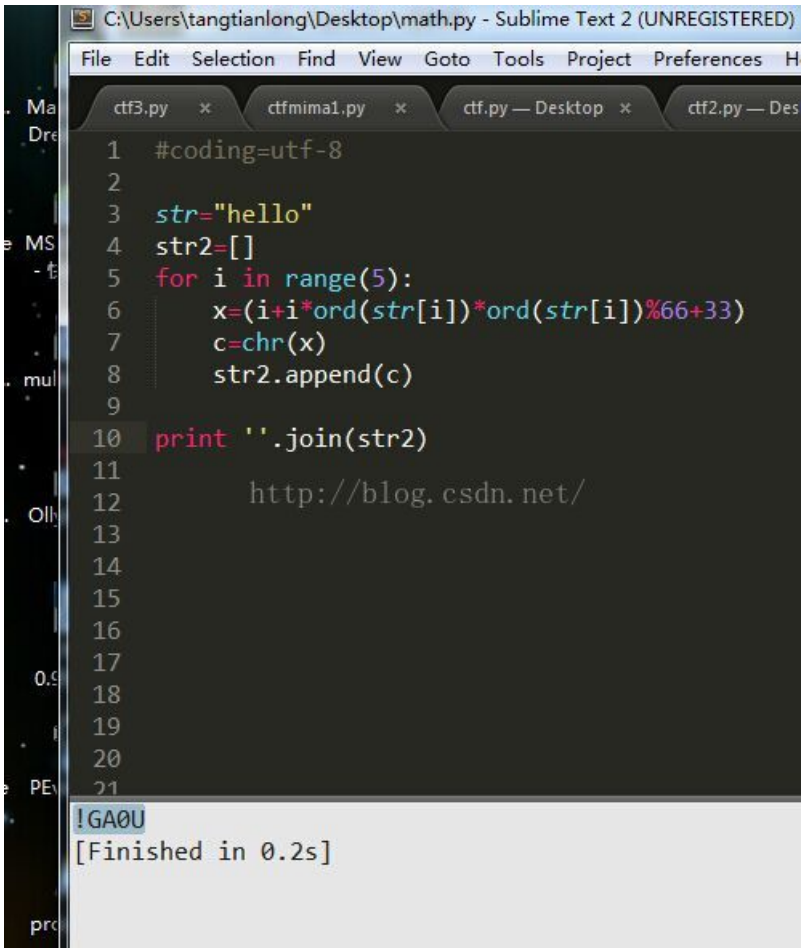
逆向的话主要就是IDA和OD的混合使用。两者各有优势，不过这道题用IDA就够了，而且OD的话貌似还调试不了，貌似加了保护。

IDA逆向的结果如下：IDA对windowsAPI逆的真心不错。

故事发生在这个函数：



我就不解释了，加密的算法还是很清楚的，然后我用py简单写了一下：



再看一下IDA，结果是拼接了一下，大家要对WINDOWS的API熟悉。答案就是Happy@!GA0U