**困惑的 flxg 小程序**

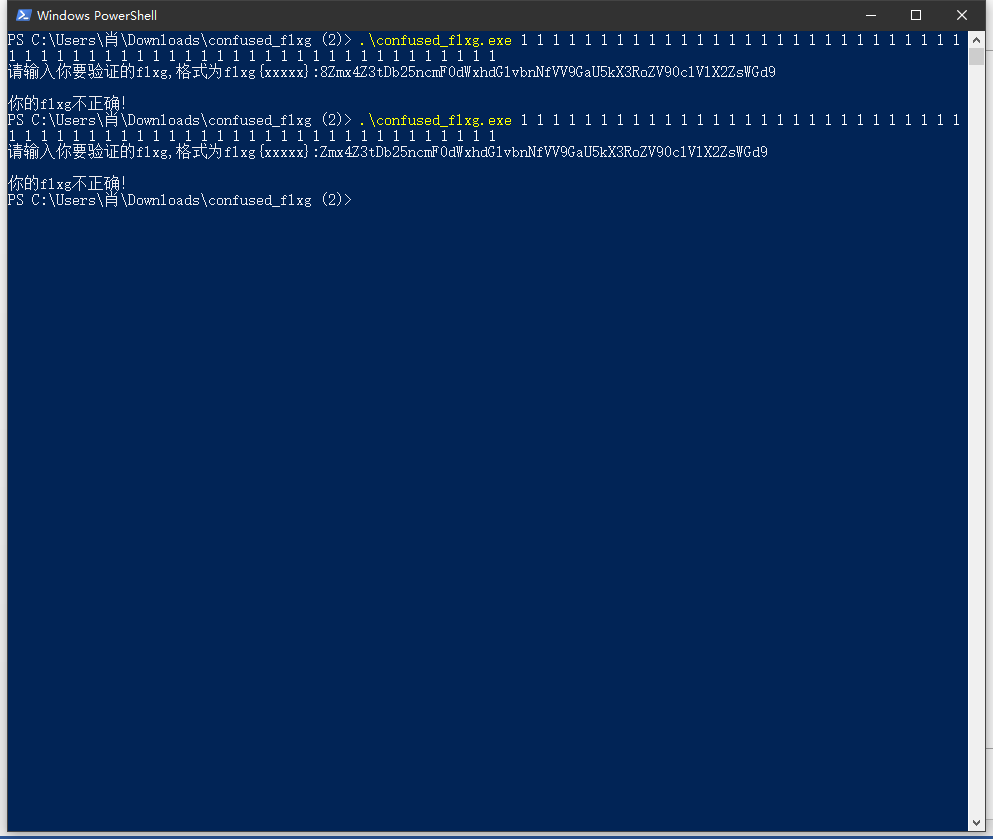
WP

先打开随便试试，发现得到一个假的flag，拖进ida，



发现当命令行参数为60个时会进行异常处理，大于或小于60都不是我们的预期

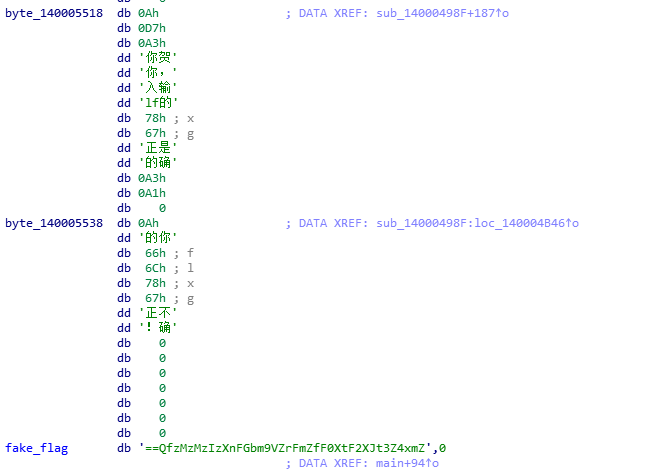
便构造60个命令行参数



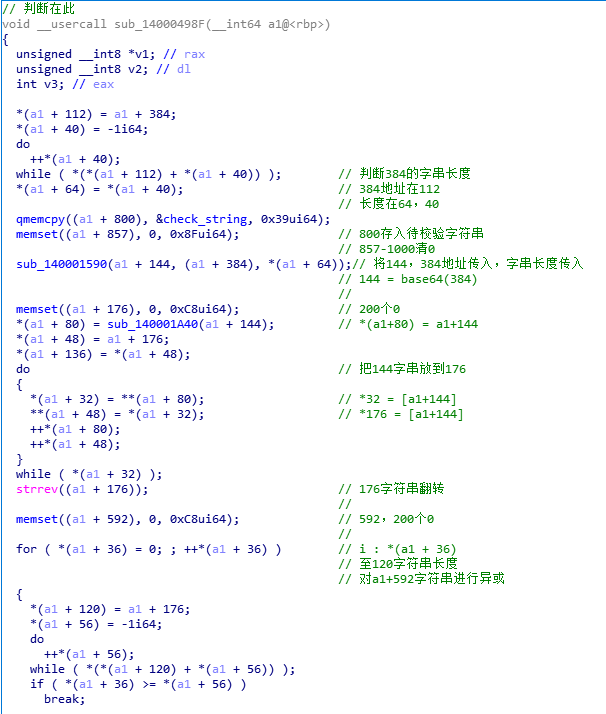
这图是后来截的

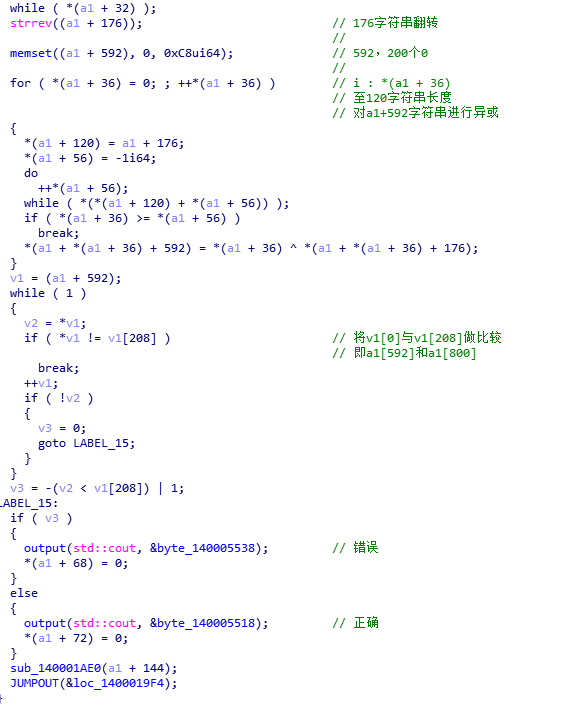
我们发现了，出现了你的flag不正确！这句话，

其实我们也可以通过strings窗口，找一下字符串，不过本题是中文，我们需要用R键手动对数据进行转换，找到



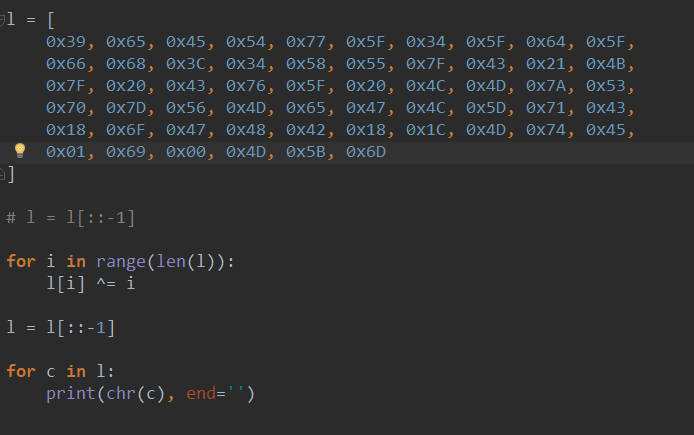
用X发现他是在异常处理函数中被引用，我们便知道了真正的判断在异常处理函数中进行。

转到异常处理函数，比较复杂，不过只要你耐心分析+动态调试，你便能发现，大部分是混淆代码



其中含有两个函数，通过x64dbg动态调试，改变程序控制流来到异常处理函数，观察修改的堆栈位置的数据，便可以知道他们的用途

导出需要比较的数据，用脚本进行还原，



得

Zmx4Z3tDb25ncmF0dWxhdGlvbnNfVV9GaU5kX3RoZV90clVlX2ZsWGd9

通过base64还原得：

flxg{Congratulations\_U\_FiNd\_the\_trUe\_flXg}