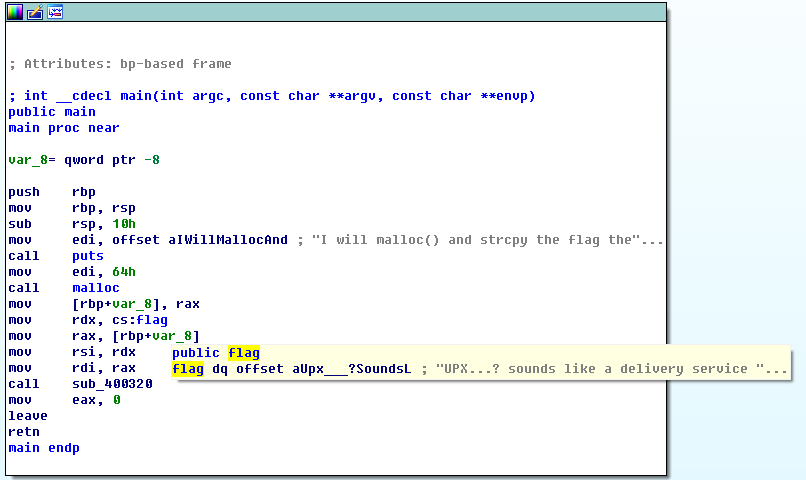
Flag类型的题目

1：题目网址： <http://pwnable.kr/bin/flag>

1. 用虚拟机打开 Firefox ESR 打开上述网址进行下载题目flag
2. 然后从终端中 xxd flag 发现flag 被UPX加壳了，这时候需要upx解壳。
3. 解壳之后把文件改成后缀elf 然后拖出来主机桌面上，这时候再用IDA进行反汇编
4. 用64位的IDA进行反汇编，得到主函数界面具体如下：



在 主函数中很快能够看见 flag 这个最后的引号 便是反汇编出的flag输入内容。

知识点：

1. 是否被upx加壳 网址：<http://blog.csdn.net/zacklin/article/details/7419001>
2. IDA 反汇编 由于我也不是太熟悉这个工具，简单的介绍它的工具的使用：

<http://www.cnblogs.com/vento/archive/2013/02/09/2909579.html>