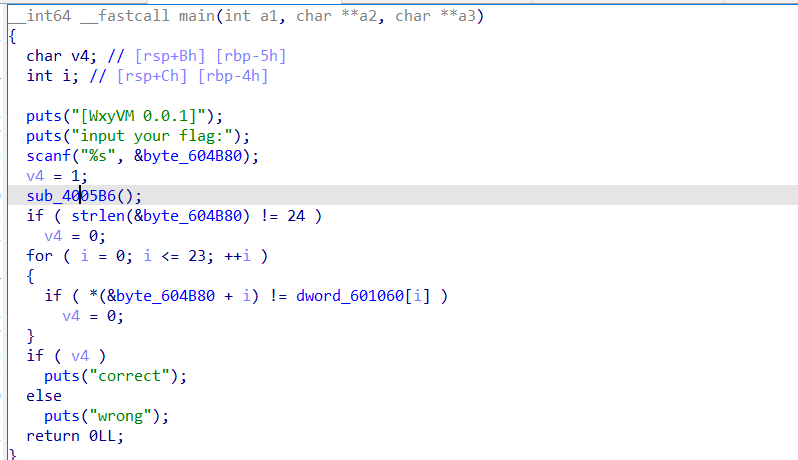
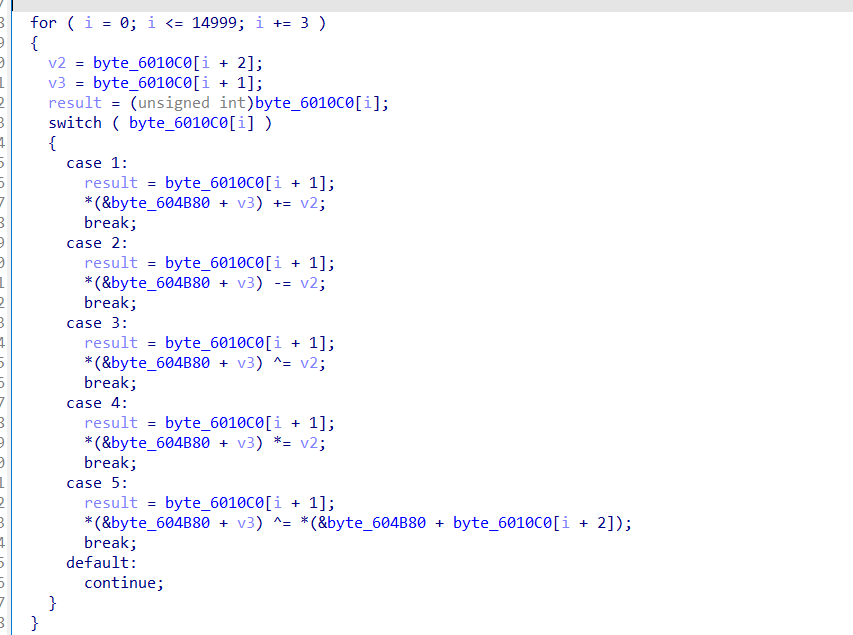
先放入die里查看文件类型确定为64位的elf

丢入ida：



再看看sub\_4005B6函数



这个result完全没什么用

并且按照步长为打印出byte\_6010C0后，发现switch语句中只有1，2，3这三种情况

这里有个很关键的两个点是：

1.dword\_601060数组内的数据是双字，而我们输入的字符的十六进制格式是单字节，所以需将双字数据取最低的八位再来运算

也就是进行&0xff或者%256取模

1. 最后得到数据还需要进行数据溢出处理，控制数据溢出。因为python的变量没有溢出之类的概念，所以还需要再对最后的数据进行&0xff（也可以%256）

