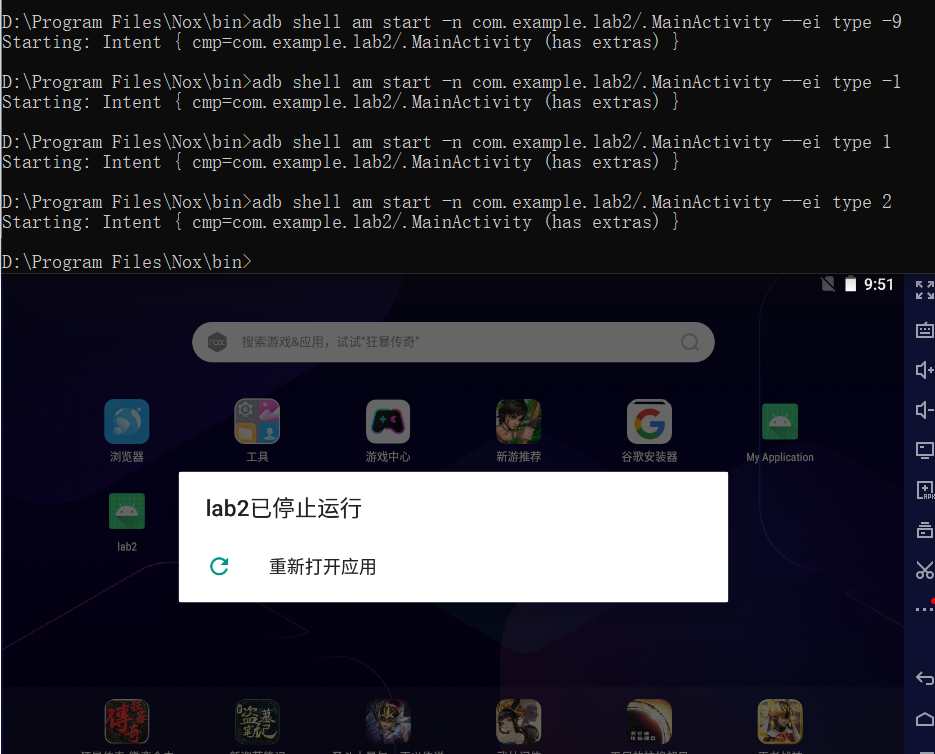
**Lab 2. Android App Reverse II**

* **Task A**

(1) Your Answer

[If you choose to write an app to send the Intent, please submit the APK to the Git server and copy the Intent-sending code here.]

发送意图的指令是：adb shell am start -n com.example.lab2/.MainActivity --ei type 2以及其他，具体的内容如下，改变参数为1、-9、2等可以使得程序停止运行，而参数为-1时不会停止

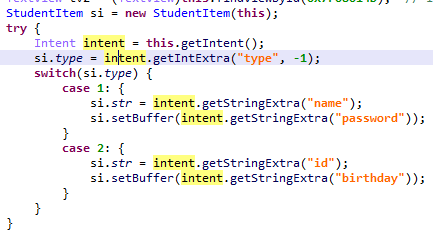


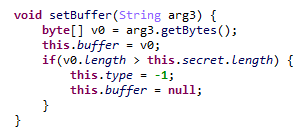
(2) Writeup

[Record how you solve this task here.]

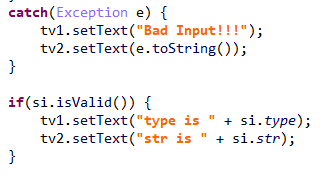
在获取意图的地方用到了getIntExtra()函数，如果传入的mValue有效则si.type的值就是这个有效值，否则就是默认的-1.然而在输入有效值（除了-1之外的其他数值）之后，程序会运行到setbuffer，读取到一块空的null区域，导致程序崩溃。

意图首先是传进一个参数，这个参数是“type”类型且有效的话，这个参数就赋值给si.type，不然si.type就为-1，上面定义的type是int类型的，就是说传进来的第一个参数应该是一个int类型的参数。如果只传一个参数，改变参数为1、-9、2等可以使得程序停止运行，而参数为-1时不会停止，这说明只传一个参数进去，程序往下会运行到setbuffer并读取到一块空的null区域，导致程序崩溃。



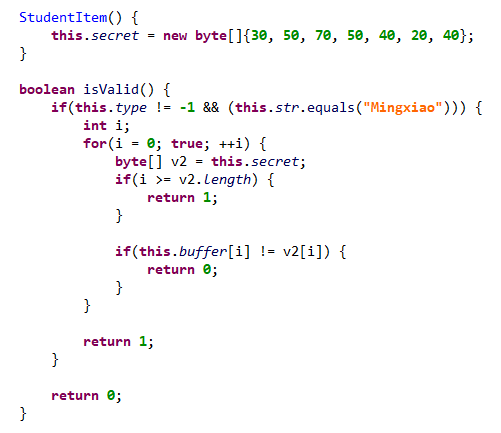


除此之外，如果按照代码的逻辑，我们还可以得到一个bad input的输出结果，如下图所示，这是我们在传进第一个参数之后再传几个参数进去之后的结果，传输的指令是——adb shell am start -n com.example.lab2/.MainActivity --ei type 1 --es name xiaoming --ei password 122，运行到chatch()后面并截获内容：

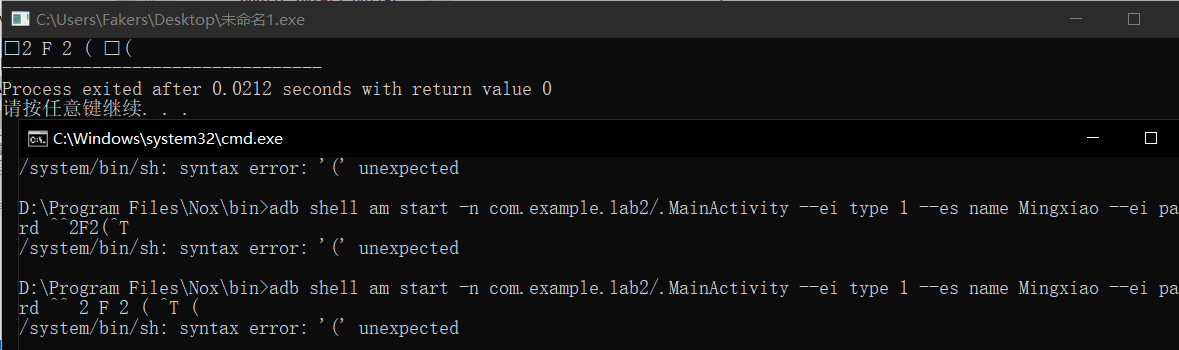




接着又尝试了其他传入数据，传id/password进去，发现程序也会崩溃,尝试着使得输出的内容按照isValid给出，但是由于ASCAII码20对应的字符不可显，无法完成这部分操作：

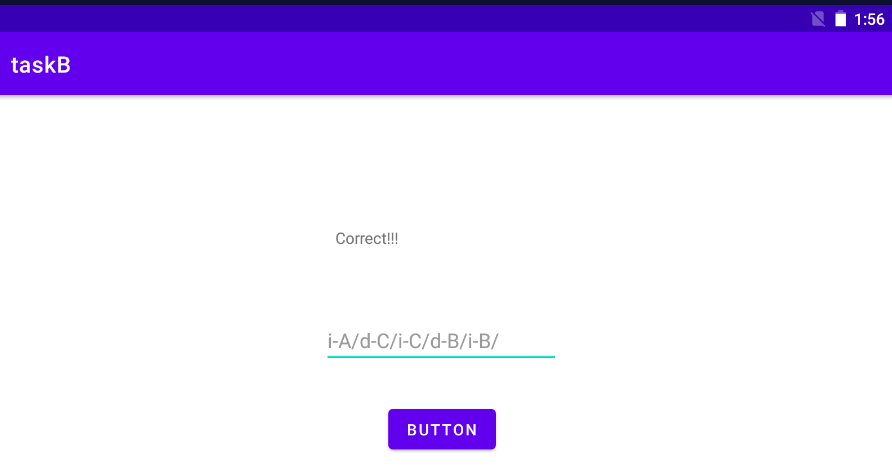






* **Task B**

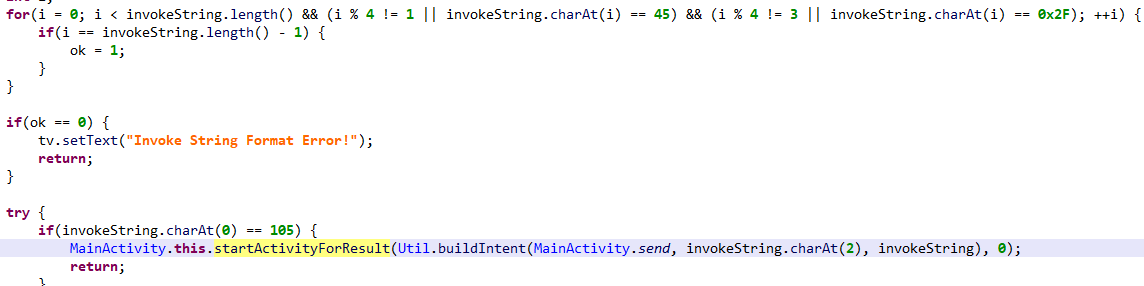
(1) Your Answer



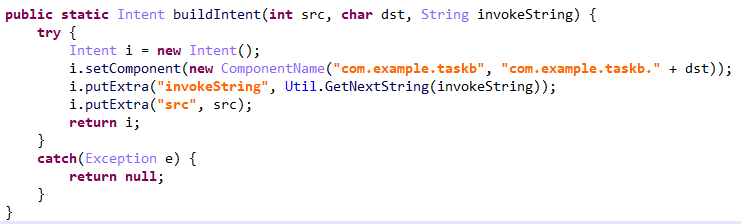
(2) Writeup

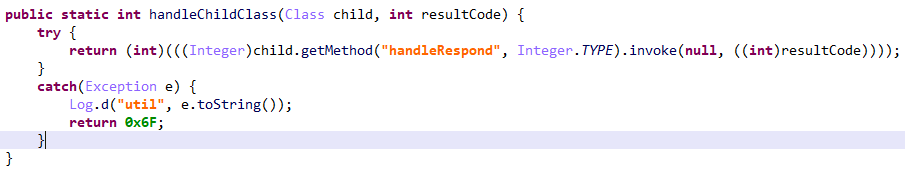
[Record how you solve this task here.]

onActivityResult()当中显示如果arg5==900则输出界面是correct，那么就寻找arg5在代码中的是如何计算出来的，顺着程序的逻辑往下读一步一步解决问题：

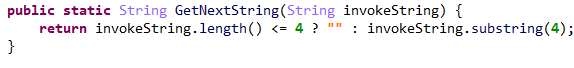


首先要解决的是ASCII码为45、0x2F、105、100分别代表什么，以便于使得输入的序列可以满足达到最终成功输出的所有“ok”都为1，容易直到他们分别代表符号- / i d 这样就可以继续往下探讨每一层调用的方向。





结合class中对Util的调用并观察Util模块当中的两个函数，他们分别实现了1、把本层调用的classT1当中的send推向下一层classT2并作为下一层（classT2）的src，并行地截取输入序列的后面内容。2、将下一层classT2的replyValue在T2的handleRespond映射之后的值作为返回值



在Util中也可以看出输入的执行序列是每四个一组，且为了使得mainActivity当中识别序列之后的ok为1输入序列的格式就是“(i或者d) - (要跳转到的class,A or B or C) /”,结合每个class当中reply(true)的需要，传输的src也就有了固定的方向——iA,从class A进入，这是因为class A 最后的replyValue值是900符合最终需要；dC,为了实现 class A 的需要，向下递归到class C，调用C中的响应函数将 A.send改成300以便传输作为Ｃ的src……

以此类推最终得到答案序列ｉ－Ａ／ｄ－Ｃ／ｉ－Ｃ／ｄ－Ｂ／ｉ－Ｂ／