**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.]

我没有发送Intent，我通过阅读代码发现错误，有关于发送的漏洞：

在 **StudentItem** 类中，**buffer** 字段是从意图中获取的，没有对其进行任何安全检查，存在缓冲区溢出或其他类型的漏洞风险。

**setBuffer()** 方法中的输入没有经过任何验证，因此可能会导致缓冲区溢出或其他类型的漏洞风险。

在 **onCreate()** 方法中，**type** 字段的值是从意图中获取的，但是没有对其进行任何安全检查，存在可能的安全漏洞风险。

(2) Writeup

[Record how you solve this task here.]

修改onCreate()方法,通过对type检测后在进行录入保证安全。

@Override

protected void onCreate(Bundle savedInstanceState) {

* super.onCreate(savedInstanceState);
* this.setContentView(0x7F0B001C); // layout:activity\_main
* TextView tv1 = (TextView)this.findViewById(0x7F08014C); // id:textView
* TextView tv2 = (TextView)this.findViewById(0x7F08014D); // id:textView2
* StudentItem si = new StudentItem(this);
* Intent intent = getIntent();
* int type = intent.getIntExtra("type", -1);
* switch (type) {
* case 1: {
* String name = intent.getStringExtra("name");
* String password = intent.getStringExtra("password");
* if (name != null && !name.isEmpty() && password != null) {
* si.str = name;
* si.setBuffer(password);
* si.type = type;
* }
* break;
* }
* case 2: {
* String id = intent.getStringExtra("id");
* String birthday = intent.getStringExtra("birthday");
* if (id != null && !id.isEmpty() && birthday != null) {
* si.str = id;
* si.setBuffer(birthday);
* si.type = type;
* }
* break;
* }
* }
* catch(Exception e) {
* tv1.setText("Bad Input!!!");
* tv2.setText(e.toString());
* }
* if (si.isValid()) {
* tv1.setText("type is " + si.type);
* tv2.setText("str is " + si.str);
* }
* }

**Task B**

(1) Your Answer

i-A/d-C/i-C/d-B/i-B/

(2) Writeup

[Record how you solve this task here.]

通过代码知道，要开启下一个Activity第一个字符必须为’I’，每4个字符第二个字符必须为’-’，每4个字符第四个字符必须为’/’。

经过看代码发现想要打印Correct必须要传入MainActivity的resultCode为900，而与900有关的只有文件A，而A要输出900必须要resultCode为1000，与1000有关的只有文件C，而C要输出1000必须要resultCode为1200，与1200有关的文件只有文件B。

要在进入C前进行C处理才能使src为300，要在进入B之前进行B处理才能使src为500.