**暨 南 大 学**

**本科生课程论文**

**论文题目： 我要记账APP开发**

**学 院： 智能科学与工程学院**

**学 系：**

**专 业： 信息安全**

**课程名称： 移动软件开发与安全**

**学 期： 2021~2022年第一学期**

**学生姓名： 邱湘鹏**

**学 号： 2019051108**

**2021年 12 月 日**

目录

[第1章 我要记账APP开发 3](#_Toc90149923)

[1.1 软件需求及功能分析 3](#_Toc90149924)

[1.2 Activity设计 3](#_Toc90149925)

[1.3 关键实现技术 3](#_Toc90149926)

[1.4 测试及使用说明 5](#_Toc90149927)

[1.5 开发过程说明 7](#_Toc90149928)

[1.6 有待完善的地方 8](#_Toc90149929)

[第2章 Android安全调查 9](#_Toc90149930)

[第3章 总结及课程感想 11](#_Toc90149931)

# 我要记账APP开发

## 软件需求及功能分析

软件需要能有增删改查相关记录的功能。增加的记录需要进行细分，如可以分为是收入还是支出，是什么事件的收支等。删即删除指定的记录。改指要能在一定范围内更改指定记录的信息。查即实现账目浏览以及简单的分析统计。

## Activity设计

本项目包含5个Activity。

1.activity\_main：作为app首页，主要是简单的布局和一个ViewPager2用其适配器来装载RecycleView。

2. activity\_fragment\_main：数据记录的展示的部分。放置RecyclerView以及跳往增加记录页面的按钮。代码处设计RecyclerView的适配器。并使此页面能获得其他Activity传回的数据，将数据展示在相关视图，并实现改变和删除等各种功能。

3. activity\_expenditure\_record：支出数据项设置的地方。设置了许多按钮及相关响应，可以在此页面设置金额、日期、类别等，并可通过按钮跳转到收入activity。

4. activity\_income\_record：收入数据项设置的地方。设置了许多按钮及相关响应，可以在此页面设置金额、日期、类别等，并可通过按钮跳转到支出activity。

5. activity\_item：设置RecyclerView中每一个条目布局以及类的信息设置。

## 关键实现技术

1. 支出或收入设置界面，每一个图标都是ImageButton，通过设置按钮点击监听事件，当点击时切换图片，并记住这次点击的视图。点击下一个视图时将上一次点击的按钮视图恢复。

2.不同Activity之间信息的传递使用registerForActivityResult，启动一个activity需要一个laucher，这个laucher由registerForActivityResult返回，这个方法有两个参数，一个参数为一个抽象类ActivityResultContrac的实现，另一个参数是一个函数式接口的实现。

3.进入APP的主界面，由两个Activity组成。Main设置进本布局和ViewPager2，用有RecyclerView的布局通过viewPagerFragments装入。RecyclerView的每一项使用RecyclerView.Adapter设置。ViewPager的功能就是可以使视图滑动，用于实现多页面的切换效果,其直接继承了ViewGroup类，所以它是一个容器类 。使用时需要一个PagerAdapter适配器类给它提供数据，来完成页面数据的绑定，这个PagerAdapter是一个适配器基类。ViewPager经常和Fragment一起使用。ViewPager2在ViewPager的基础上规定了统一使用FragmentStateAdapter以及PagerAdapter统一使用RecyclerView.Adapter等。

Fragment是一个界面的一部分。主要是用于屏幕分辨率的问题。比如pad的读书软件就和手机上的读书软件不同，因为他们的尺寸不同，所以对同一产品需要设计不同的软件，而Fragment正好解决这个问题，只需做一个软件，让软件自动适应屏幕。Fragment必须是依存与Activity而存在的，因此Activity的生命周期会直接影响到Fragment的生命周期。

对于Adapter，Android是完全遵循MVC模式设计的框架,Activity是Controller,layout是View 。因为layout有数种布局,很多数据不能直接绑定上去,因此Android使用Adapter，作为复杂数据的展示的转换载体,各种Adapter只是转换的方式和能力不一样。Adapter常用来管理数据，使数据绑定到控件变得更简单灵活（比如列表的数据，网格的数据），为容器提供子视图，利用视图的数据和元数据来构建每个子视图。

4.日期的设置使用java Calendar类获取，并使用安卓自带的DatePickerDialog控件可视化选取日期。

5.存储数据方法：将相关数据存入私有目录中的文件，使用输入输出流读取文件内容。

6.类按日期排序：首先类要继承相关接口并重写接口的比较函数，让它按日期格式比较



public int compareTo(item\_setting o) {

SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");

Date a = null;

try {

a = sdf.parse(this.Date);

} catch (ParseException e) {

e.printStackTrace();

}

Date b = null;

try {

b = sdf.parse(o.getDate());

} catch (ParseException e) {

e.printStackTrace();

}

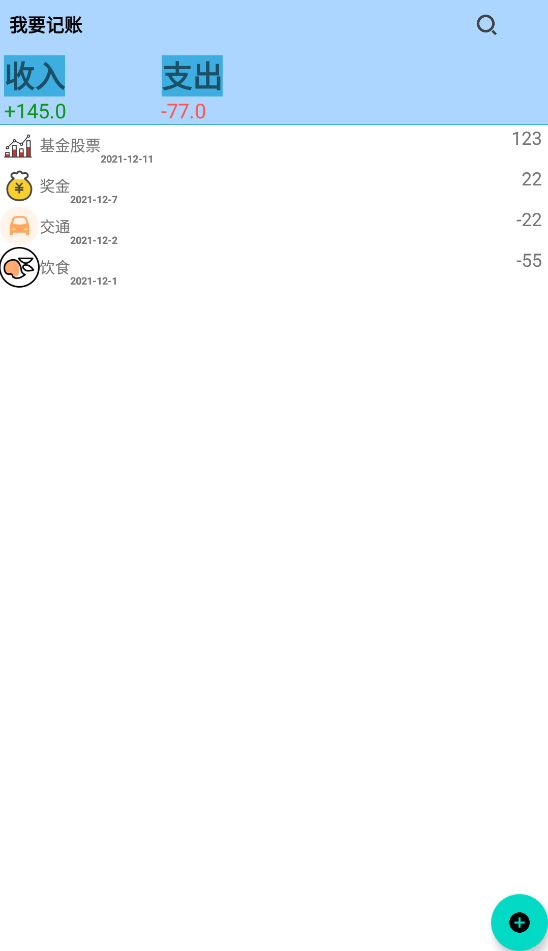
return a.compareTo(b);

}

之后在需要排序的地方调用Collections.sort()对相关数据进行排序即可。

## 测试及使用说明

1.主界面

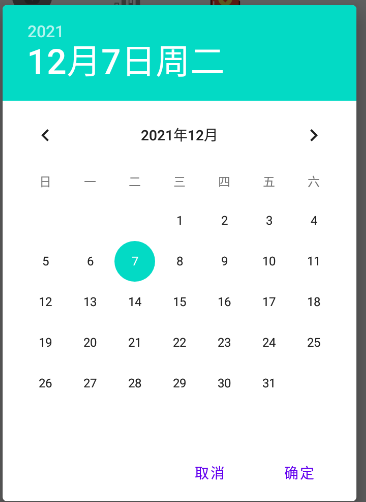


主界面的设计为上面一部分显示总收入和总支出情况，下面显示记录的具体信息，右下角的按钮进入记账页面。每个信息会按照日期降序排序。

2.记账页面



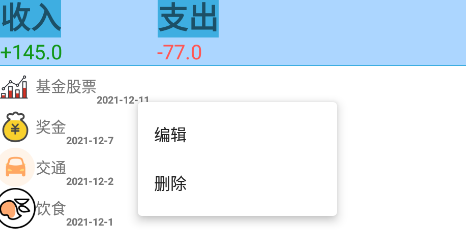
记账页面上方的支出、收入按钮指跳转到记录支出或收入页面，确定则是填完信息后点击返回主页面。也可以什么都不填按左上角的×返回。下方类别按钮点击后会显示为选定的图片，如果想选另一个类别，只需直接点另一个，原来选中的按钮会自动变为非选定状态。设置日期按钮点击后会出现一个日历控件。



点击上面的年可以设置年份。

设置完后回主界面会更新相应内容。

3.对着要修改的项长按会跳出选择菜单



点击编辑会跳转到设置页面，会依据支出或者收入信息优先跳转到该页面，并传递且自动设置此信息的金额和日期信息。



重新设定日期后主界面会将信息按日期重新排序显示



删除按钮则将该条信息从当前位置删除。

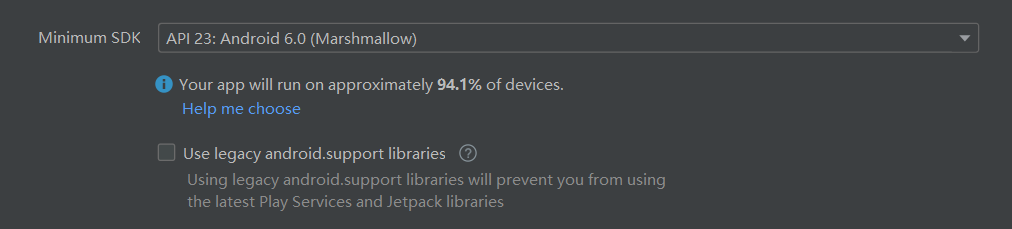
## 开发过程说明

软件开发环境，开发过程，Github网址等。

1.Adroid Stdio版本



2.SDK版本



3.开发过程

1.开始先进行各个Activity的布局设计，然后将想法用适当的控件实现，去网上找各个按钮的Icon以及对layout背景按钮等尝试不同的颜色使界面看着更美观。使用一个变量保存上次点击信息的方法实现图标的变化与自动恢复。并设置每个item的布局。调整布局位置与找图标和为每个按钮设置点击事件较花时间。



每个item设计为最左边存放收入/支出类型的图片，在图片右边设置类型名，在类型名下面设置记录日期，最右边记录此项金额。

2.考虑各个Activity怎么互相连接，数据怎么互相传输。最终决定使用按钮进行页面的跳转，使用ActivityResultLauncher来实现Activity间的信息传递。为了配合用按钮进行支出、收入页面跳转的设计，在registerForActivityResult中设置判断，如果传回的数据中有表示跳转页面的特殊值就将当前信息传入要跳转的页面。进行Adapter的配置重写。调试实现界面间的成功跳转以及传递要的数据，并成功实现RecyclerView的记录功能，成功实现增的功能。此阶段容易出现各种数据没有初始化或者变量名不匹配或者考虑缺失等情况，从而导致某个页面无法初始化造成程序崩溃，如保存每个item的list需要new 一个ArrayList<>()类，传递时收到点击某个按钮的事件后要将需要的变量重赋值以及将变量放入intent。此处因为变量较多以及有几种不同的情况，传变量时容易写漏，打断点补全花了较多时间。

3.进行删改功能以及数据保存的实现。在重写的RecyclerViewAdapter里添加onCreateContextMenu函数实现Recycler中的项长按菜单，添加onMenuItemClick实现点击删除或更改功能。

然后考虑如何进行数据的保存。大概找到三种实现方法，一个是存入私有目录中，一个是存入指定文件还有一个是用数据库存储。如果用数据库存储要改变之前的设计，指定文件在其他设备上可能会有问题，所以最终选择存入项目带的默认目录中。决定实现方法后将读取与保存语句添加到每个数据发生改变的地方。

4.添加时间以及总支出、收入统计的简单显示。网上查找实现设置时间的方法，添加一个按钮设置时间，更改单个item的布局，重写相关的类以及增加传输的数据，要在每个需要的地方按逻辑增加时间的传递与设置，花费较多时间。

5.Gitee网址: <https://gitee.com/qxp123/woyaojizhang>

## 有待完善的地方

1.对于设置每一项相关信息的界面更好的方法是使用ViewPager2和TableLayout装载支出和收入页面。用Fragment设置每个按钮，让他们能自适应设备。

2.设置抽屉布局做为历史查看、分析统计的入口，补充相关功能。

3.按钮的响应应该有其他方法来减少代码量。

4.代码模块梳理的更清楚一点，将类的定义与功能的实现分开。

# Android安全调查

安卓开发由对应的编程语言以及安卓相应的类和组件（Activity、Service、BroadcastReceiver、ContentProvider 等）构成。所以安卓安全包括了所使用的语言语法、使用安全以及安卓组件相应特性的安全。

以JAVA语言开发安卓程序为例，对于程序交互的基本功能输入输出，就可能遭受到DoS攻击（洪泛攻击）。如BufferedReader.readLine当接收到无限长度的行，不包含换行/回车的巨大文件时

会使StringBuilder 变量的内存资源耗尽。一般解决方法为进行输入输出流限制。因此安全涉及到每一个基础点。以下是几个注意事项的例子：

1.静态字段

应尽可能地避免使用非final公共静态变量，因为无法判断代码有无权限改变这些变量值。甚至可能导致设想中相互独立的子系统之间发生不可预知的交互。

2.访问权限

尽可能缩小方法和字段的作用域是一个惯例。如检查包访问权限的成员能否改成私有的，保护类型的成员可否改成包访问权限的或者私有的。对于公共变量应尽量避免直接访问，通过函数和接口进行获取和修改。对于任何公共方法，如果它们能够访问或修改任何关键的内部状态，要使它们包含安全控制，如进行权限或者条件判断的访问限制。

3. 对象序列化

当要通过网络传输一个对象数据(例如从一个JVM传输到另一个JVM)时，需要将对象实例转换为字节序列。这时需要调用Serilizable接口，对一些敏感信息（如密码，银行卡号等），为了安全起见，不希望在网络操作（主要涉及到序列化操作，本地序列化缓存也适用）中被传输，这些信息对应的变量就需要加上transient关键字。如果资源，如文件句柄，不被声明为transient，该对象在序列化状态下可能会被修改，从而使得被反序列化后获取对资源的不当访问。

4.敏感信息及时清除

当保存敏感信息时,尽量保存在如数组这样的可变数据类型中，而不是保存在字符串这样的不可变对象中，这样可得敏感信息可以尽早显式地被清除。最好进行手动显示清除，因为回收器可能不会清除这段内存，或者很久后才会回收。尽早清除信息能有效使得来自虚拟机外部的堆检查攻击变得困难。

其他安全问题主要有:框架低版本漏洞、空指针的引用、整数溢出、命令注入、SQL注入、XSS及CSRF、跳转漏洞、HTTP Response Splitting漏洞、路径可控制及代码注入、资源泄露及对象相等、线程安全等。

对于安全漏洞查找这一问题，一般对代码的安全测试都是与一个应用程序进行交互，通过设计输入及观察相应内容两个步骤进行。检查方法需要根据经验设计，但普遍有以下三种方法：

1.从进入点开始跟踪用户向应用程序提交的数据，审查负责处理这些数据的代码

2.在代码中搜索表示存在常见漏洞的签名，并审查这些签名，确定某个漏洞的真实存在

3.对内在危险的代码进行逐行审查，理解逻辑，并确定存在的问题

此外使用一些工具协助查找和进行提示来提高效率。

对于安卓组件特性安全，基本点与以上相同，以下列举几个安卓安全的特别例子：

1. android:allowbackup 属性必须设置为 false，阻止应用数据被导出

android:allowBackup 是 Android 提供的 adb 调试功能，如果设置为 true，可以导出应用数据备份并在任意设备上恢复。这对应用安全性和用户数据隐私构成极大威胁，所以必须设置为 false，防止数据泄露。

2. 程序进行网络通信时，如果使用自定义 HostnameVerifier 实现类，必须在 verify()方法中校验服务器主机名的合法性，否则可能受到中间人攻击。在与服务器建立 https 连接时，如果 URL 的主机名和服务器的主机名不匹配，则可通过该回调接口来判断是否应该允许建立连接。如果回调内实现不恰当，没有有效校验主机名，甚至默认接受所有主机名，会大大增加安全风险。

3. 在 SDK 支持的情况下，Android 应用必须使用 V2 签名，这将对 APK 文件的修改做更多的保护。android7.0引入了V2签名方式。对比V1最大的区别是V1是先解压存档文件,在对其中内容进行计算验证。而V2签名是在整个apk文件的二进制内容上计算和验证的，并且V2签名的apk不能再修改，比如解压，解压之后签名会失效。所以，用V2签名后，apk的安装速度会变快(省去解压过程)，安全性会有保证(对整个apk验证)。

4. 所有的 Android 基本组件都不应在没有严格权限控制的情况下，将 android:exported 设置为 true。

5. 确保应用发布版本的 android:debuggable 属性设置为 false。

6.不要把敏感信息打印到 log 中

在开发过程中，为了方便调试，通常会使用 log 函数输出一些关键流程的信息，这

些信息中通常会包含敏感内容，让攻击者更加容易了解 APP 内部结构，方便破解和

攻击，甚至直接获取到有价值的敏感信息。

还有许多具体的点无法简单说完，总的来说安卓安全和其它开发安全本质上应遵守的基本准则是一样的，而具体如何遵守这些标准与规则需要具体的学习，熟悉安卓特性并做长期积累。

# 总结及课程感想

课程从最基础的Android Studio安卓程序项目创建开始讲起，包括RelativeLayout与LinearLayout等基础布局的使用，Activity间的各种操作，各种安卓进本控件如Recyclerview、Fragment、WebView、SurfaceView等的用法，还有网络与程序交互等安卓程序各种重要功能的实现方法。

通过课程的学习，我学到了移动软件开发的基本思想，一些简单功能的实现方法，以及诸如git、网络交互获得数据等的软件必要操作的熟悉，建立起了对于移动软件开发比较全面的概念。通过对相关开发安全注意事项资料的查阅，对移动软件开发安全有了一些基本的了解。

随着学习的深入，我也感受到移动开发是建立在JAVA等语言开发之上的广阔领域，其功能以及安全的实现需要结合很多计算机知识。对于本课程的感想，个人觉得本课程讲解的内容基础且细致，很适合新手入门。特别是随着实验的进展，能很好的感受与建立移动开发的基础知识。课程难度适中对于不想做开发工作的同学来说是一次很好的体验，对于想做开发工作的同学来说能起到引领作用。是一门内容设置合理的好课。