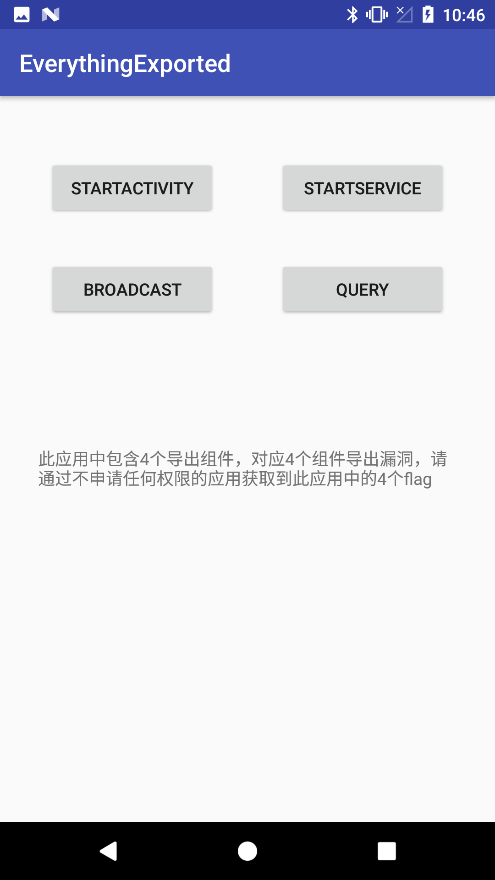
组件暴露漏洞练习APP

设计思路：

包含四种组件，Activity, service , content provider , broadcast receiver

1. FlagActivity暴露，接收一个username与 password的extra，并在 setResult中返回flag1。
2. FlagService 实现了onBind与onTransact，其它应用可以使用binder与其进行通信，实现了两种code，0x1为flag2，在binder中放入username与password，验证通过后即会在 reply 中返回 flag2。0x2留作其它用
3. FlagReceiver接收广播，由于未作权限限制，未提高优先级，可被其它应用实施广播拦截，发送广播flag的操作在 FlagService的0x2请求。
4. FlagProvider是一个导出的flag，只实现了query请求，可以任意查询指定的数据库内容，造成数据库的泄露。

界面如下：



Exp：详见代码。

1. 实现 startActivity 以及 onActivityResult，接收flag1

2. 实现使用binder与service进行通信，发送parcel数据并接收reply中的flag2

3. 实现使用binder与service进行通信，并注册广播接收flag3

4. 经过简单的逆向分析，通过content://URI 访问目标应用数据库中的数据并获取 flag4

