Đại học Quốc gia Thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin (UIT)

BÁO CÁO BÀI TẬP

Môn học: Bảo mật Web và Ứng dụng

Bài tập buổi 9:

Android Security

GV: Nghi Hoàng Khoa

Ngày báo cáo: 19/05/2023

Nhóm: Pengu

1. THÔNG TIN CHUNG:

Lớp: NT213.N21.ANTT

STT	Họ và tên	MSSV	Email
1	Phạm Phúc Đức	20520162	20520162@gm.uit.edu.vn
2	Nguyễn Hoàng Phúc	20520277	20520277@gm.uit.edu.vn
3	Nguyễn Đức Tấn	20520751	20520751@gm.uit.edu.vn
4	Nguyễn Nhật Hiếu Trung	20520830	20520830@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:[1]

STT	Công việc	Kết quả tự đánh giá	Người đóng góp
1	Phân tích các ứng dụng android của 1 công ty.	100%	Cả nhóm
2	Viết 2 ứng dụng Android cơ bản có các tính năng kiểm soát truy cập lẫn nhau	100%	Cả nhóm

[1] Ghi nội dung công việc, các kịch bản trong bài Thực hành

BÁO CÁO CHI TIẾT

1. Phân tích các ứng dụng android của 1 công ty.

Sử dụng công cụ package viewer để xem các quyền của hai ứng dụng Facebook và Messenger của công ty Meta.

1.1. Thực hiện xem các quyền hạn được cấp của ứng dụng

a. Ứng dụng Messenger:

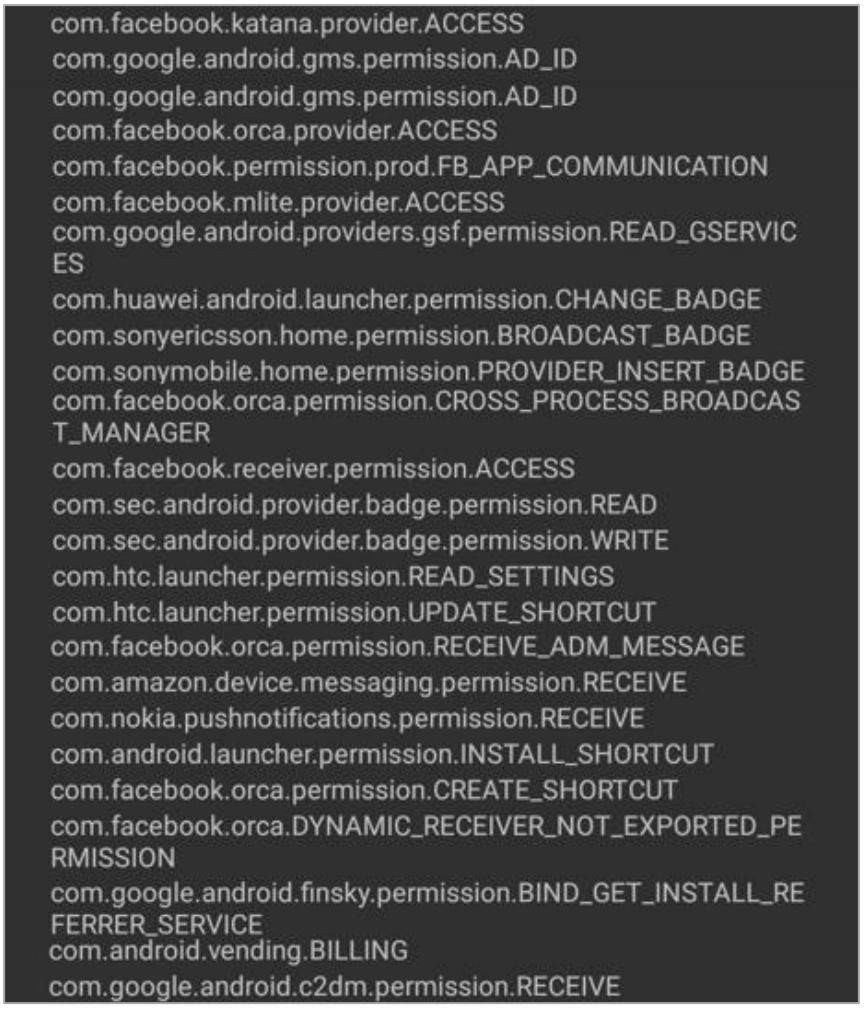
Hình 1: Các quyền được cấp cho ứng dụng Messenger

- android.permission.READ_MEDIA_AUDIO: cho phép ứng dụng đọc nội dung audio từ thiết bị.
- android.permission.READ _MEDIA_VIDEO: cho phép ứng dụng đọc nội dung video từ thiết bị.
- android.permission.READ_MEDIA_IMAGES: cho phép ứng dụng đọc nội dung hình ảnh từ thiết bị.
- android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATION: cho phép ứng dụng yêu cầu từ người dùng để được miễn trừ khỏi quá trình tối ưu hóa pin tự động trên thiết bị.
- ONS.android.permission.POST_NOTIFICATIONS: cho phép ứng dụng gửi thông báo trên thiết bị.
- android.permission.SCHEDULE_EXACT_ALARM: cho phép ứng dụng lập lịch đặt chính xác báo động hoặc thông báo theo thời gian cụ thể trên thiết bị.
- android.permission.INTERNET: cho phép ứng dụng truy cập internet trên thiết bị.
- android.permission.GET _ACCOUNTS [dangerous]: cho phép, ứng dụng có khả năng truy cập và đọc thông tin về tài khoản đã được cấu hình trên thiết bị.
- android.permission.ACCESS_NETWORK_STATE: cho phép ứng dụng truy cập trạng thái mạng trên thiết bị.
- android.permission.WAKE_LOCK: cho phép ứng dụng giữ thiết bị ở trạng thái hoạt động (awake) trong khi màn hình đã tắt hoặc thiết bị đã vào chế độ ngủ.
- android.permission.VIBRATE: cho phép ứng dụng có khả năng kích hoạt tính năng rung (vibrate) trên thiết bị.
- android.permission.READ_CONTACTS [dangerous]: cho phép đọc đọc các thông tin như tên, số điện thoại, địa chỉ email, địa chỉ và thông tin khác trên thiết bị.
- android.permission.READ_PROFILE:
- android.permission.WRITE_EXTERNAL_STORAGE [dangerous]: cho phép ứng dụng thêm xóa sửa dữ liệu bộ nhớ trên thiết bị.
- android.permission.READ _PHONE_STATE [dangerous]: cho phép ứng dụng đọc trạng thái số điện thoại trên thiết bị.

- android.permission.READ _PHONE_NUMBERS [dangerous]: cho phép ứng dụng truy cập và đọc số điện thoại trên thiết bị.
- android.permission.ACCESS_WIFI_STATE: cho phép ứng dụng truy cập trạng thái wifi trên thiết bị.
- android.permission.RECEIVE_BO0T_COMPLETED:
- android.permission.READ_SYNC_SETTINGS
- android.permission.RECEIVE_SMSs [dangerous]
- android.permission.RECEIVE_MMS [dangerous]
- android.permission.READ_SMS [dangerous]
- android.permission.WRITE_SMS
- android.permission.SEND_SMS [dangerous]
- android.permission.CHANGE_NETWORK_STATE: cho phép ứng dụng truy cập trạng thái của kết nối mạng trên thiết bị.
- android.permission.RECORD AUDIO [dangerous]: cho phép ứng dụng truy cập vào ghi âm trên thiết bị.
- android.permission.SYSTEMALERT_WINDOW
- android.permission.CALL_PHONE [dangerous]
- android.permission.MODIFY_AUDIO_SETTINGS:
- android.permission.DoWNLOAD_WITHOUT_NOTIFICATION
- android.permission.AUTHENTICATE_ACCOUNTS
- android.permission.MANAGE_ACCOUNTS
- android.permission.WRITE_CONTACTS [dangerous]
- android.permission.WRITE_SYNC_SETTINGS
- Android.permission.NFC: cho phép ứng dụng truy cập vào tính năng NFC (Near Field Communication) trên thiết bị.
- Android.permission.BLUETOOTH: cho phép ứng dụng truy cập vào tính năng bluetooth trên thiết bị.
- android.permission.CAMERA [dangerous]: cho phép ứng dụng truy cập vào tính năng camera trên thiết bị.

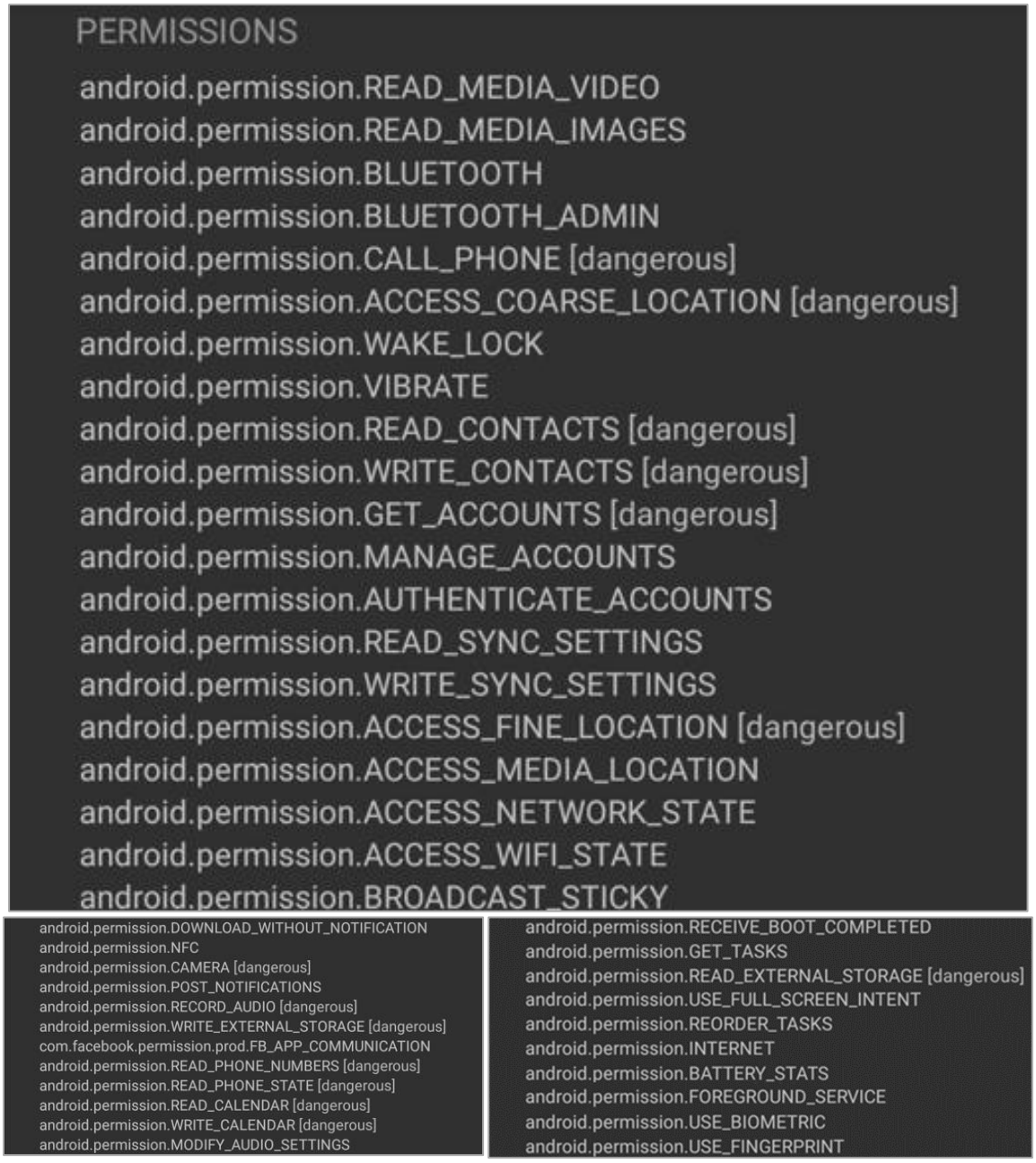
- android.permission.ACCESS_FINE_LOCATION [dangerous]: cho phép ứng dụng truy cập vào vị trí chính xát trên thiết bị.
- android.permission.ACCESS_COARSE_LOCATION [dangerous]: cho phép ứng dụng truy cập địa chỉ vị trí của các phương tiện truyền thông (media) trên thiết bị.

Các quyền hạn tùy chỉnh messenger được cấp:



Hình 2: Quyền hạn tuỳ chỉnh được cấp

b. Ứng dụng Facebook:



Hình 3: Permission được cấp cho ứng dụng facebook

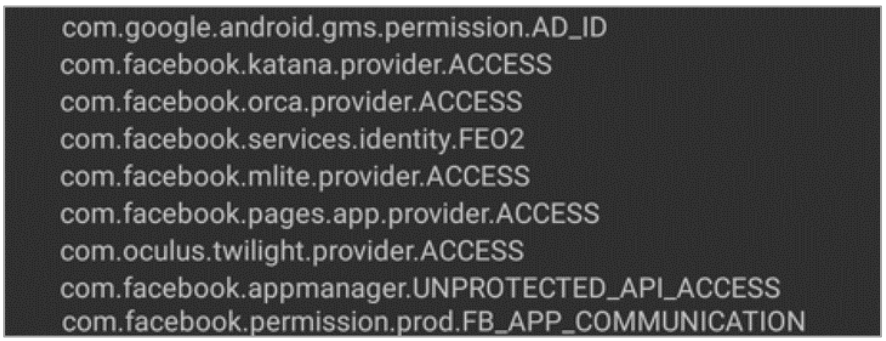
- android.permission.READ_MEDIA_VIDEO: cho phép ứng dụng đọc nội dung video từ thiết bị.
- android.permission.READ_MEDIA_IMAGES: cho phép ứng dụng đọc nội dung hình ảnh từ thiết bị.
- android.permission.BLUETOOTH: cho phép ứng dụng truy cập sử dụng Bluetooth từ thiết bị.
- android.permission.CALL_PHONE: cho phép ứng dụng truy cập vào chức năng gọi điện trên thiết bị.

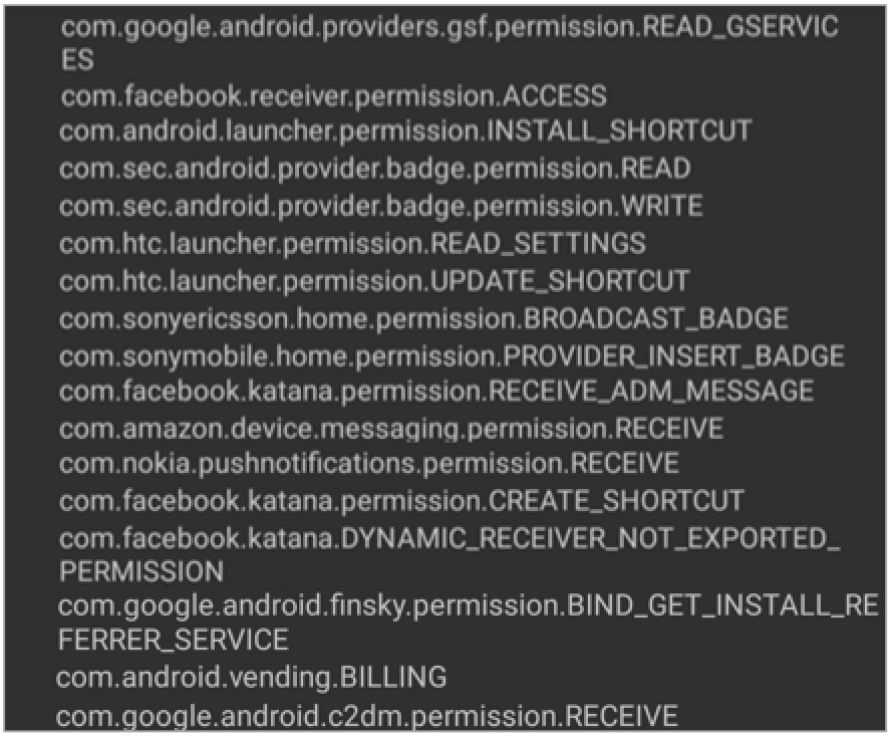
- android.permission.ACCESS_COARSE_LOCATION [dangerous]: cho phép ứng dụng truy cập vị trí của thiết bị.
- android.permission.WAKE_LOCK: cho phép ứng dụng giữ thiết bị ở trạng thái hoạt động (awake) trong khi màn hình đã tắt hoặc thiết bị đã vào chế độ ngủ.
- android.permission.READ _CONTACTS [dangerous]: cho phép đọc đọc các thông tin như tên, số điện thoại, địa chỉ email, địa chỉ và thông tin khác trên thiết bị.
- android.permission.WRITE_CONTACTS [dangerous]: cho phép ứng dụng ghi (thêm, sửa đổi, xóa) thông tin liên hệ trong danh bạ (contacts) trên thiết bị.
- android.permission.GET_ACCOUNTS [dangerous]: cho phép ứng dụng truy cập danh sách các tài khoản đã được đăng nhập trên thiết bị.
- android.permission.MANAGE _ACCOUNTS: cho phép ứng dụng quản lý tài khoản người dùng trên thiết bị.
- android.permission.AUTHENTICATE_ACCOUNTS cho phép ứng dụng xát thực tài khoản người dùng trên thiết bị.
- android.permission.READ_SYNC_SETTINGS: cho phép ứng dụng đọc cài đặt đồng bộ hóa (sync settings) trên thiết bị.
- android.permission.WRITE_SYNC_SETTINGS: cho phép ứng dụng thay đổi cài đặt đồng bộ hóa (sync settings) trên thiết bị.
- android.permission.ACCESS_FINE_LOCATION [dangerous]: cho phép ứng dụng truy cập vào vị trí chính xác của thiết bị.
- android.permission.ACCESS_MEDIA_LOCATION: cho phép ứng dụng truy cập địa chỉ vị trí của các phương tiện truyền thông (media) trên thiết bị.
- android.permission.ACCESS_NETWORK_STATE: cho phép ứng dụng truy cập trạng thái của kết nối mạng trên thiết bị.
- android.permission.ACCESS_WIFISTATE: cho phép ứng dụng truy cập trạng thái của kết nối Wi-Fi trên thiết bị.
- android.permission.BROADCAST_STICKY: cho phép ứng dụng gửi và nhận các thông báo gắn kết (sticky broadcasts).
- android.permission.DOWNLOAD_WITHOUT_NOTIFICATION: cho phép ứng dụng tải xuống tập tin từ Internet mà không hiển thị thông báo cho người dùng.

- Android.permission.NFC: cho phép ứng dụng truy cập vào tính năng NFC (Near Field Communication) trên thiết bị.
- android.permission.CAMERA [dangerous]: cho phép ứng dụng truy cập vào camera trên thiết bị.
- android.permission.RECORD_AUDIO [dangerous]: cho phép ứng dụng truy cập vào ghi âm trên thiết bị.
- android.permission.WRITE_EXTERNAL_STORAGE [dangerous]: cho phép ứng dụng thêm xóa sửa dữ liệu bộ nhớ trên thiết bị.
- android.permission.READ_PHONE_NUMBERS [dangerous]: cho phép ứng dụng truy cập và đọc số điện thoại trên thiết bị.
- android.permission.READ_PHONE_STATE [dangerous]: cho phép ứng dụng đọc thông tin trạng thái số điện thoại trên thiết bị.
- android.permission.READ_CALENDAR [dangerous]: cho phép ứng dụng đọc thông tin lịch có trên thiết bị.
- android.permission.WRITE_CALENDAR [dangerous]: cho phép ứng dụng sửa thông tin lịch có trên thiết bị.
- android.permission.MODIFYAUDIO_SETTINGS: cho phép ứng dụng thay đổi cài đặt âm thanh trên thiết bị.
- android.permission.READ_PROFILE: cho phép ứng dụng thông tin từ hồ sơ người dùng, bao gồm tên, hình ảnh, địa chỉ email, số điện thoại, giới tính, ngày sinh,..
- android.permission.CHANGE_NETWORK_STATE: cho phép ứng dụng thay đổi trạng thái mạng trên thiết bị.
- android.permission.CHANGE_WIFI_STATE: cho phép ứng dụng thay đổi trạng thái wifi trên thiết bị.
- android.permission.SYSTEM_ALERT_WINDOW: cho phép ứng dụng hiển thị các cửa sổ pop-up hoặc thông báo trên các ứng dụng khác hoặc trên màn hình chính của thiết bị.
- android.permission.RECEIVE_BOOT_COMPLETED: cho phép ứng dụng nhận thông báo khi thiết bị khởi động lại.

- android.permission.GET_TASKS: cho phép ứng dụng truy cập và thông tin về các hoạt động (tasks) đang chạy trên thiết bị.
- android.permission.READ_EXTERNAL_STORAGE[dangerous]:]: cho phép ứng dụng đọc dữ liệu từ bộ nhớ ngoài của thiết bị, chẳng hạn như thẻ SD hoặc bộ nhớ trong.
- android.permission.USE_FULL_SCREEN_INTENT: cho phép ứng dụng sử dụng các thông báo full screen (toàn màn hình) khi hiển thị thông báo.
- android.permission.REORDER TASKS: cho phép ứng dụng sắp xếp lại các nhiệm vụ (tasks) trên màn hình chính của người dùng.
- Android.permission.INTERNET: cho phép ứng dụng truy cập vào internet trên thiết bị.
- android.permission.BATTERY_STATS: cho phép ứng dụng truy cập vào trạng thái pin trên thiết bị.
- android.permission.FOREGROUND _SERVICE: cho phép ứng dụng chạy dịch vụ trong trạng thái nổi bật (foreground service).
- android.permission.USE_BIOMETRIC: cho phép ứng dụng sử dụng các tính năng sinh trắc học của thiết bị.
- android.permission.USE_FINGERPRINT: cho phép ứng dụng sử dụng vân tay trên thiết bị.

Các quyền hạn tuỳ chỉnh được cấp:





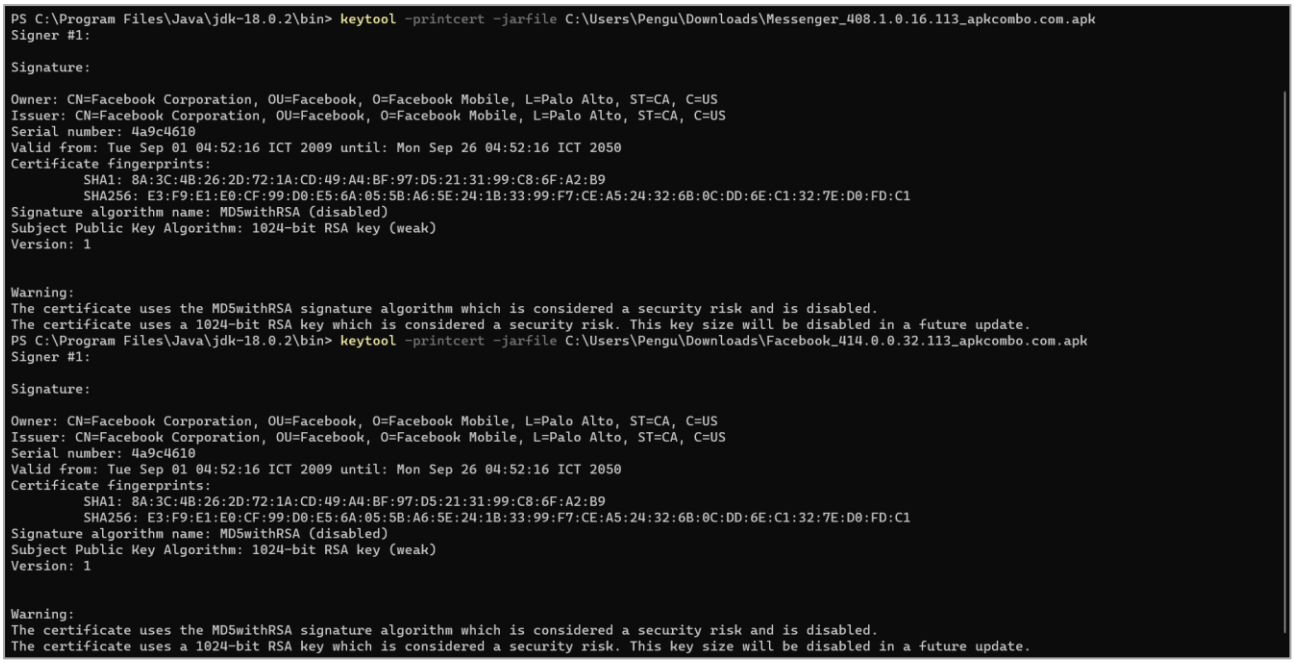
➔ Một số quyền có thể thấy ở cả 2 ứng dụng: *.CAMERA, *.ACCESS_FINE_LOCATION tương ứng sẽ là truy cập camera và vị trí khi sử dụng.

Trong nhóm hình 1 có quyền *.READ_EXTERNAL_STORAGE nằm ở gần cuối là quyền yêu cầu cho phép đọc bộ nhớ, từ phiên bản **API level 33** trở đi, quyền này không còn tác dụng nữa và sẽ sử dụng thay thế với các quyền như là READ_MEDIA_AUDIO, READ_MEDIA_IMAGES, READ_MEDIA_VIDEO.

Một số quyền tùy chỉnh thấy ở cả hai ứng dụng: .Provider truy cập vào dữ liệu được cung cấp bởi ứng dụng Facebook, .Receiver quyền nhận các thông báo từ Facebook, .Service thực hiện các tác vụ chạy nền của ứng dụng Facebook, com.google.android.gms.permission.AD_ID quyền đọc và sử dụng Advertising ID của thiết bị để liên kết với các dịch vụ quảng cáo hoặc thu thập dữ liệu liên quan đến quảng cáo.

1.2. Xem các thông tin về chữ ký trên các file APK của ứng dụng

Sử dụng công cụ keytool có trong thư mục C:\Program Files\Java\jdk-18.0.2\bin để xem tất cả chữ kí có trong file apk gồm có Messenger và Facebook:



Hình 4: Xem thông tin chữ kí của các file apk

Apk được download trên: apkcombo

Thông tin chữ kí nhận được cho app messenger:

Signer #1:

Signature:

Owner: CN=Facebook Corporation, OU=Facebook, O=Facebook Mobile, L=Palo Alto, ST=CA, C=US

Issuer: CN=Facebook Corporation, OU=Facebook, O=Facebook Mobile, L=Palo Alto, ST=CA, C=US

Serial number: 4a9c4610

Valid from: Tue Sep 01 04:52:16 ICT 2009 until: Mon Sep 26 04:52:16 ICT 2050

Certificate fingerprints:

SHA1: 8A:3C:4B:26:2D:72:1A:CD:49:A4:BF:97:D5:21:31:99:C8:6F:A2:B9

SHA256: E3:F9:E1:E0:CF:99:D0:E5:6A:05:5B:A6:5E:24:1B:33:99:F7:CE:A5:24:32:6B:0C:DD:6E:C1:32:7E:D0:FD:C1

Signature algorithm name: MD5withRSA (disabled)

Subject Public Key Algorithm: 1024-bit RSA key (weak)

Version: 1

Warning:

The certificate uses the MD5withRSA signature algorithm which is considered a security risk and is disabled.

The certificate uses a 1024-bit RSA key which is considered a security risk. This key size will be disabled in a future update.

Thông tin chữ kí nhận được cho app facebook:

Signer #1:

Signature:

Owner: CN=Facebook Corporation, OU=Facebook, O=Facebook Mobile, L=Palo Alto, ST=CA, C=US

Issuer: CN=Facebook Corporation, OU=Facebook, O=Facebook Mobile, L=Palo Alto, ST=CA, C=US

Serial number: 4a9c4610

Valid from: Tue Sep 01 04:52:16 ICT 2009 until: Mon Sep 26 04:52:16 ICT 2050

Certificate fingerprints:

SHA1: 8A:3C:4B:26:2D:72:1A:CD:49:A4:BF:97:D5:21:31:99:C8:6F:A2:B9

SHA256: E3:F9:E1:E0:CF:99:D0:E5:6A:05:5B:A6:5E:24:1B:33:99:F7:CE:A5:24:32:6B:0C:DD:6E:C1:32:7E:D0:FD:C1

Signature algorithm name: MD5withRSA (disabled)

Subject Public Key Algorithm: 1024-bit RSA key (weak)

Version: 1

Warning:

The certificate uses the MD5withRSA signature algorithm which is considered a security risk and is disabled.

The certificate uses a 1024-bit RSA key which is considered a security risk. This key size will be disabled in a future update.

➔ Mỗi doanh nghiệp chỉ có 1 chữ kí riêng nên 2 ứng dụng này cũng sẽ có chữ kí giống nhau, nội dung tổng quan về chữ kí như sau:

- Owner: Chủ sở hữu là Facebook Corporation, đơn vị tổ chức (OU): Facebook, tổ chức (O): Facebook Mobile, địa điểm (L): Palo Alto, tiểu bang (ST): CA và quốc gia (C): US.
- Issuer: Cơ quan cấp chứng chỉ là Facebook Corporation
- Serial number: Số thứ tự duy nhất được gán cho chứng chỉ 4a9c4610.
- Valid from: Là thời điểm chứng chỉ có hiệu lực, từ ngày 01 tháng 09 năm 2009 và thời điểm chứng chỉ hết hiệu lực, đến ngày 26 tháng 09 năm 2050
- Signature algorithm name: Thuật toán mã hóa MD5withRSA
- Certificate fingerprints: Sử dụng Hash SHA-1 và SHA-256
- Subject Public Key Algorithm: Thuật toán khóa công khai là 1024-bit RSA.

2. Viết 2 ứng dụng Android cơ bản có các tính năng kiểm soát truy cập lẫn nhau

App LoginApp sử dụng lại từ bài tập 1, tại trang chủ sau khi đăng nhập xong, các chức năng bổ sung gồm có:

- Export các username hiện có trong SQLite database, sau đó lập tức chuyển qua ứng dụng FileControl
- Bind Service để có thể kết nối Activity với service đang chạy dưới nền để từ đó thực hiện các thao tác lấy dữ liệu từ service
- unBindService ngược lại với bindService
- Get random number lấy kết quả từ service sau khi thực hiện bindService thành công

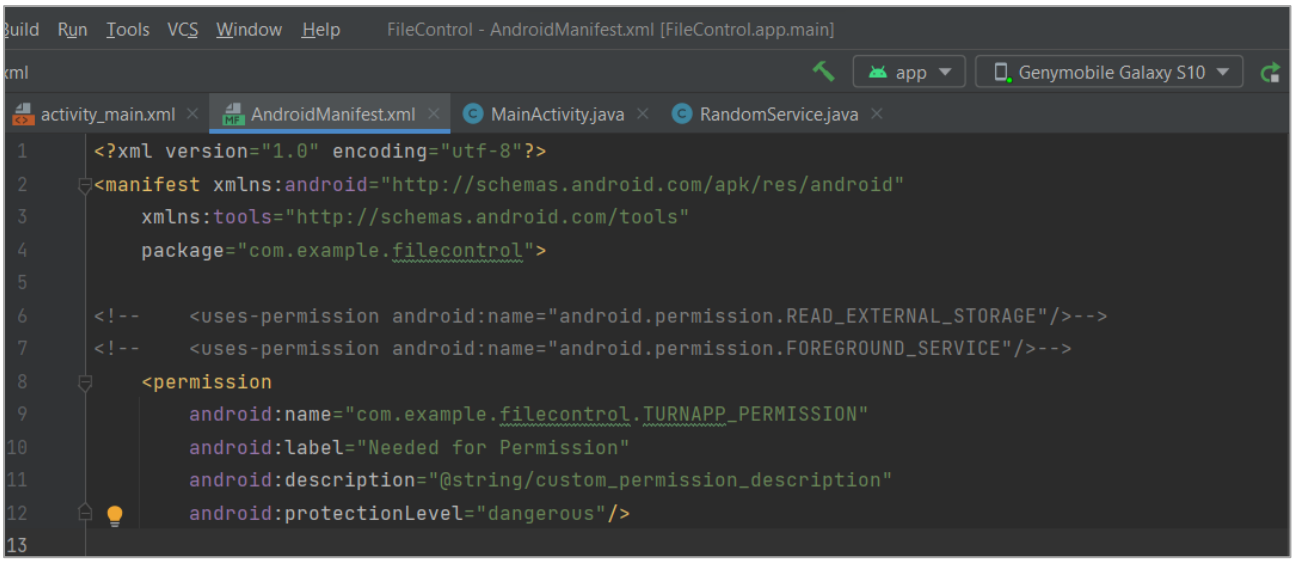
App FileControl sẽ có các chức năng như sau:

- Hiển thị hình ảnh có trong thiết bị (lấy uri sau đó hiển thị hình ảnh tương ứng uri đó)
- Start Service: khởi động 1 service thực hiện random ngẫu nhiên 1 trong khoảng cho trước.
- Stop Service: dừng việc random.

2.1. Cấp quyền cho Activity

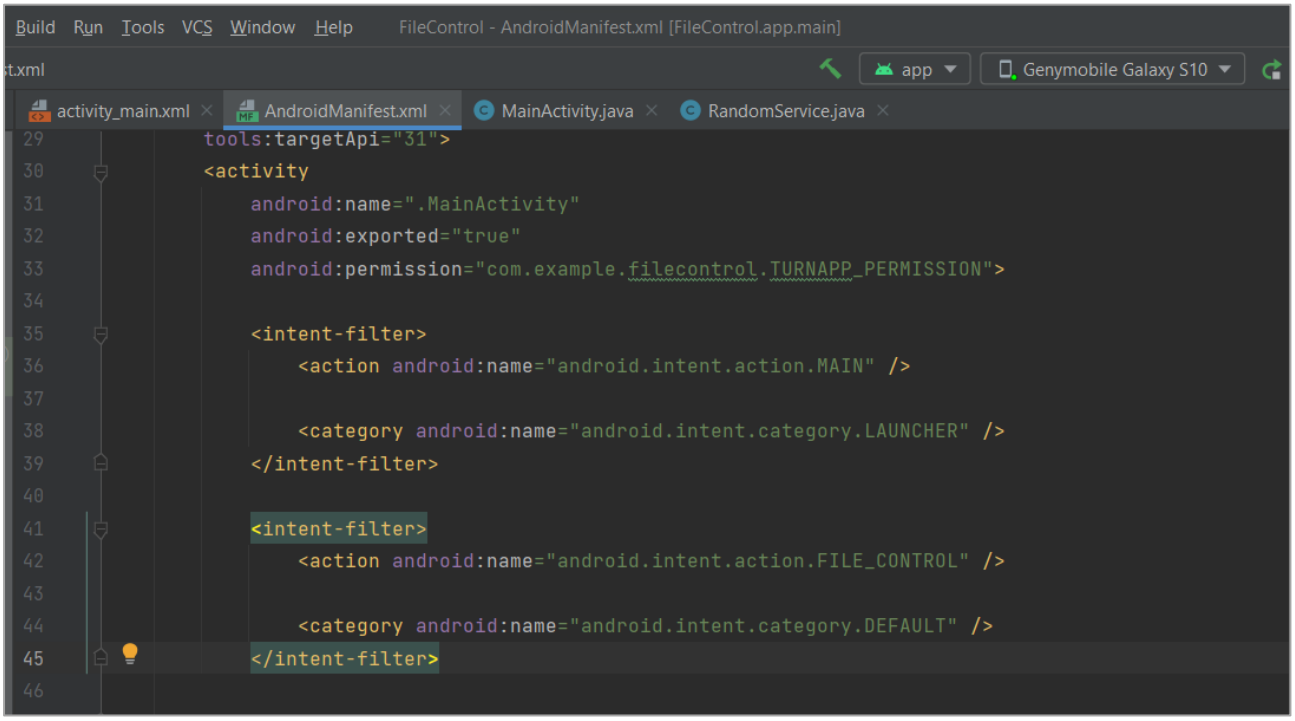
Cài đặt phần activity để có thể chuyển hướng từ trang chủ (MainActivity) của ứng dụng LoginApp qua MainActivity của FileControl:

- Trong tệp **ManiFest** của FileControl, tạo 1 permission:



Hình 5: Custom permission

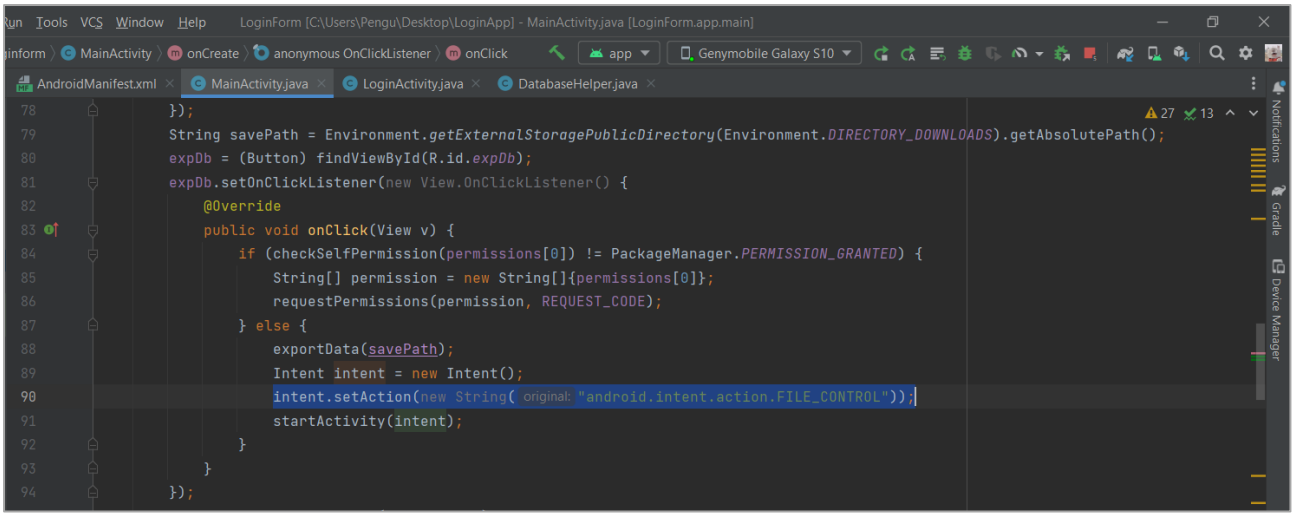
- Vẫn tại tệp đó, đặt quyền vừa custom vào trong thẻ activity đồng thời thêm 1 intent-filter:



Hình 6: Thêm intent filter

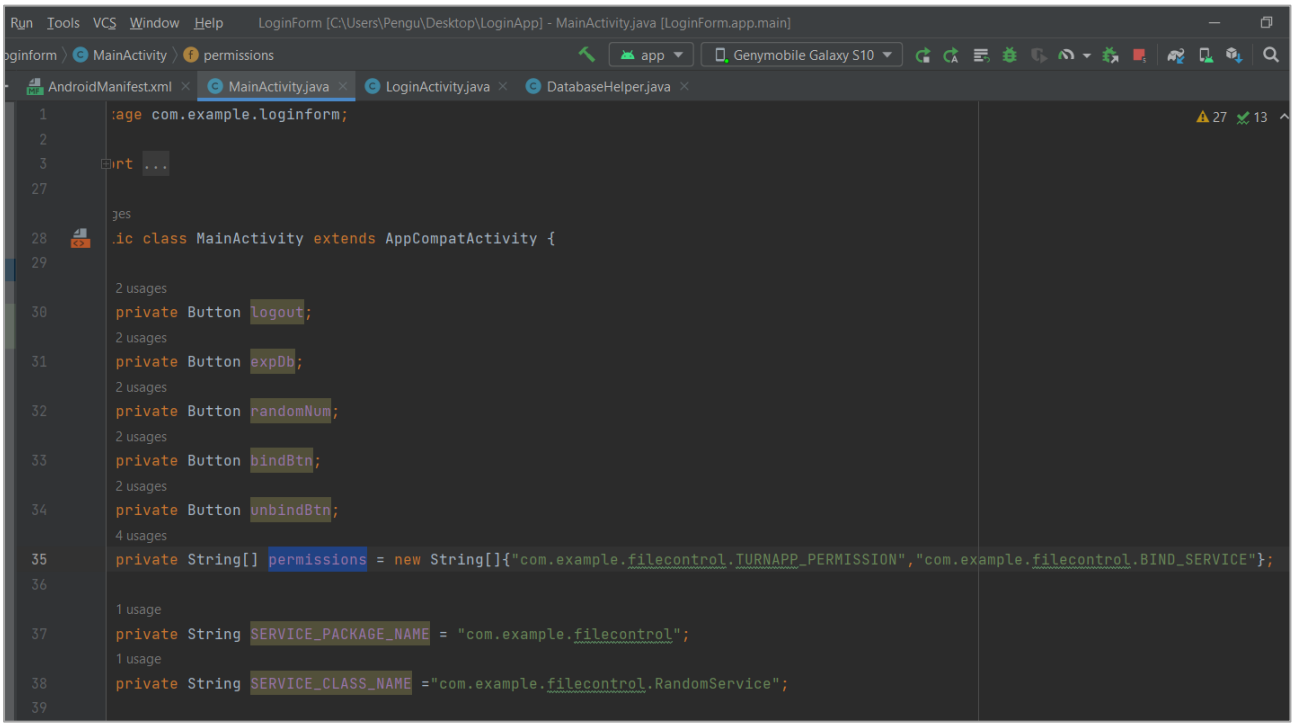
➔ Phía LoginApp khi muốn chuyển hướng sẽ gọi đến tên action này và cần có quyền được FileControl cấp.

- Trong MainActivity của LoginApp, tạo xử lí thao tác bấm nút "Get All Credentials" (Xuất tất cả username trong SQLite đồng thời chuyển hướng):



Hình 7: Kiểm tra quyền và gọi tới action với tên đã tạo ở trên

- Để dễ quản lí các quyền, thực hiện khai báo 1 mảng các quyền và quyền đang được xét tới trong phần Activity sẽ là chuỗi đầu tiên:



Hình 8: Khai báo mảng permission

2.2. Cấp quyền sử dụng service

Service sẽ được tạo trong FileControl và sử dụng Message để truyền thông tin và thực hiện các tác vụ giữa các thành phần như Service, Activity và Thread.

Tương ứng với RequestHandle trong Randomservice (FileControl), chúng ta có receiverHandler trong LoginApp:

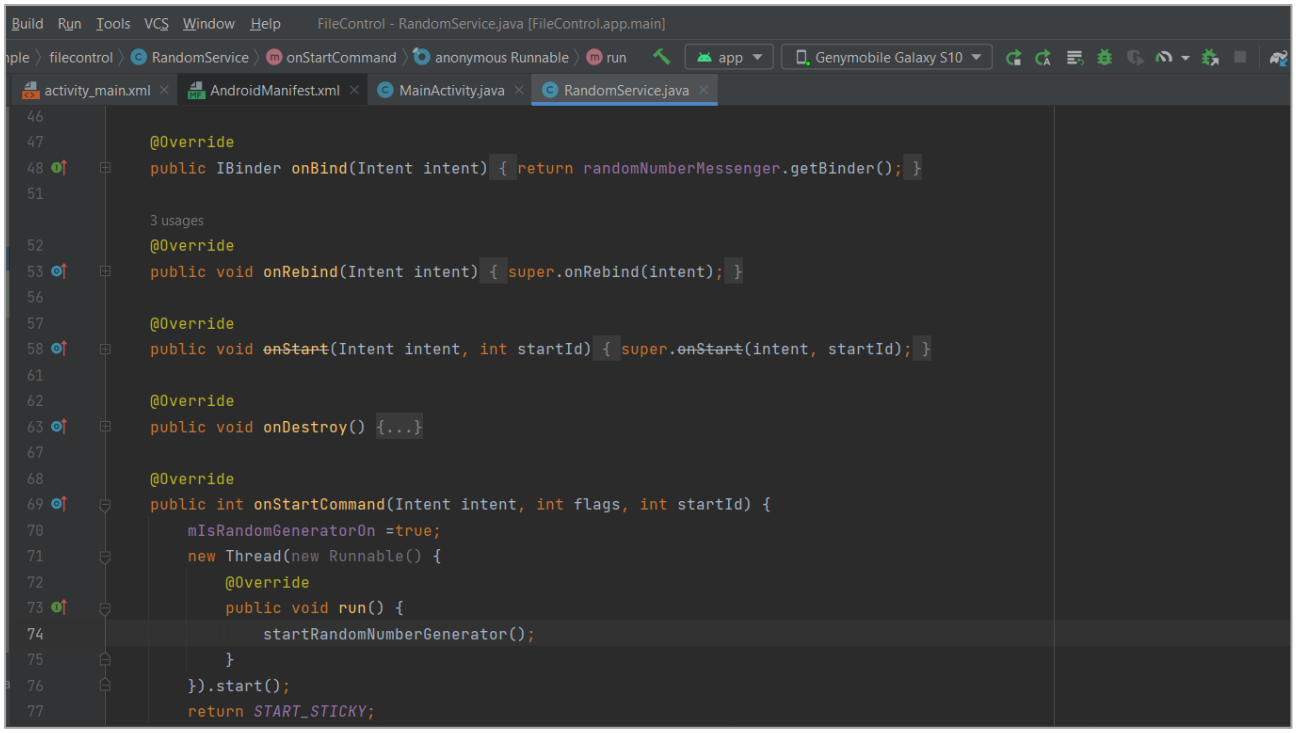
```
private class RandomNumberRequestHandler extends Handler {
    @Override
    public void handleMessage(Message msg) {

        switch (msg.what){
            case GET_RANDOM_NUMBER_FLAG:
                Message  messageSendRandomNumber=Message.obtain( h: null, GET_RANDOM_NUMBER_FLAG);
                messageSendRandomNumber.arg1=getRandomNumber();
                try{
                    msg.replyTo.send(messageSendRandomNumber);
                }catch (RemoteException e){
                    Log.i(TAG, msg: ""+e.getMessage());
                }
        }
        super.handleMessage(msg);
    }
}
```

Hình 9: RequestHadler trong FileControl

```
1 usage
class RecieveRandomNumberHandler extends Handler{
    @Override
    public void handleMessage(Message msg) {
        randomNumberValue =0;
        switch (msg.what) {
            case GET_RANDOM_FLAG:
                randomNumberValue =msg.arg1;
                textViewRandomNumber.setText("Random Number: "+ randomNumberValue);
                break;
            default:
                break;
        }
        super.handleMessage(msg);
    }
}
```

Hình 10: ReceiveHandler trong LoginApp

Các phương thức bind, ubBind, reBind để tuỳ chỉnh việc kết nối tới service:

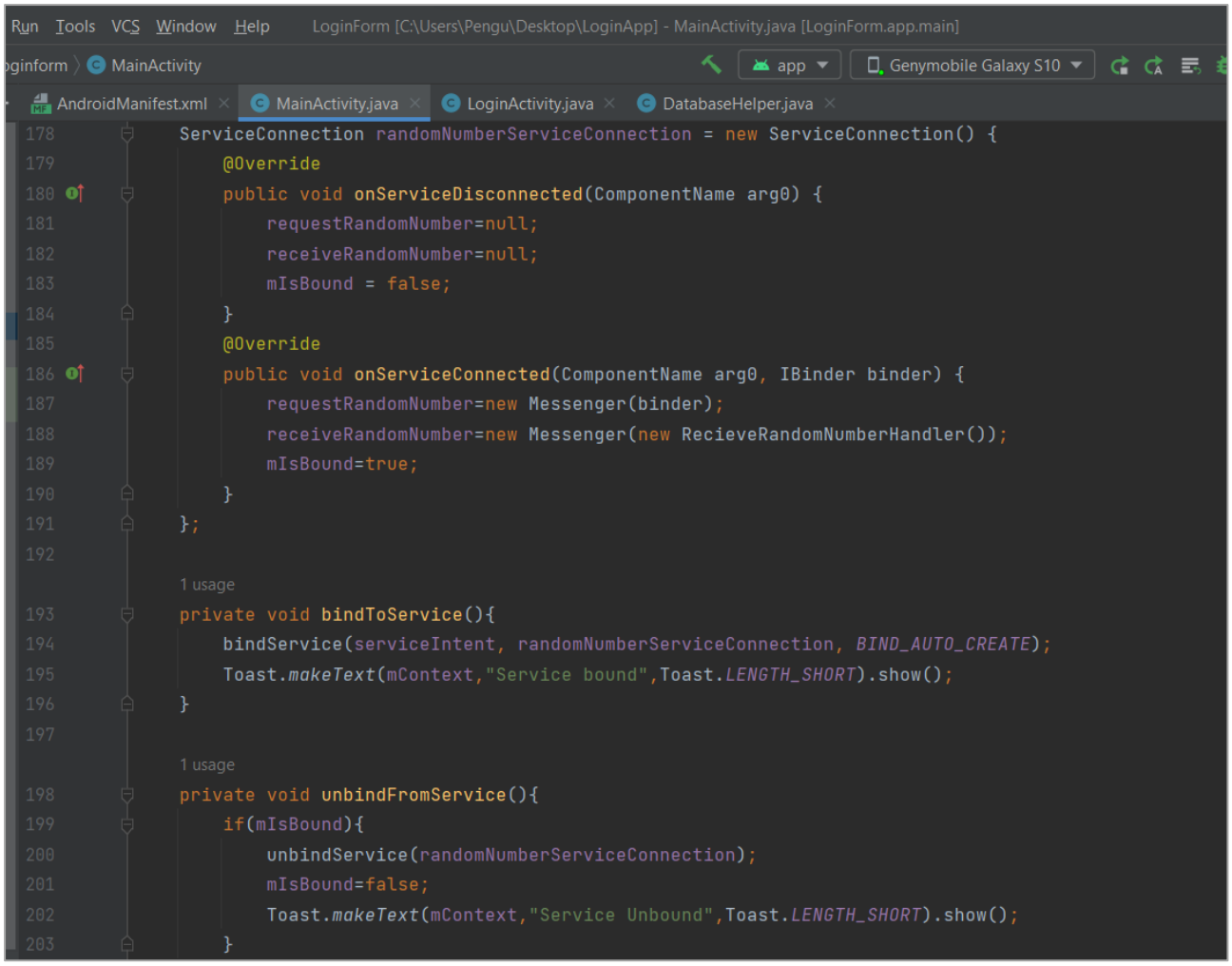


Hàm onstartCommand sẽ tạo ta 1 Thread thực hiện random số:

```
1 usage
private void startRandomNumberGenerator(){
    while (mIsRandomGeneratorOn){
        try{
            Thread.sleep( millis: 1000);
            if(mIsRandomGeneratorOn){
                mRandomNumber =new Random().nextInt(MAX)+MIN;
                Log.i(TAG, msg: "Random Number: "+mRandomNumber);
            }
        }catch (InterruptedException e){
            Log.i(TAG, msg: "Thread Interrupted");
        }
    }
}

1 usage
private void stopRandomNumberGenerator(){
    mIsRandomGeneratorOn =false;
    Toast.makeText(getApplicationContext(),"Service Stopped", Toast.LENGTH_SHORT).show();
}
```

Hình 11: Hàm random số và hàm ngưng việc này

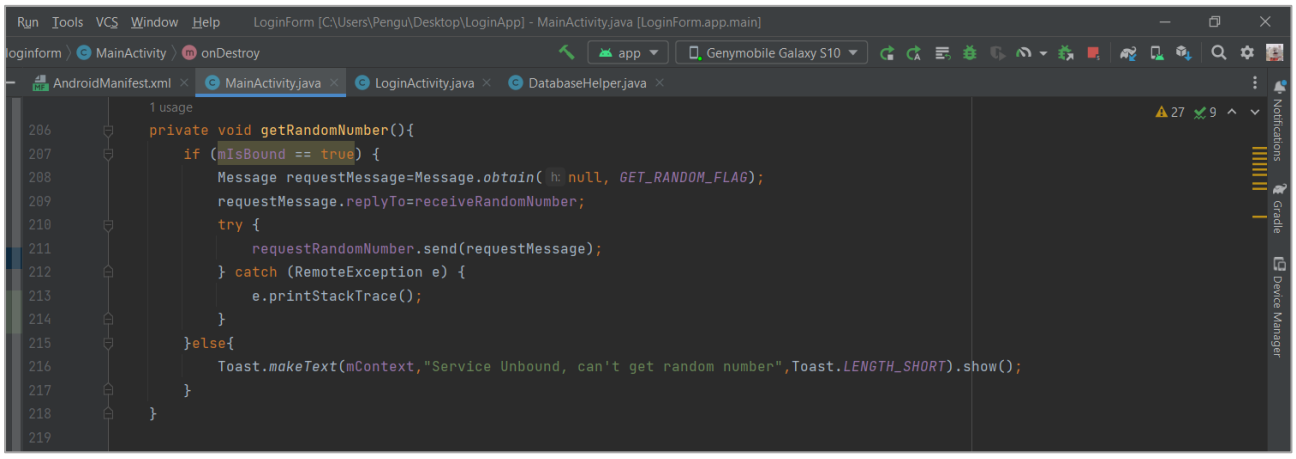
Bên LoginApp, tạo MainActivity, tạo 1 kết nối ServiceConnection và tạo các phương thức bind và unbind tới service:



```
ServiceConnection randomNumberServiceConnection = new ServiceConnection() {
    @Override
    public void onServiceDisconnected(ComponentName arg0) {
        requestRandomNumber=null;
        receiveRandomNumber=null;
        mIsBound = false;
    }
    @Override
    public void onServiceConnected(ComponentName arg0, IBinder binder) {
        requestRandomNumber=new Messenger(binder);
        receiveRandomNumber=new Messenger(new RecieveRandomNumberHandler());
        mIsBound=true;
    }
};

1 usage
private void bindToService(){
    bindService(serviceIntent, randomNumberServiceConnection, BIND_AUTO_CREATE);
    Toast.makeText(mContext,"Service bound",Toast.LENGTH_SHORT).show();
}

1 usage
private void unbindFromService(){
    if(mIsBound){
        unbindService(randomNumberServiceConnection);
        mIsBound=false;
        Toast.makeText(mContext,"Service Unbound",Toast.LENGTH_SHORT).show();
    }
```

Hình 12: Tạo kết nối và bind/unbind

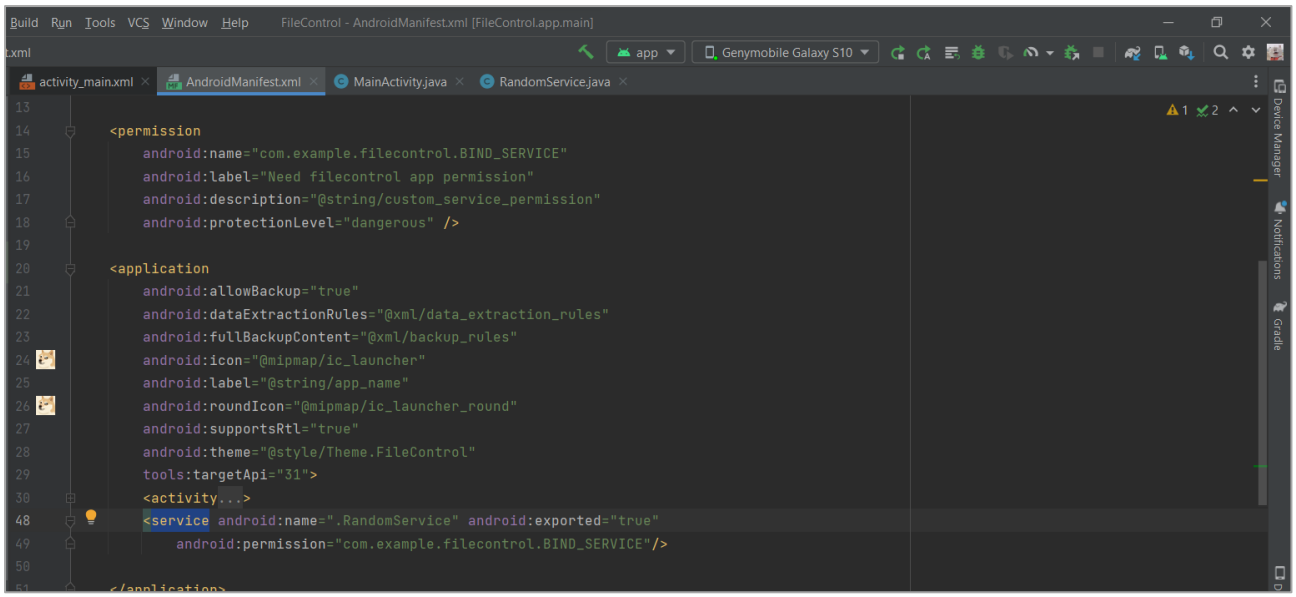
Cuối cùng lấy số đã được random dưới service:



```
1 usage
private void getRandomNumber(){
    if (mIsBound == true) {
        Message requestMessage=Message.obtain( h: null, GET_RANDOM_FLAG);
        requestMessage.replyTo=receiveRandomNumber;
        try {
            requestRandomNumber.send(requestMessage);
        } catch (RemoteException e) {
            e.printStackTrace();
        }
    }else{
        Toast.makeText(mContext,"Service Unbound, can't get random number",Toast.LENGTH_SHORT).show();
    }
}
```

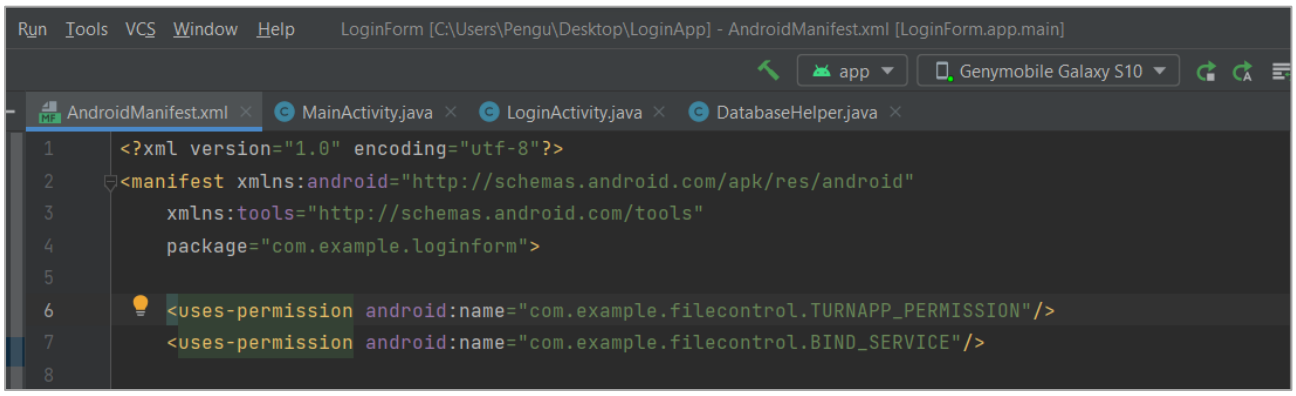
Hình 13: Hàm lấy số được random

Thực hiện tương tự activity, tạo mới 1 service và đặt custom permission tại đó, đặt giá trị `exported:true`, không khai báo intent:



Hình 14: Đặt quyền tuỳ chỉnh

Trong LoginApp, gọi tới các quyền đã tạo bên FileControl:



Hình 15: Khai báo uses-permission

DEMO:

https://youtu.be/Pth7-GTcwIs

Note: Chương trình được thử nghiệm trên Genymotion bản Android 11, trong đó có lỗi nhỏ là nút Bind Service sau khi phân quyền thành công sẽ bị văng ra khỏi ứng dụng (quay về trang login) quyền vẫn được cấp và chức năng Bind Service vẫn hoạt động đúng chức năng.

HẾT