Android Mobile Pentest 101

Lecture 10.6 – Creating Exploit: Broadcast Receivers

Mục tiêu: Hiểu Broadcast Receivers là gì

Introduction

- Bài này giúp bạn hiểu Broadcast Receivers trong android

What’s Broadcast Receivers

- Android BroadcastReceiver là một trong những thành phần chính của Android, dùng để lắng nghe các system-wide broadcast events hoặc intents.
- Broadcast Receivers đơn giản là lắng nghe (và có thể trả lời) các lời gọi từ hệ thống hoặc app khác
- Khác với Activity, android BroadcastReceiver không có interface để tương tác.

Let’s code

- Có nhiều cách để setup Broadcast Receivers, bạn nên google thêm nếu hứng thú, ở đây mình chỉ show cách mình hay làm (demo thôi mà ☺)

Let’s code

- Bây giờ chúng ta sẽ code 1 chương trình lắng nghe lời gọi tới AIRPLANE_MODE
- Định nghĩa class Broadcast, extends từ BroadcastReceiver

```
class Broadcast extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
        Log.d(Broadcast.class.getSimpleName(), "Air Plane mode");
    }
}
```

- Sau đó tạo đối tượng của lớp Broadcast trong onCreate(), nó sẽ lắng nghe các intent AIRPLANE_MODE, nghĩa là nếu user bật tắt cái AIRPLANE_MODE, thì chương trình của ta sẽ nghe được và log nó trong logcat

```
Broadcast = new Broadcast();
IntentFilter filter = new IntentFilter("android.intent.action.AIRPLANE_MODE");
registerReceiver(broadcast, filter);
```

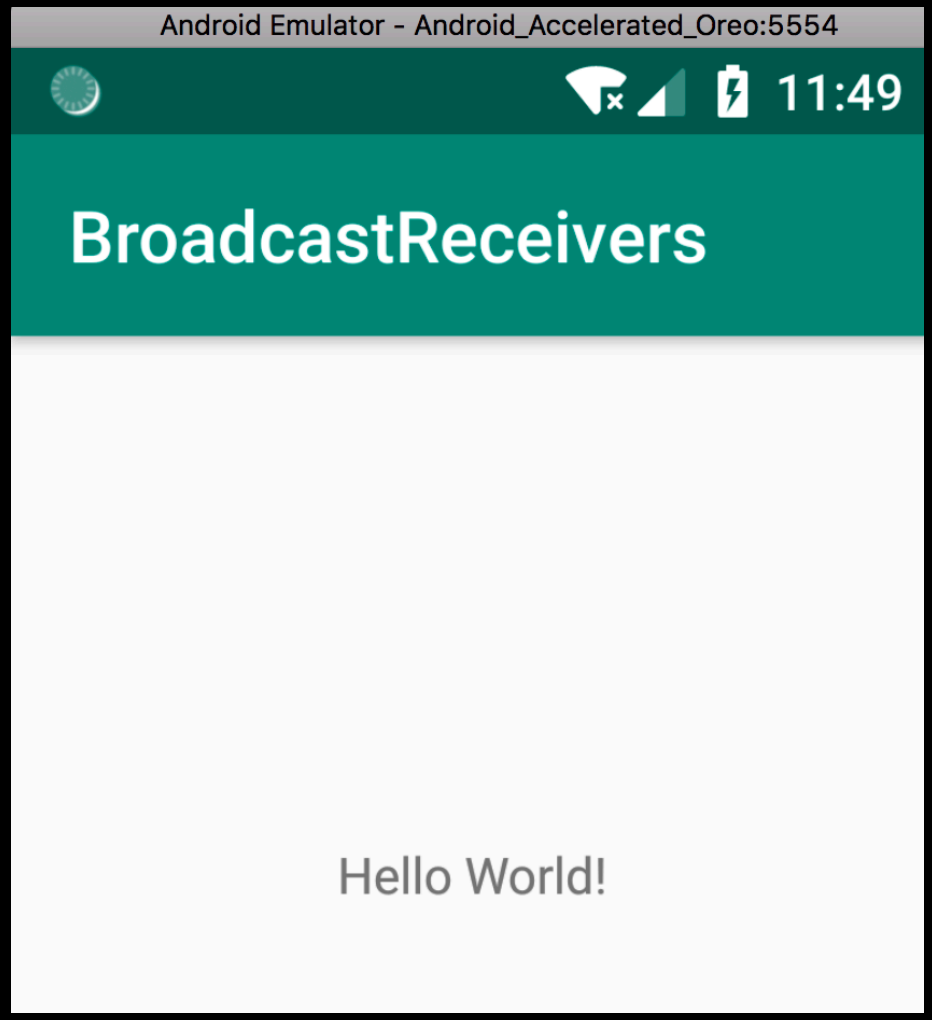
Let’s code

- Code nhìn như này:

```
public class MainActivity extends AppCompatActivity {

    private Broadcast broadcast;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        broadcast = new Broadcast();
        IntentFilter filter = new IntentFilter( action: "android.intent.action.AIRPLANE_MODE");
        registerReceiver(broadcast, filter);
    }

    @Override
    protected void onStop() {
        super.onStop();
        unregisterReceiver(broadcast);
    }
}

class Broadcast extends BroadcastReceiver {
    @Override
    public void onReceive(Context context, Intent intent) {
        Log.d(Broadcast.class.getSimpleName(), msg: "Air Plane mode");
    }
}
```

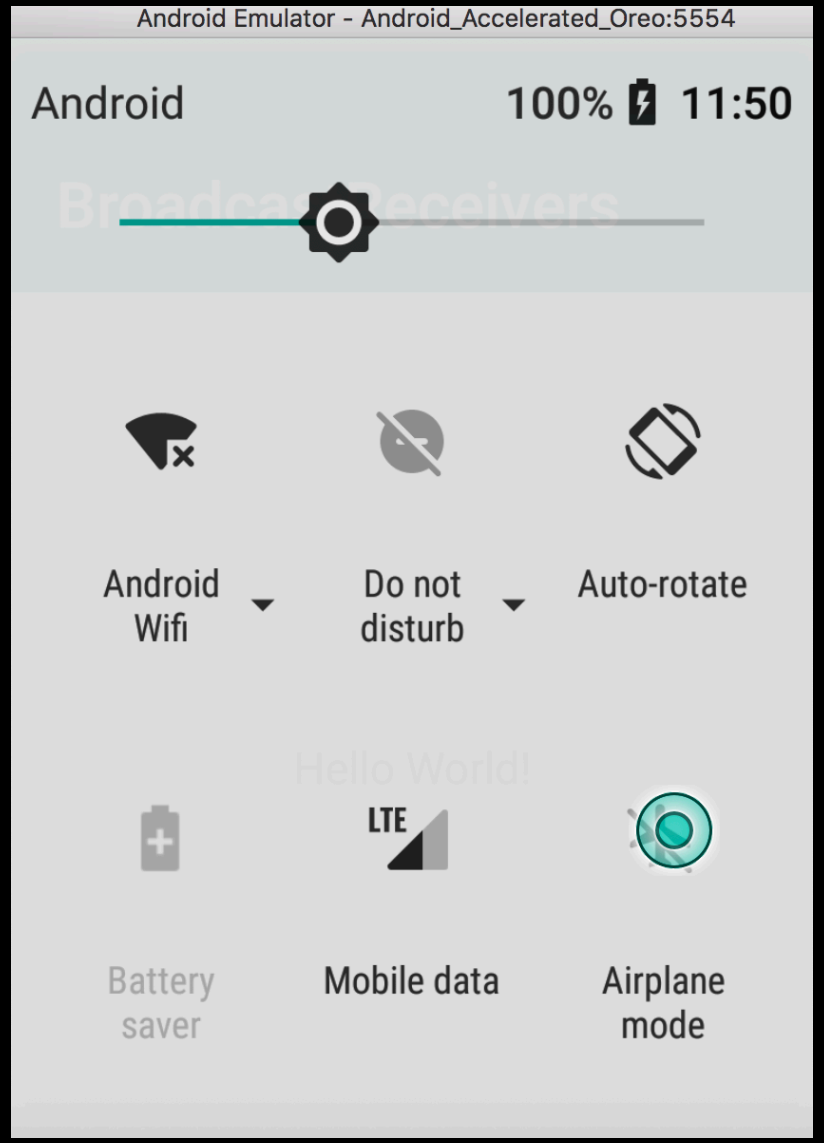
Let’s code

- Chạy lên nào



Let’s code

- Bật/Tắt AirPlane Mode thử coi



Let’s code

- Trong logcat:

```
3/com.example.broadcastreceivers D/OpenGLRenderer: HWUI GL Pipeline
3/com.example.broadcastreceivers I/zygote: android::hardware::configs
3/com.example.broadcastreceivers I/OpenGLRenderer: Initialized EGL, v
3/com.example.broadcastreceivers D/OpenGLRenderer: Swap behavior 1
3/com.example.broadcastreceivers W/OpenGLRenderer: Failed to choose c
3/com.example.broadcastreceivers D/OpenGLRenderer: Swap behavior 0
3/com.example.broadcastreceivers D/EGL_emulation: eglCreateContext: 0
3/com.example.broadcastreceivers D/EGL_emulation: eglMakeCurrent: 0xa
3/com.example.broadcastreceivers D/EGL_emulation: eglMakeCurrent: 0xa
2/com.example.broadcastreceivers D/Broadcast: Air Plane mode
2/com.example.broadcastreceivers D/Broadcast: Air Plane mode
2/com.example.broadcastreceivers D/Broadcast: Air Plane mode
2/com.example.broadcastreceivers D/Broadcast: Air Plane mode
```

- Full code ở: https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_BroadcastReceivers