Android Mobile Pentest 101

Lecture 10.6 – Creating Exploit: Broadcast Receivers

Goal: Understand broadcast receivers component

Introduction

- This lecture will help you understand basic broadcast receivers

What’s Broadcast Receivers

- Android BroadcastReceiver is a dormant component of android that listens to system-wide broadcast events or intents.
- Broadcast Receivers simply respond to broadcast messages from other applications or from the system itself
- These messages are sometime called events or intents
- Unlike activities, android BroadcastReceiver doesn’t contain any user interface.

Let’s code

- There are many ways to setup Broadcast Receivers, you should google for it, I will introduce the method that I always do (for demo purpose, since we are hacker, not developer ☺)

Let’s code

- We’re going to define the broadcast receivers which listen for AirPlane Mode On/off
- We defined the class Broadcast, extends from BroadcastReceiver

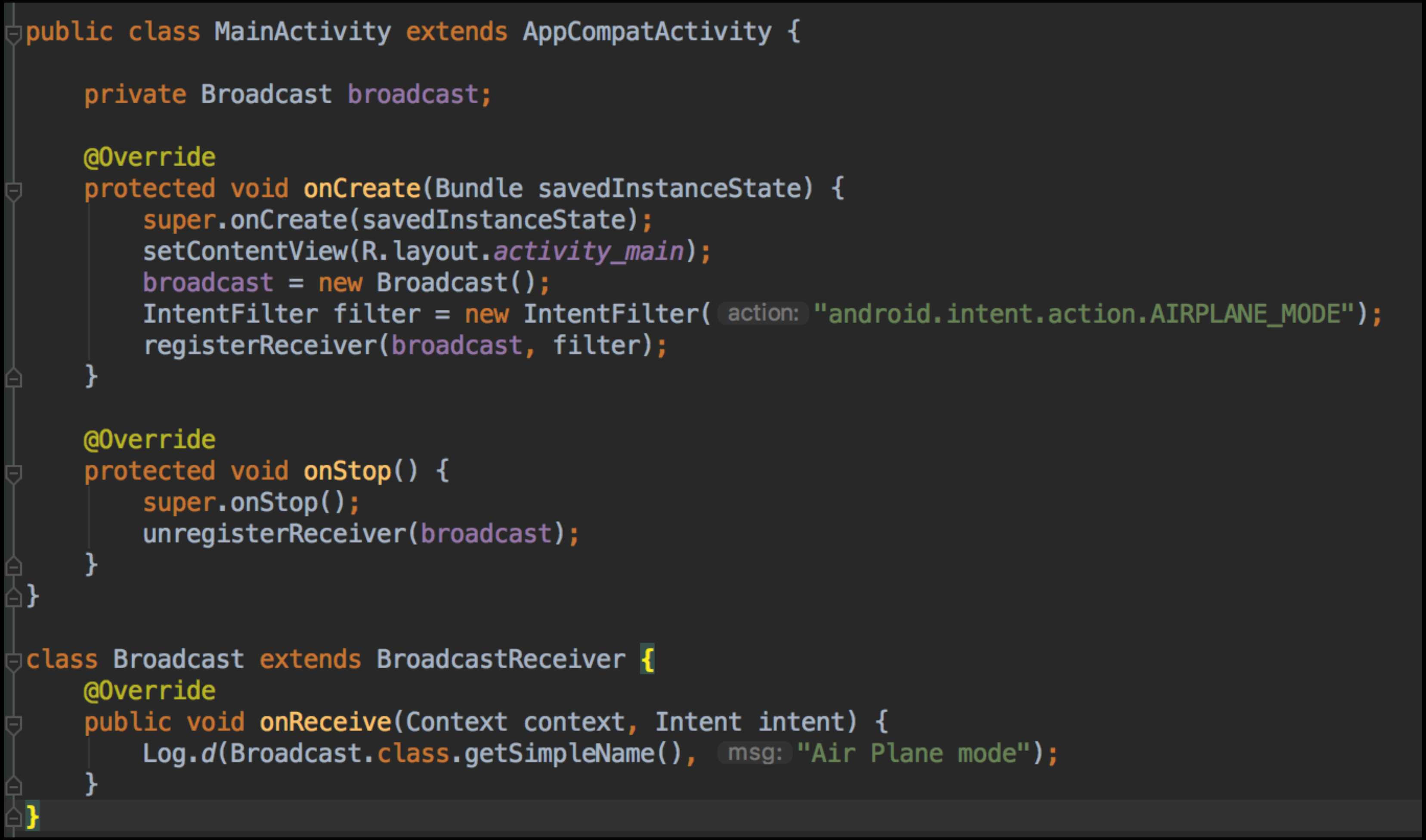
```
class Broadcast extends BroadcastReceiver {
   @Override
   public void onReceive(Context context, Intent intent) {
      Log.d(Broadcast.class.getSimpleName(), "Air Plane mode");
   }
}
```

- Then we create its object in onCreate(), It will listen for intent AIRPLANE_MODE, means when user turn on/ off the airplane mode on phone, the receiver will receive the intent and log it in logcat

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

Let’s code

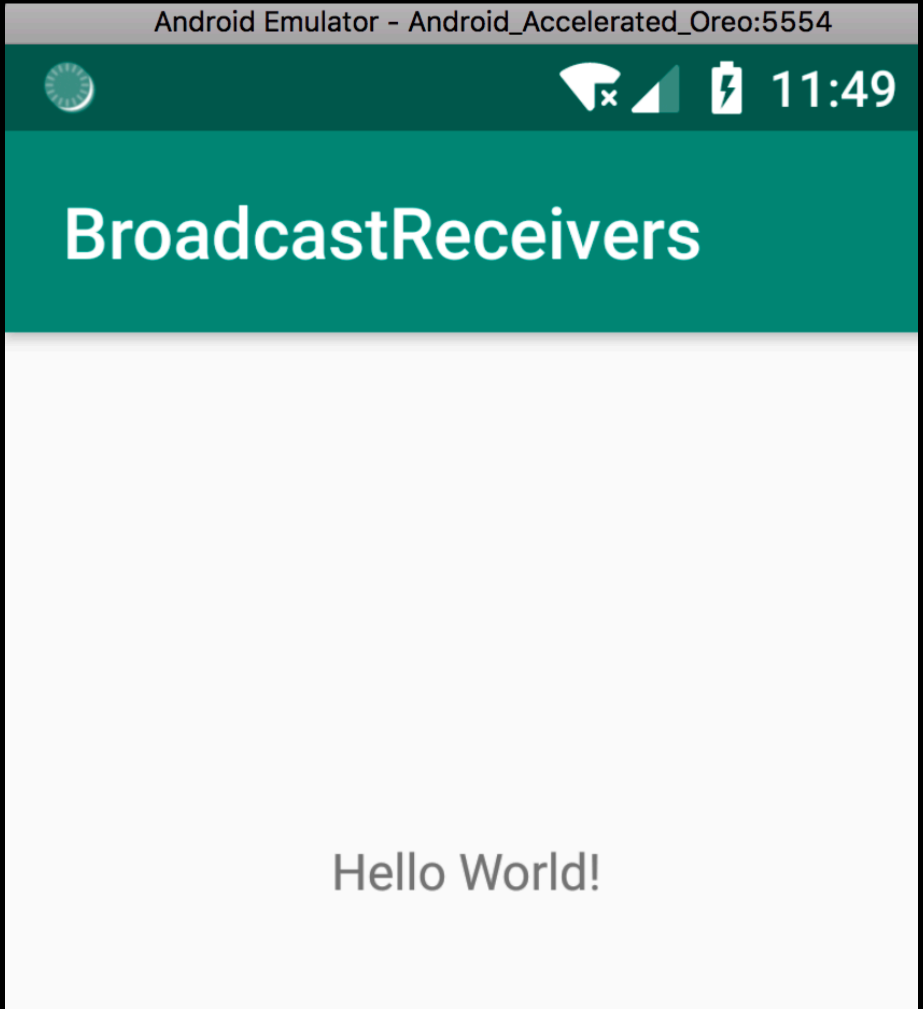
- Code may look like:



```
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");
    }
}
```

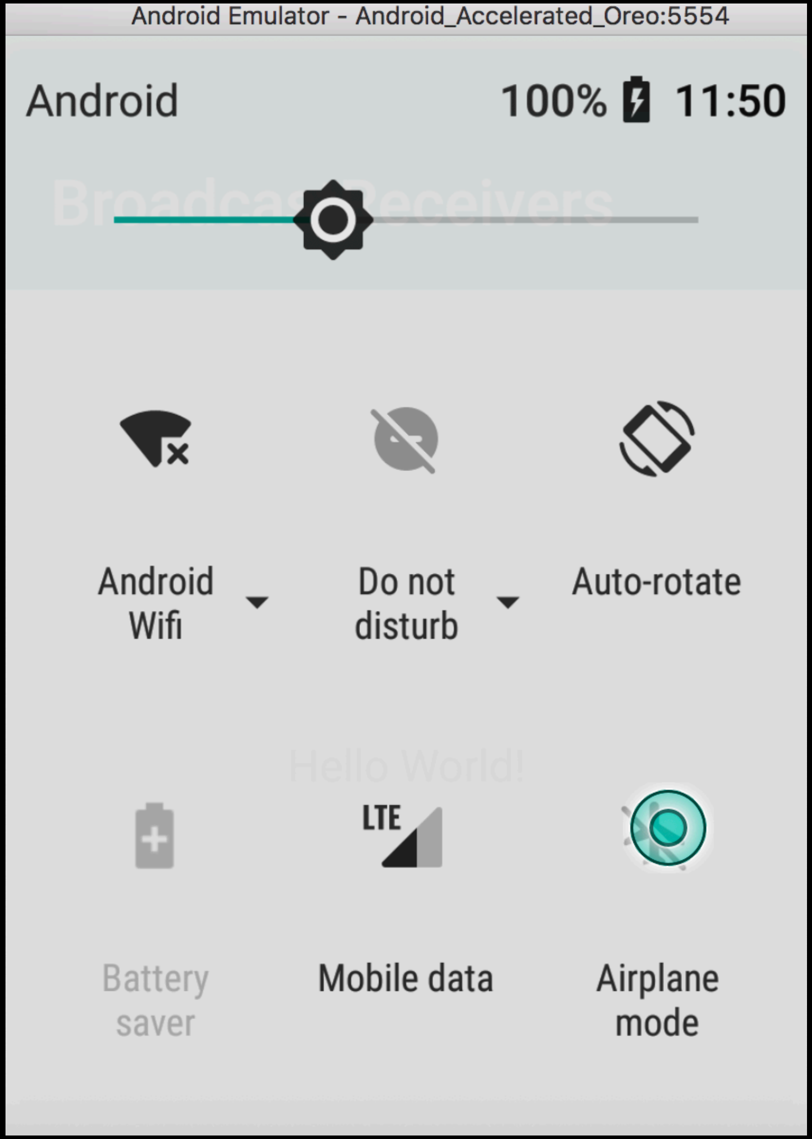
Let’s code

- Run our code



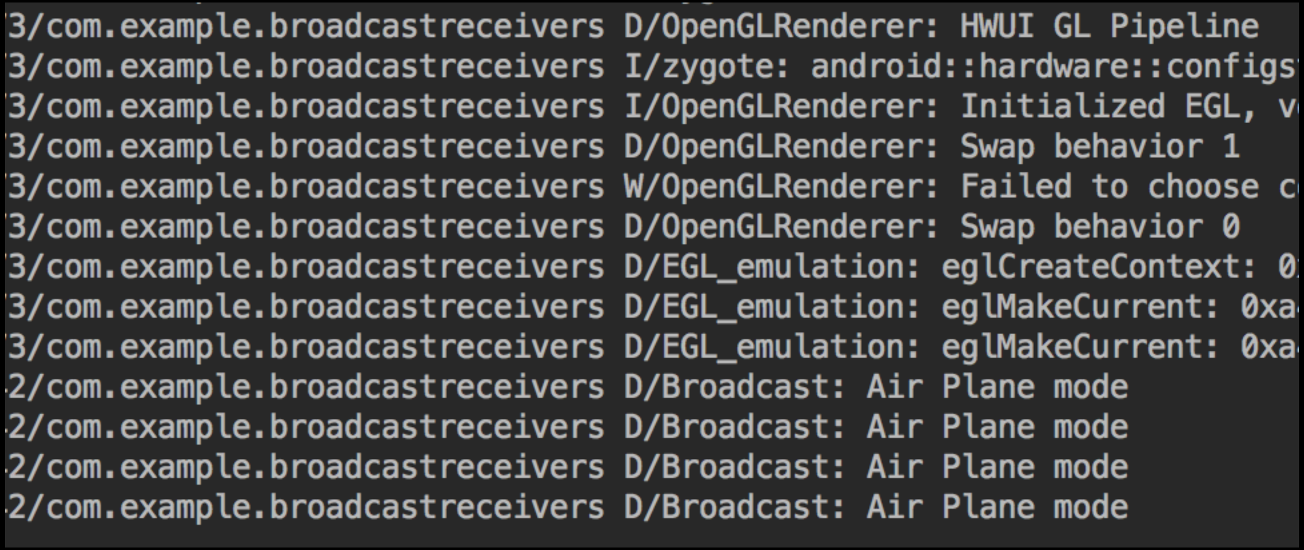
Let’s code

- Try click on/off AirPlane Mode on phone



Let’s code

- In 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
```

- Grab full code at: https://github.com/tsug0d/AndroidMobilePentest101/blob/master/lab/MainActivity.java_BroadcastReceivers