Activities Access

## Background

Android activity navigation is quite like how Internet navigation works. In web-based applications, many pages are public. For example, we could access many pages by adding its name after the domain name, like so: <http://host/home.html>. In Android, we could do the same thing -- we could navigate to any activity using “am” package commands.

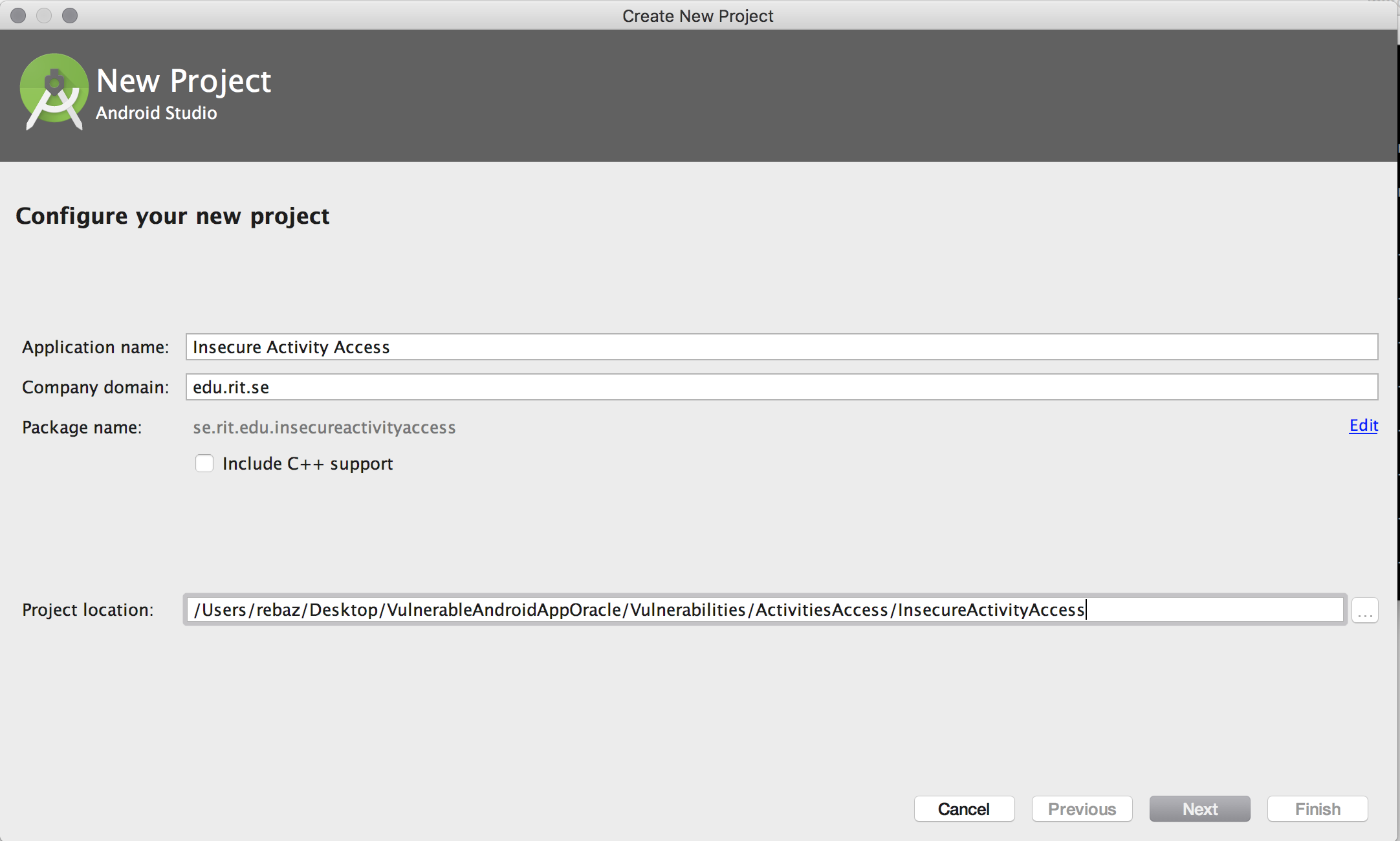
This could be quite the security problem. There are certain activities whose access should be restricted. Take a bank app that has two activities: the first activity for login and the second activity for making transactions the user must login to do transactions.

The security weakness here is that hackers could possibly circumvent login and navigate to the restricted-access activities by using “am” package commands.

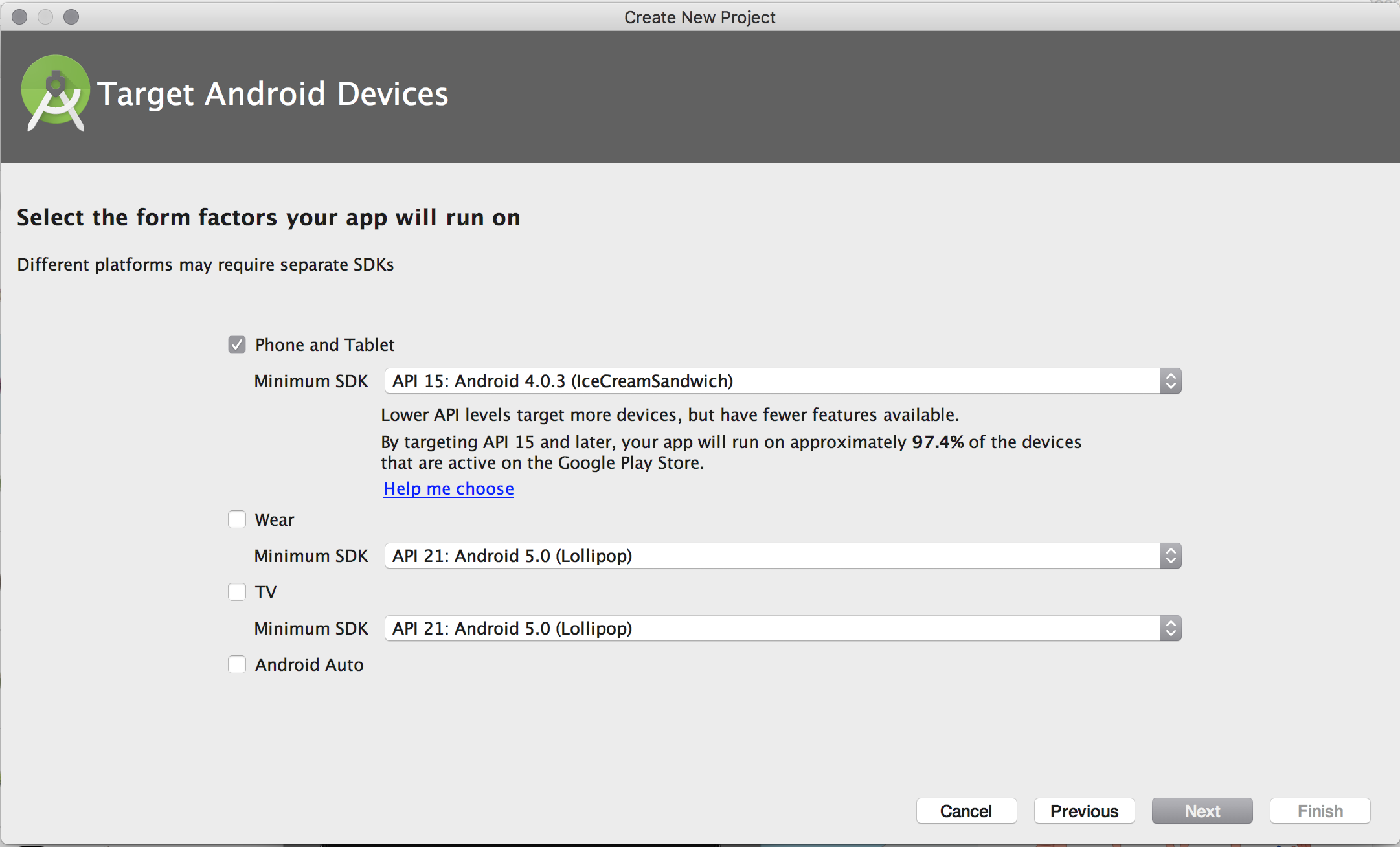
## Activity Instructions

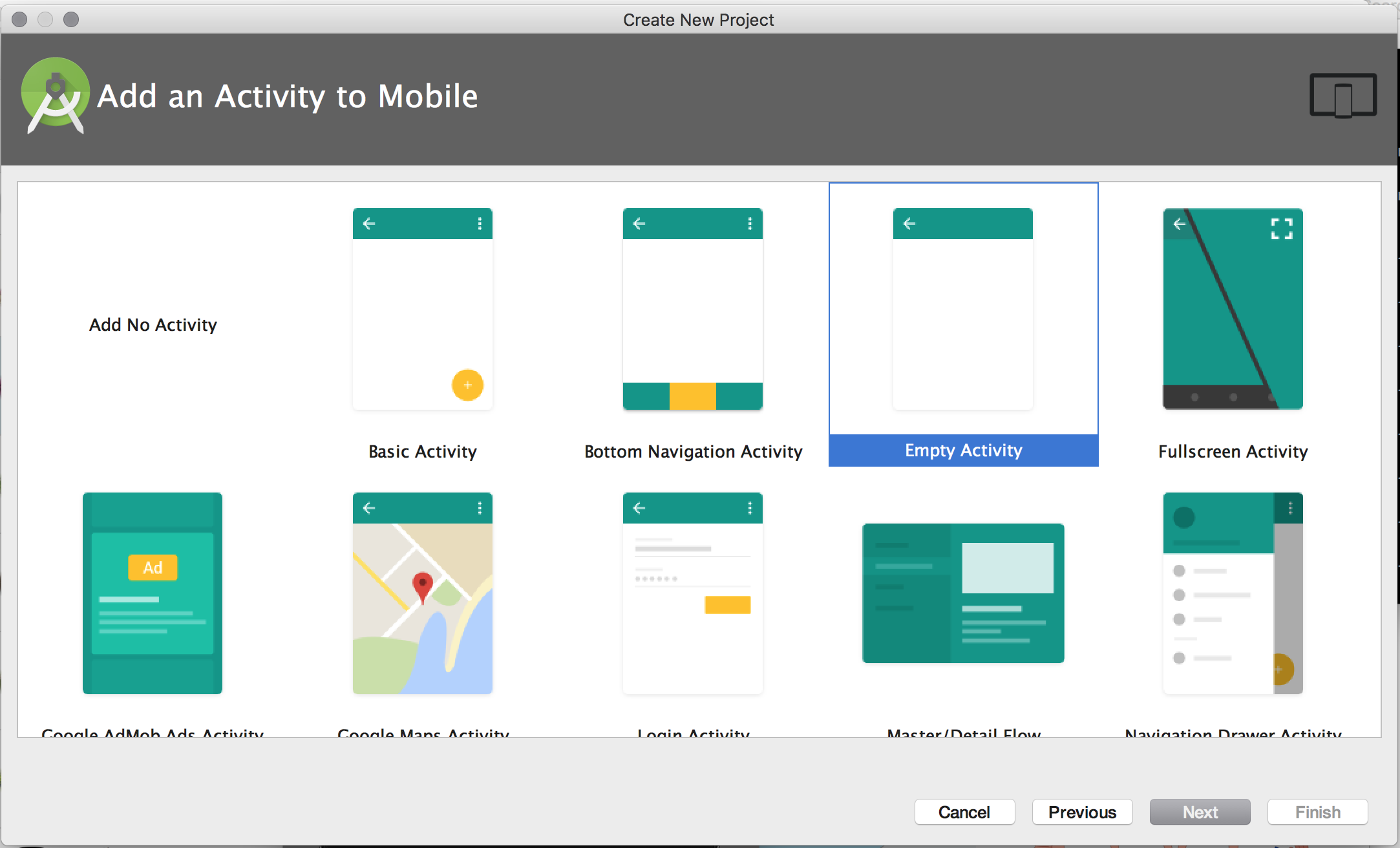
We will illustrate the problem by creating an app and exploiting it ourselves.

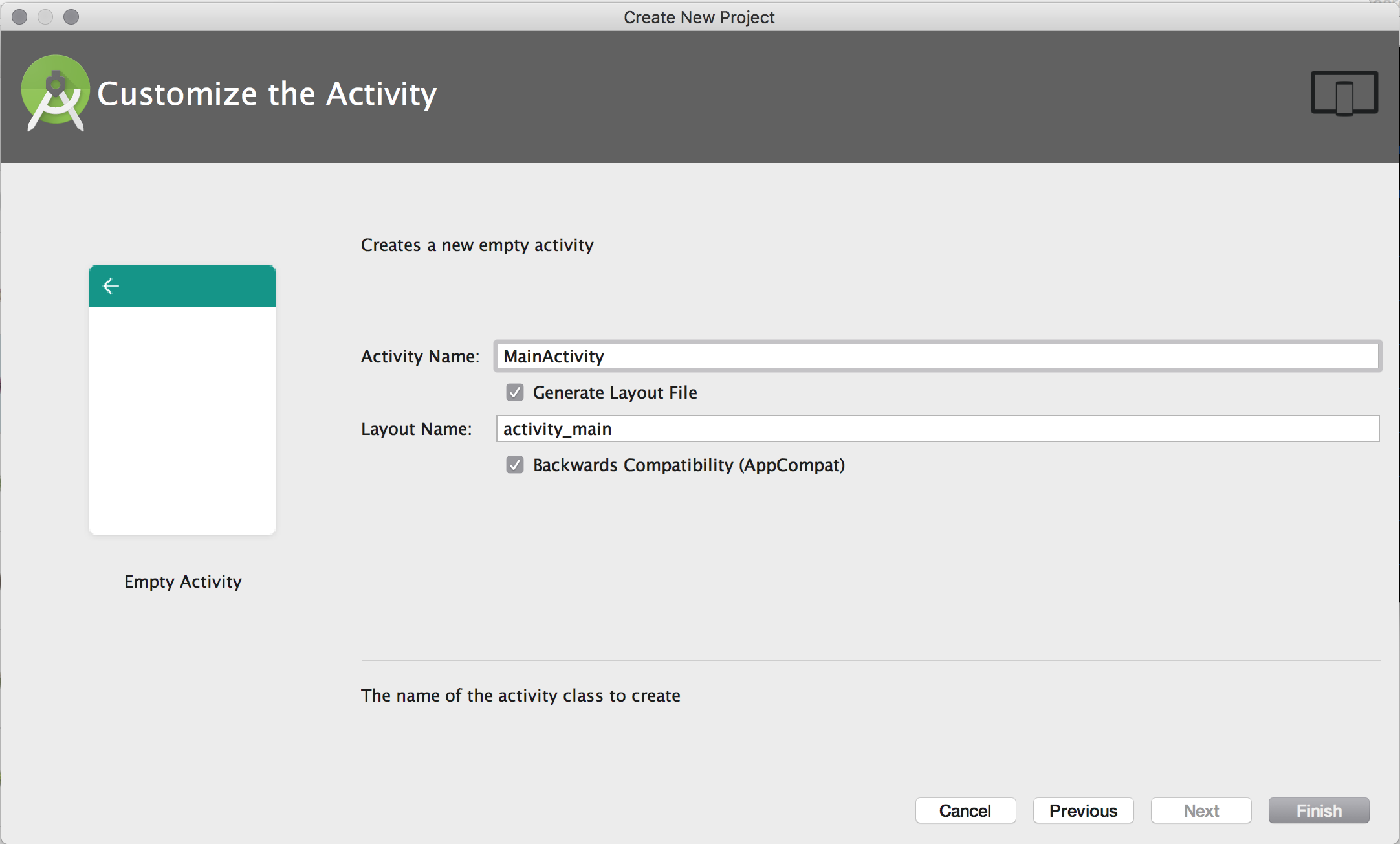
1. Create an app that asks the user to enter a username and password. Upon correct entry of login credentials, the user will be redirected to the second page to change their password.
2. Show how an attacker might access the activity to change the user password without login.
3. Explain techniques we might use to defend ourselves.
4. Project Creation
   1. Follow the screens below to create a new project:



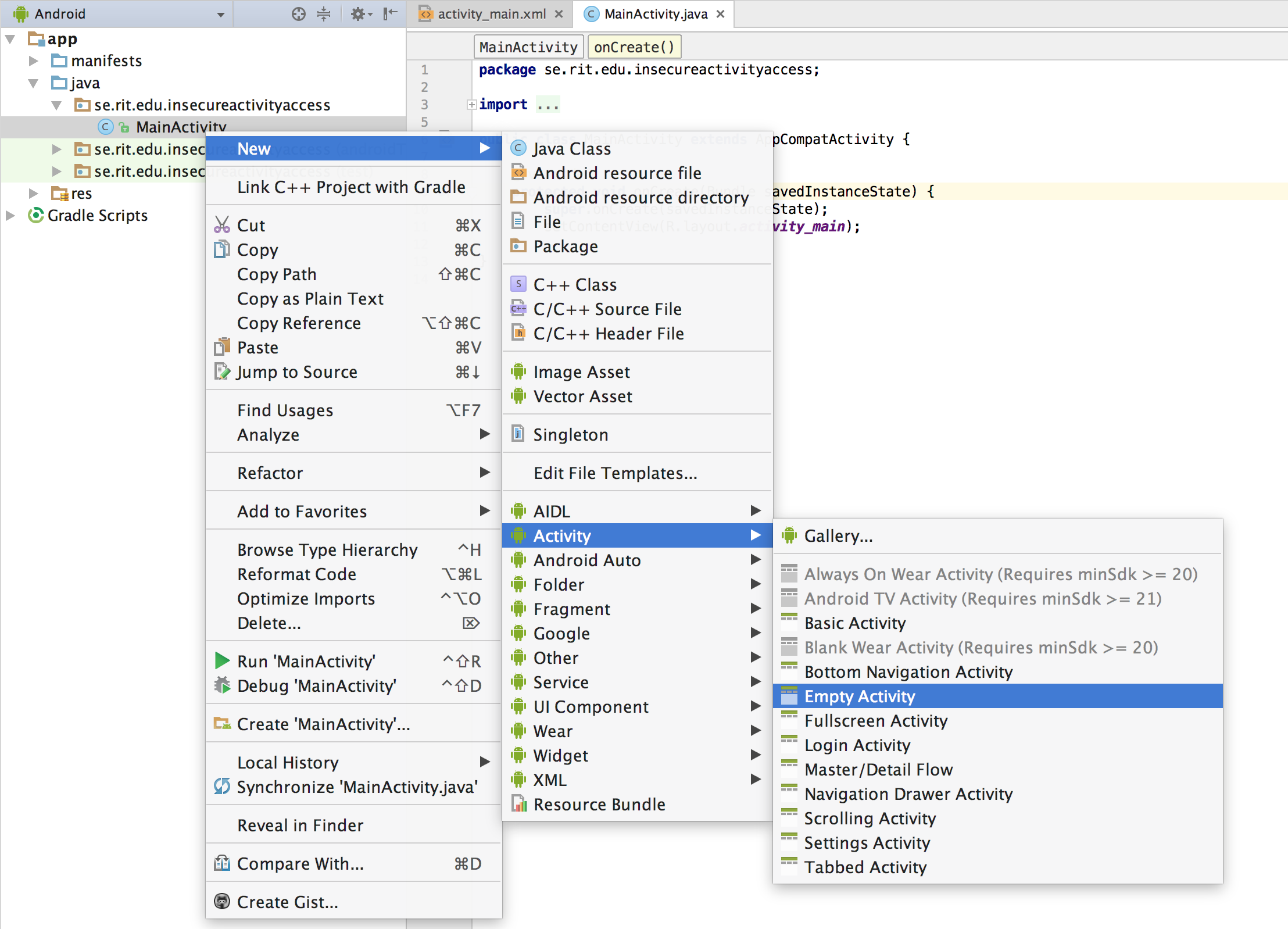
Name the project “Insecure Activity Access”.





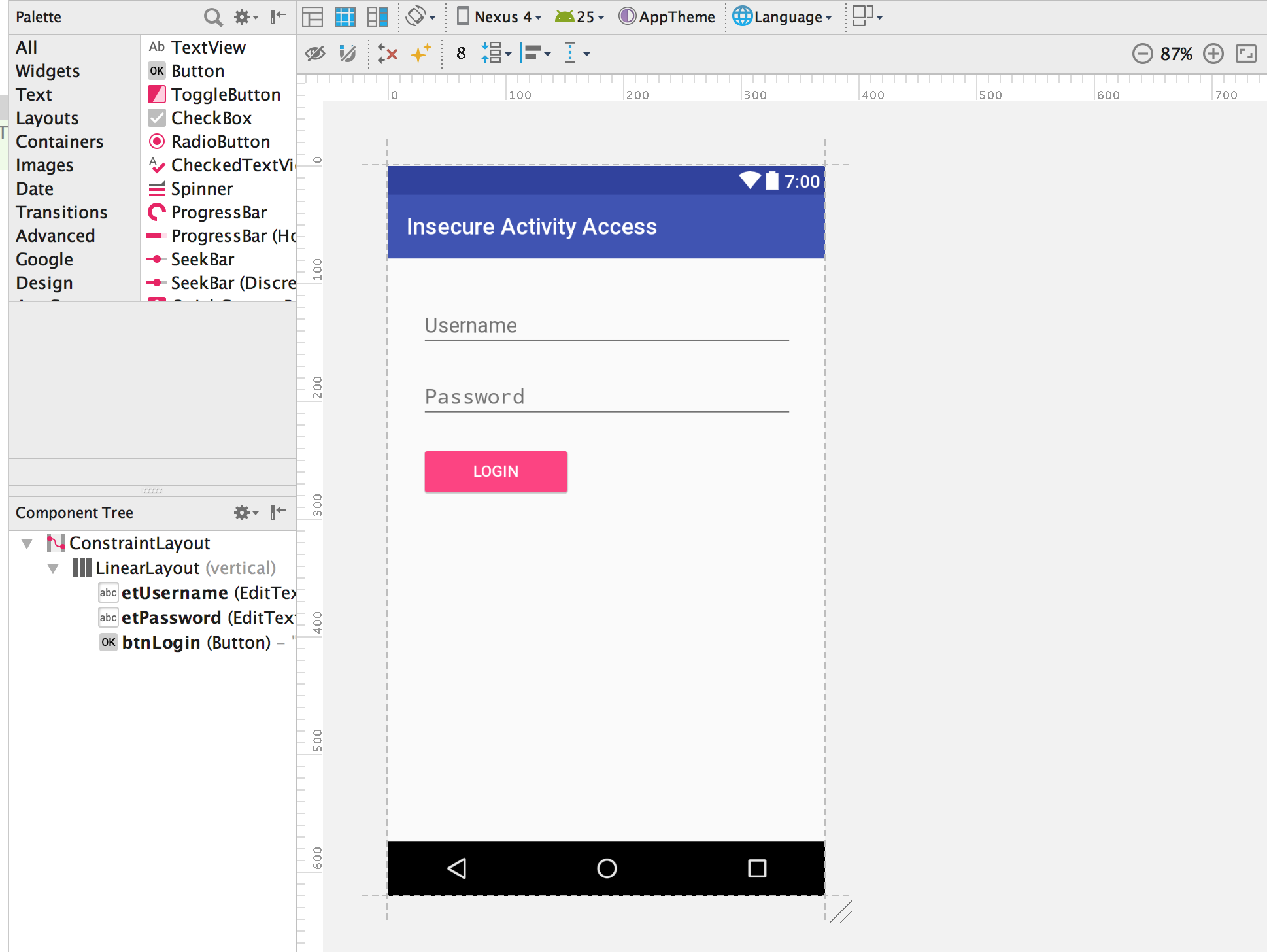


1. Add an Activity
   1. Add a new activity called “Main2Activity.java” by clicking on “ActivityMain.java”, found under “app/java/package\_name\_here/MainActivity” as shown in the image below



1. Construct User Interface
2. Open activity\_main.xml and clear all and paste the following code

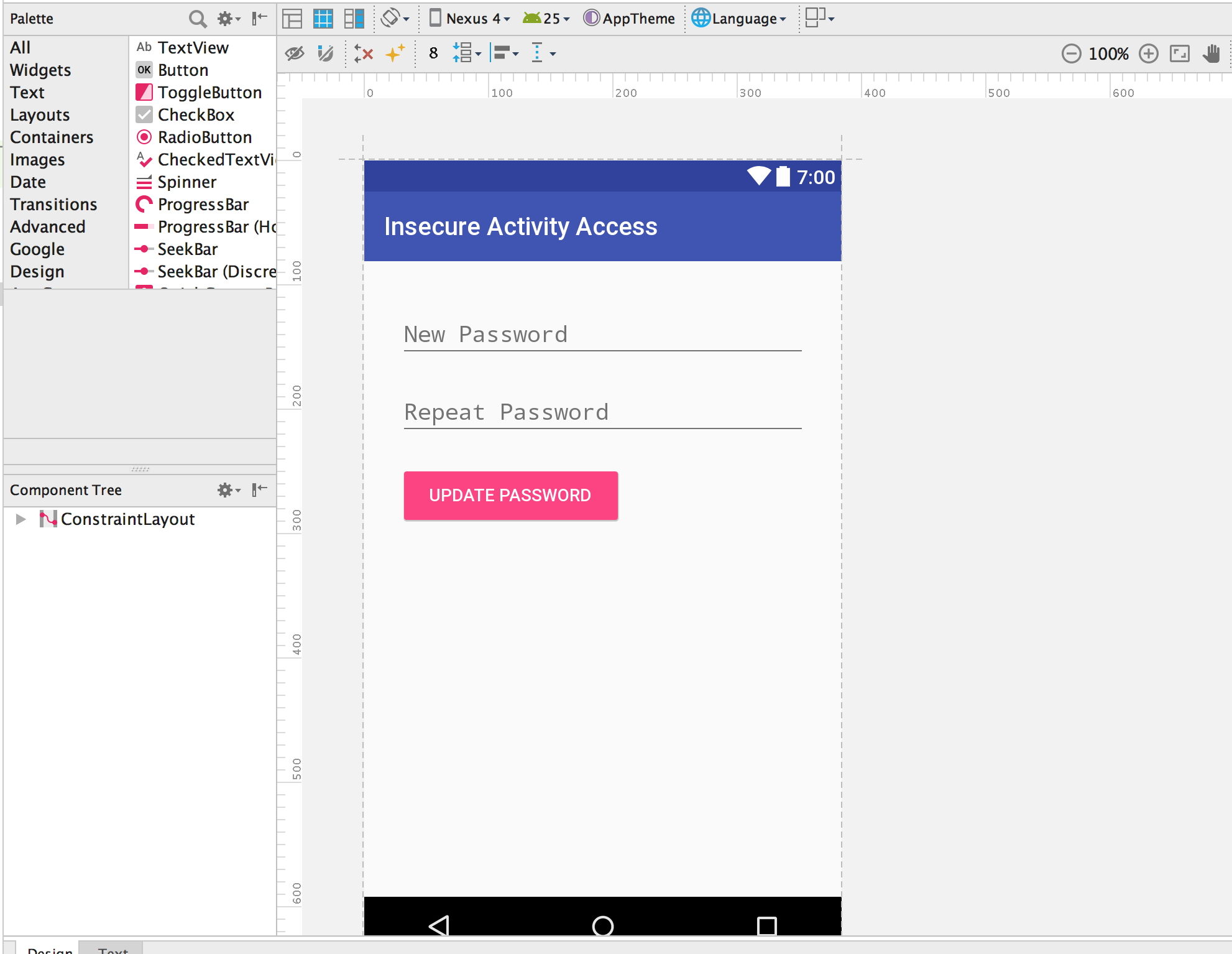
|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <android.support.constraint.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:app="http://schemas.android.com/apk/res-auto"  xmlns:tools="http://schemas.android.com/tools"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  android:layout\_marginTop="30dp"  android:layout\_marginLeft="20dp"  android:layout\_marginRight="20dp"  tools:context=".MainActivity">  <LinearLayout  android:layout\_width="328dp"  android:layout\_height="495dp"  android:layout\_weight="1"  android:orientation="vertical"  tools:layout\_editor\_absoluteX="8dp"  tools:layout\_editor\_absoluteY="8dp">  <EditText  android:id="@+id/etUsername"  android:layout\_width="match\_parent"  android:layout\_height="wrap\_content"  android:ems="10"  android:hint="Username"  android:inputType="textPersonName" />  <EditText  android:id="@+id/etPassword"  android:layout\_width="match\_parent"  android:layout\_height="wrap\_content"  android:layout\_marginTop="20dp"  android:ems="10"  android:hint="Password"  android:inputType="textPassword" />  <Button  android:id="@+id/btnLogin"  style="@style/Widget.AppCompat.Button.Colored"  android:layout\_width="133dp"  android:layout\_height="wrap\_content"  android:layout\_marginTop="20dp"  android:text="Login" />  </LinearLayout>  </android.support.constraint.ConstraintLayout> |

This is what the layout should look like:

1. Construct the layout for the second activity by pasting the following to activity\_main2.xml

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <android.support.constraint.ConstraintLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:app="http://schemas.android.com/apk/res-auto"  xmlns:tools="http://schemas.android.com/tools"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  android:layout\_marginTop="30dp"  android:layout\_marginLeft="20dp"  android:layout\_marginRight="20dp"  tools:context=".Main2Activity">  <LinearLayout  android:layout\_width="328dp"  android:layout\_height="495dp"  android:layout\_weight="1"  android:orientation="vertical"  tools:layout\_editor\_absoluteX="8dp"  tools:layout\_editor\_absoluteY="8dp"  android:weightSum="1">  <EditText  android:id="@+id/etUsername"  android:layout\_width="match\_parent"  android:layout\_height="wrap\_content"  android:ems="10"  android:hint="New Password"  android:inputType="textPassword" />  <EditText  android:id="@+id/etPassword"  android:layout\_width="match\_parent"  android:layout\_height="wrap\_content"  android:layout\_marginTop="20dp"  android:ems="10"  android:hint="Repeat Password"  android:inputType="textPassword" />  <Button  android:id="@+id/btnLogin"  style="@style/Widget.AppCompat.Button.Colored"  android:layout\_width="180dp"  android:layout\_height="wrap\_content"  android:layout\_marginTop="20dp"  android:text="Update Password"  android:layout\_weight="0.01" />  </LinearLayout>  </android.support.constraint.ConstraintLayout> |

The second activity should look like this



1. Code

Open MainActivity.java, found under “app/java/your\_package\_name”, and add the following code:

* 1. Add the following code inside the **onCreate** method:

|  |
| --- |
| @Override  **protected void** onCreate(Bundle savedInstanceState) {  **super**.onCreate(savedInstanceState);  setContentView(R.layout.***activity\_main***);   *// username and password hardcoded for testing purpose* **final** String USERNAME = **"admin"**;  **final** String PASSWORD = **"admin"**;    *// initialize user name instance with the real input in xml* **final** EditText etUsername = (EditText)findViewById(R.id.***etUsername***);   *// initialize password instance with the real input in xml* **final** EditText etPassword = (EditText)findViewById(R.id.***etPassword***);   *// initialize login button instance* **final** Button btnLogin = (Button)findViewById(R.id.***btnLogin***);  btnLogin.setOnClickListener(**new** View.OnClickListener() {  **public void** onClick(View v) {   *// collect user's username input* String username = etUsername.getText().toString();   *// collect user's password input* String password = etPassword.getText().toString();   *// compare values* **if**(USERNAME.equals(username) && PASSWORD.equals(password))  {  Toast.*makeText*( MainActivity.**this**,  **"You are logged in successfully"**,  Toast.***LENGTH\_LONG***).show();   Intent intent = **new** Intent(getApplicationContext(), Main2Activity.**class**);startActivity(intent);  }   **else** {  Toast.*makeText*( MainActivity.**this**,  **"Invalid credentials"**,  Toast.***LENGTH\_LONG***).show();  }  }  });    } |

* 1. Add the following imports to the file, below the package declaration.

|  |
| --- |
| **import** android.content.Intent; **import** android.support.v7.app.AppCompatActivity; **import** android.os.Bundle; **import** android.view.View; **import** android.widget.Button; **import** android.widget.EditText; **import** android.widget.Toast; |

Open Main2Activity.java, and add the following code:

* 1. Add the following code inside the **onCreate** method:

|  |
| --- |
| @Override **protected void** onCreate(Bundle savedInstanceState) {  **super**.onCreate(savedInstanceState);  setContentView(R.layout.***activity\_main2***);   Bundle b = getIntent().getExtras(); } |

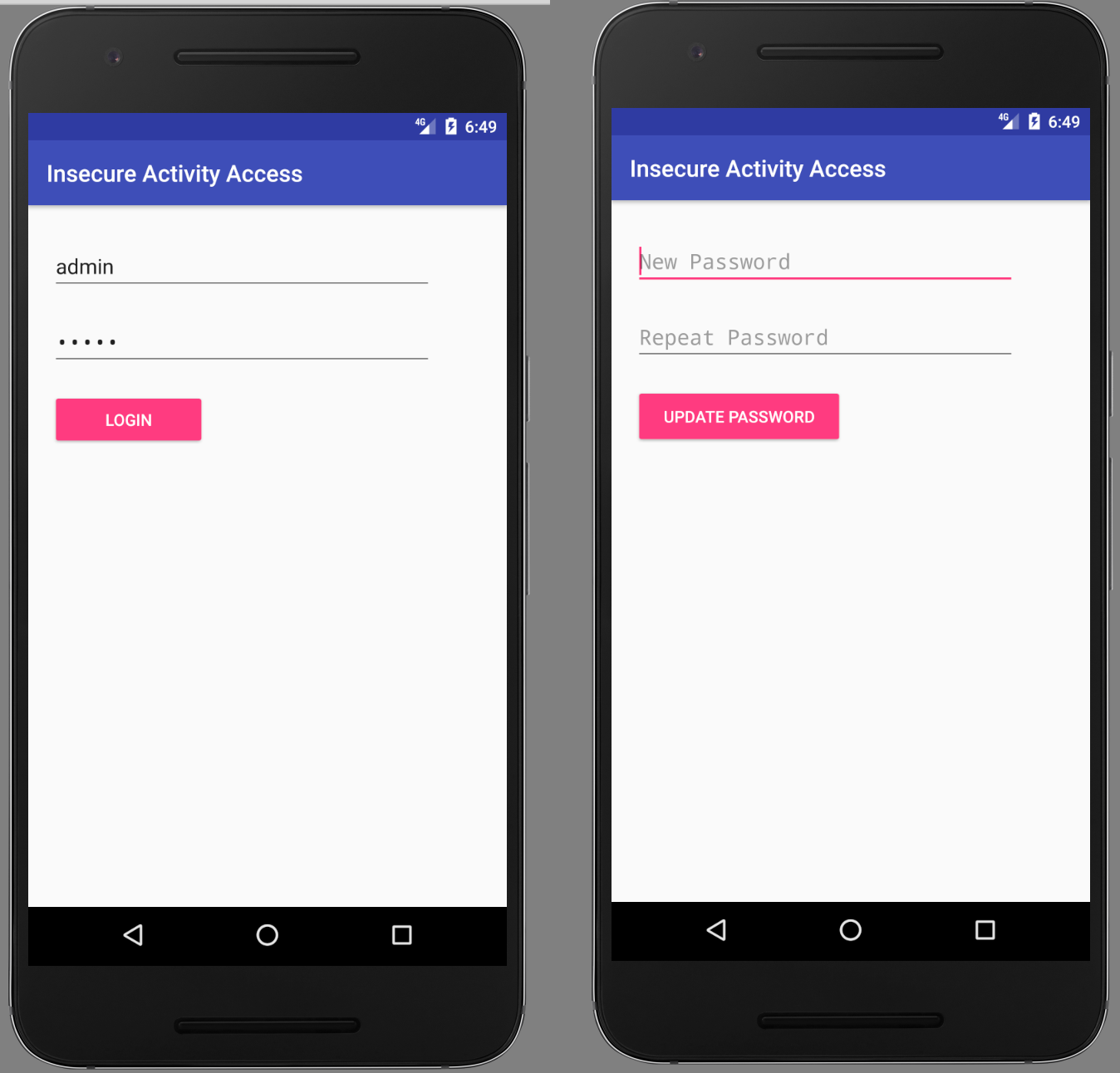
The above code achieves the following:

1. Upon creation of the MainActivity class, the **onCreate** method executes.
   1. Passes the Bundle named savedInstanceState to the superclass AppCompatActivity
   2. Initializes the variables declared in the first part with their corresponding layout objects.
   3. Creates a listener for the login button that upon click, will:
      1. Compare the credentials entered to the strings we have saved. If the credentials match what we have, we create an Intent with the second activity.
      2. Start the second activity.
2. Upon creation of the Main2Activity class, the **onCreate** method executes.
   1. Passes the Bundle named savedInstanceState to the superclass AppCompatActivity
   2. Sets the content view to be the layout we designed for the second activity.
   3. Grabs the bundle that came with the Intent.

## Exploitation Instructions

We shall see for ourselves how we can view the login credentials.

1. Run the app. Enter the login credentials of “admin” for username and “admin” for password (demonstration purposes only).



1. Using adb shell, view the saved preferences file by:
   1. Open Terminal or Command Prompt.
   2. Run the following commands.
      1. On Mac OS X:

cd Library/Android/sdk/platform-tools

On Windows:

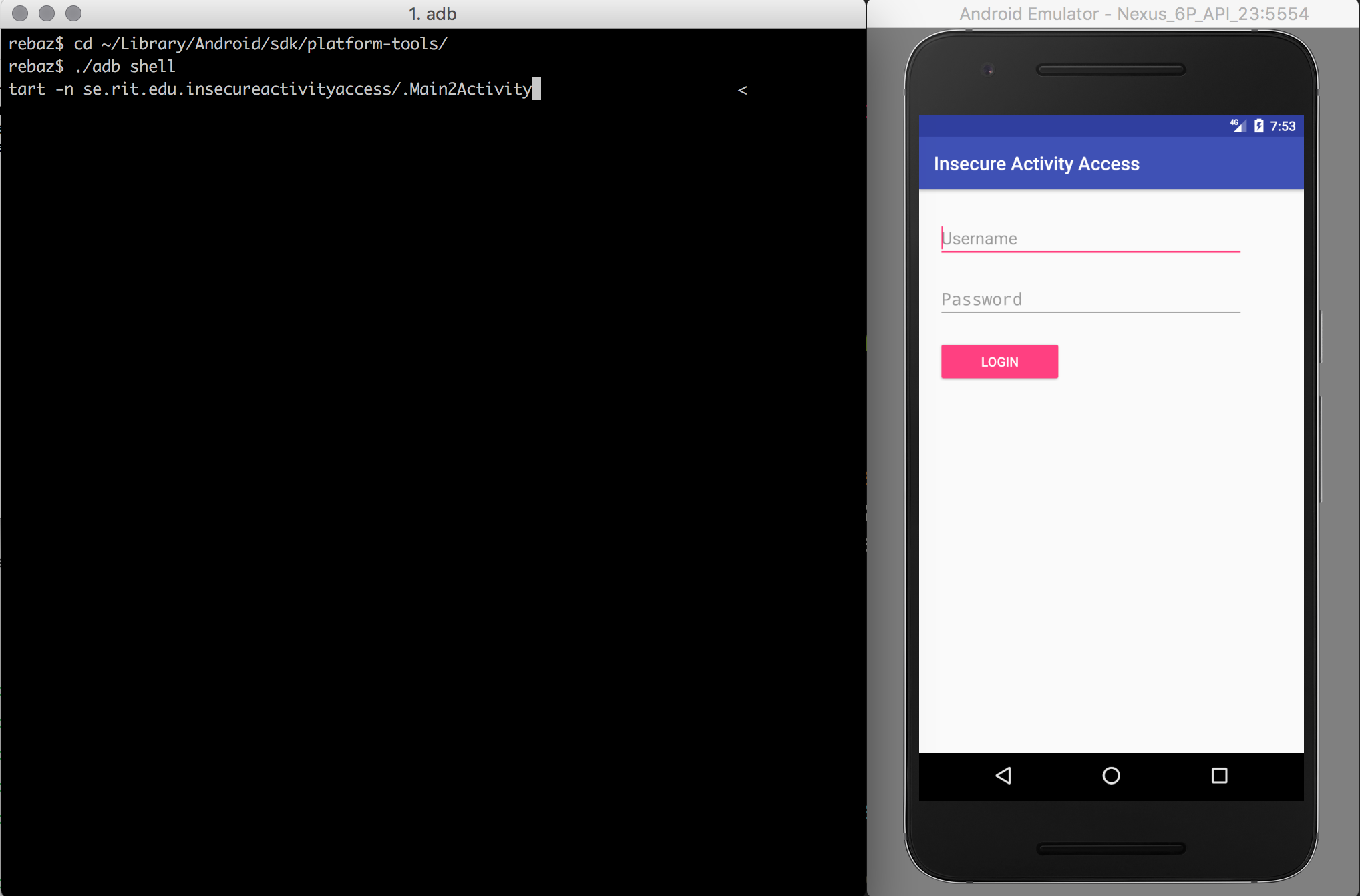
cd C:\Users\YOUR\_USERNAME\_HERE\AppData\Local\Android\sdk\platform-tools

* + 1. From here, it doesn’t matter what platform you are running this on. We simply needed to find the Android/sdk/platform-tools directory.

./adb shell

* + 1. am start –n package\_name/.ActivityName

1. Once you have executed the commands above, you will be sent to the activity that is supposed to be after login only. We will be able to change the password without login.



## 

## Defense

To fix this problem, we will send the key associated with the value over the intent to change password activity. In the second activity, we will then read the key and make sure the value is correct. If it is correct, we can start the password-changing activity. Otherwise, we will dismiss the activity. Then, when we run the “am” command without the key to open Main2Activity, it will not open.

1. Code

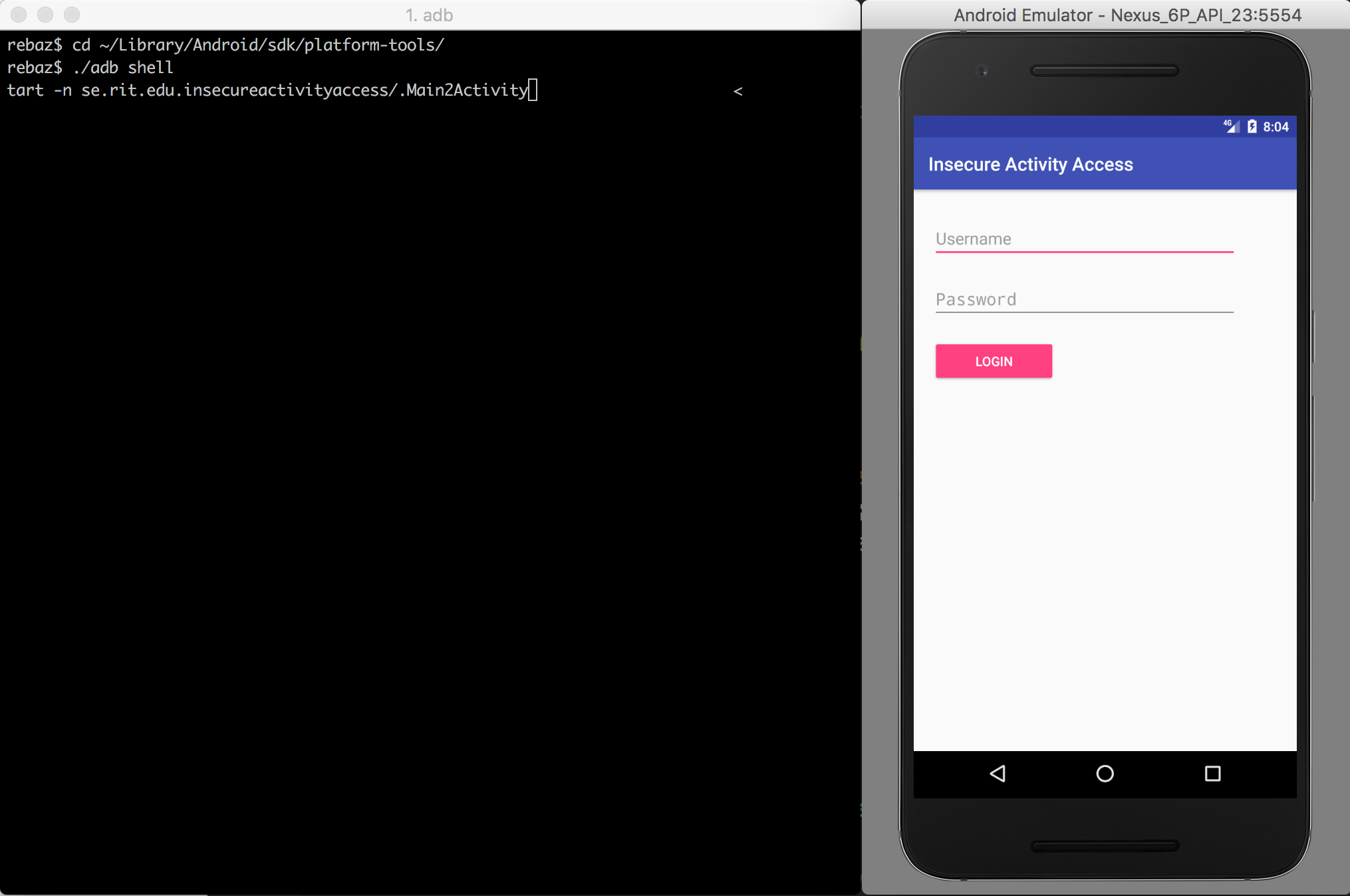
The **onCreate** method of the MainActivity class is very like the one we see in the previous part. The only thing that has changed is the highlighted line: we include a key-value pair with the intent we are passing to the startActivity function.

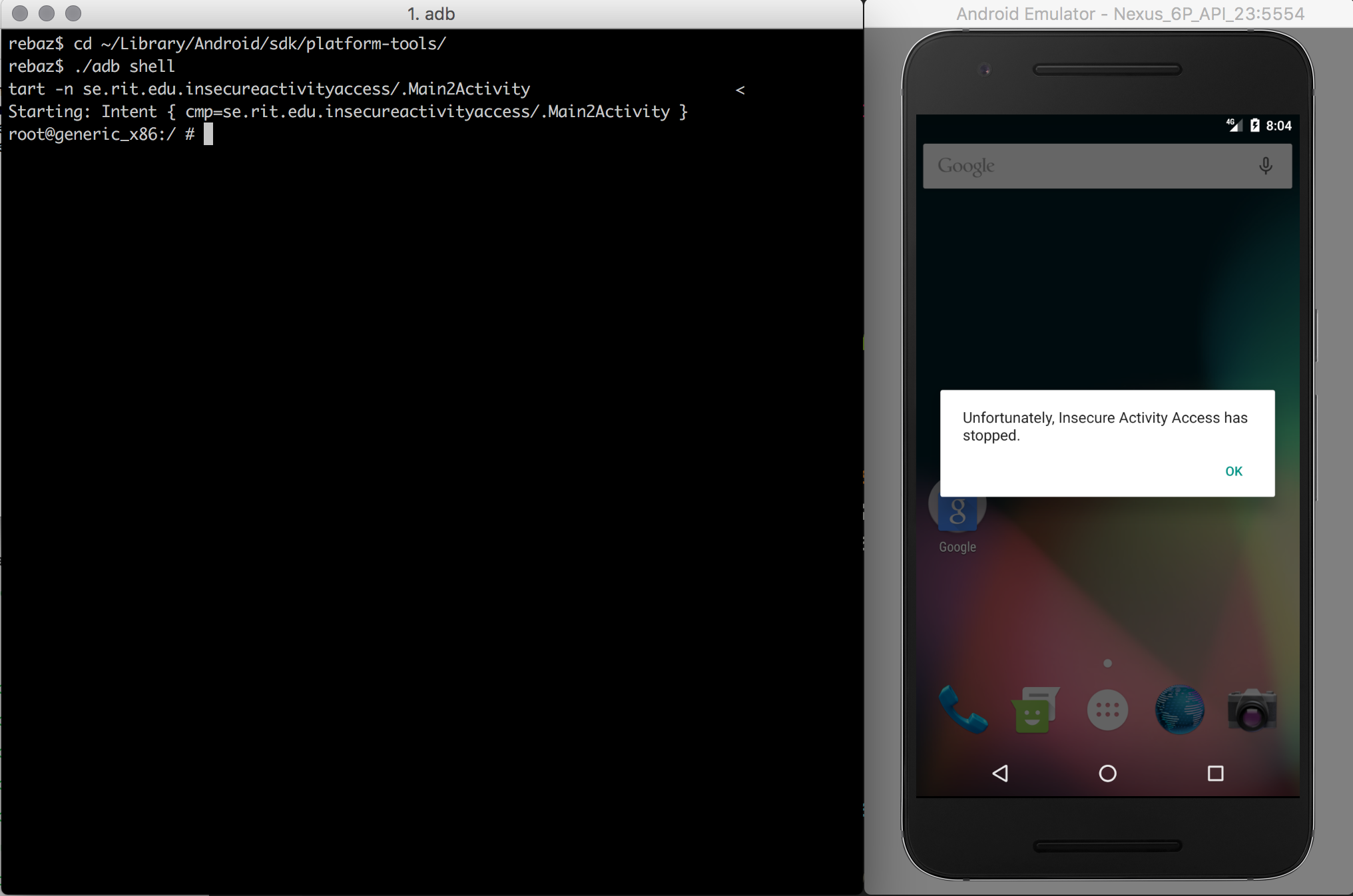
|  |
| --- |
| @Override  **protected void** onCreate(Bundle savedInstanceState) {  **super**.onCreate(savedInstanceState);  setContentView(R.layout.***activity\_main***);   *// username and password hardcoded for testing purpose* **final** String USERNAME = **"admin"**;  **final** String PASSWORD = **"admin"**;    *// initialize user name instance with the real input in xml* **final** EditText etUsername = (EditText)findViewById(R.id.***etUsername***);   *// initialize password instance with the real input in xml* **final** EditText etPassword = (EditText)findViewById(R.id.***etPassword***);   *// initialize login button instance* **final** Button btnLogin = (Button)findViewById(R.id.***btnLogin***);  btnLogin.setOnClickListener(**new** View.OnClickListener() {  **public void** onClick(View v) {   *// collect user's username input* String username = etUsername.getText().toString();   *// collect user's password input* String password = etPassword.getText().toString();   *// compare values* **if**(USERNAME.equals(username) && PASSWORD.equals(password))  {  Toast.*makeText*( MainActivity.**this**,  **"You are logged in successfully"**,  Toast.***LENGTH\_LONG***).show();   Intent intent = **new** Intent(getApplicationContext(), Main2Activity.**class**);  *intent.putExtra("key", 3433);* startActivity(intent);  }   **else** {  Toast.*makeText*( MainActivity.**this**,  **"Invalid credentials"**,  Toast.***LENGTH\_LONG***).show();  }  }  }); |

Now, we change the **onCreate** method of the Main2Activity class to check the intent it is passed for the key-value pair. If it is incorrect, or non-existent, then the Main2Activity class will simply not start.

|  |
| --- |
| @Override **protected void** onCreate(Bundle savedInstanceState) {  **super**.onCreate(savedInstanceState);  setContentView(R.layout.***activity\_main2***);   Bundle b = getIntent().getExtras();   **int** key = b.getInt(**"key"**);  **if** (key != 3433)  finish(); } |

1. When we run the same commands in adb again, we will get the following screens:



****

As we can see, an attacker would no longer be able to access the “change password” screen without the key-value pair.