Ex140 Submission

Gary Jones

Contents

Executive Summary

Goals

The goal of this exercise is to use mobile application penetration testing techniques to see if a mobile app is exposing sensitive data.

Risk Ranking/Profile

The findings of this exercise is critical as the credentials are hard-coded in the software.

Summary of Findings

The username and password is hard-coded under the ItemListActivity/Async directory on line 146. This is easily decrypted to show the credentials.

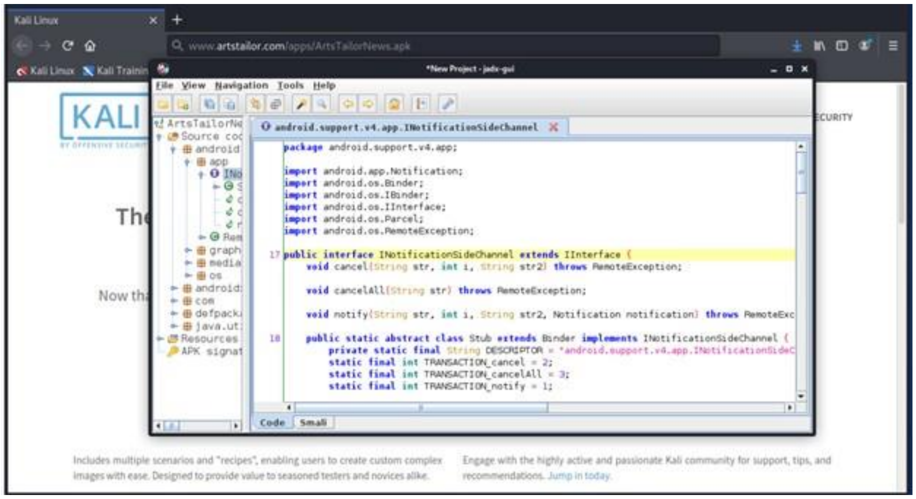
Recommendation Summary

Do not hard-code the credentials within the software.

Attack Narrative

To begin I downloaded the apk file we were set to analyze from http://www.artstailor.com/apps/ArtsTailorNews.apk and loaded it into jadx-gui (see figure 1). After this I navigated throughout the different directories looking for anything obviousl that would compromise the integrety of the system. Within the directory

Source code/com/example.artstailor.com/ItemListActivity/Async on line 146 I identified that credentials were being hardcoded (see figure 2). After this I saved the credentials into a file and rant base64 -d to decrypt the information thus revealing the user credentials (see figure 3). By logging in with this information a user is able to pull all records from the test database.

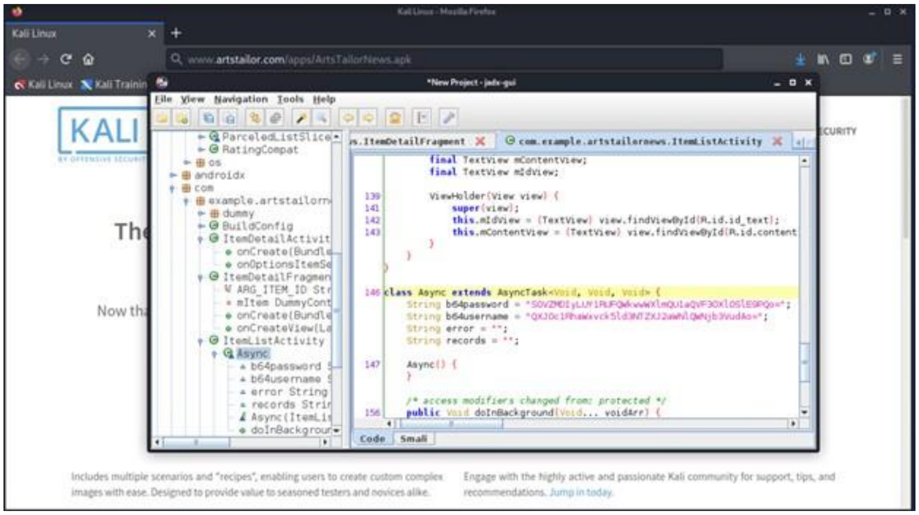

Kali Linux
www.artstailor.com/apps/ArtsTailorNews.apk
*New Project - jadx-gui
File View Navigation Tools Help
android.support.v4.app.INotificationSideChannel
Code Smali

```
package android.support.v4.app;

import android.app.Notification;
import android.os.Binder;
import android.os.IBinder;
import android.os.IInterface;
import android.os.Parcel;
import android.os.RemoteException;

public interface INotificationSideChannel extends IInterface {
    void cancel(String str, int i, String str2) throws RemoteException;

    void cancelAll(String str) throws RemoteException;

    void notify(String str, int i, String str2, Notification notification) throws RemoteExc

    public static abstract class Stub extends Binder implements INotificationSideChannel {
        private static final String DESCRIPTOR = "android.support.v4.app.INotificationSideC
        static final int TRANSACTION_cancel = 2;
        static final int TRANSACTION_cancelAll = 3;
        static final int TRANSACTION_notify = 1;
```

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.

Engage with the highly active and passionate Kali community for support, tips, and recommendations. Jump in today.

Figure 1:

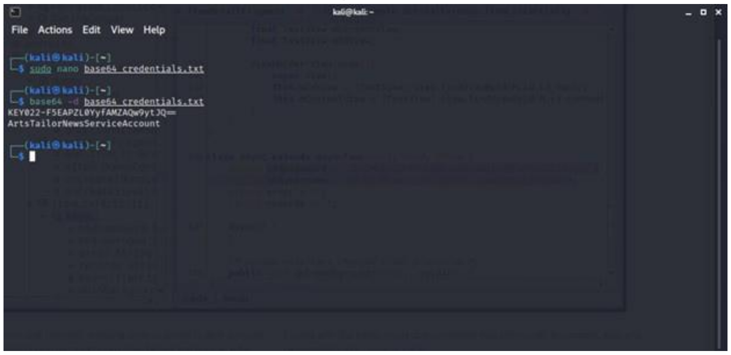

Kali Linux - Mozilla Firefox
www.artstailor.com/apps/ArtsTailorNews.apk
*New Project - jadx-gui
File View Navigation Tools Help
s.ItemDetailFragment
com.example.artstailornews.ItemListActivity
Code Smali

```
            final TextView mContentView;
            final TextView mIdView;

            ViewHolder(View view) {
                super(view);
                this.mIdView = (TextView) view.findViewById(R.id.id_text);
                this.mContentView = (TextView) view.findViewById(R.id.content
            }
        }
    }

class Async extends AsyncTask<Void, Void, Void> {
        String b64password = "S0VZMDIyLUY1RUFQWkwwWXlmQU1aQVF3OXl0SlE9PQo=";
        String b64username = "QXJ0c1RhaWxvck5ld3NTZXJ2aWNlQWNjb3VudAo=";
        String error = "";
        String records = "";

        Async() {
        }

        /* access modifiers changed from: protected */
        public Void doInBackground(Void... voidArr) {
```

Includes multiple scenarios and "recipes", enabling users to create custom complex images with ease. Designed to provide value to seasoned testers and novices alike.

Engage with the highly active and passionate Kali community for support, tips, and recommendations. Jump in today.

Figure 2:



```
┌──(kali㉿kali)-[~]
└─$ sudo nano base64_credentials.txt

┌──(kali㉿kali)-[~]
└─$ base64 -d base64_credentials.txt
KEY022-F5EAPZL0YyfAMZAQw9ytJQ==
ArtsTailorNewsServiceAccount

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 3: