National Forensic Sciences University

School of Cyber security and Digital Forensics

Subject: CTMSCS S2 P3 Android Security

(TA-II Assignment)

Submitted to: Mr. Digvijay Singh Rathod and Mr. Jay Teraiya

Submitted by: Disha Sharma (240103002014)

Submission Date: 06/04/2025

INDEX

1. Android Studio and AVD
2. Android Debug Bridge Commands
3. DIVA Vulnerable Application
4. Reverse Engineering
5. Request Interception
6. Insecure Bank2 Application
7. GoatDroid Practical
8. Open GApps
9. Security Auditing using Drozer
10. Analysis using MobSF and FRIDA
11. OWASP Security Shepherd

Demonstration of Android Application Framework component such as Activity and android manifest file etc. using Android Studio.

activity_main.xml | AndroidManifest.xml | MainActivity.java

```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="TA2_Assignment"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.TA2_Assignment"
        tools:targetApi="31">
        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```

activity_main.xml | AndroidManifest.xml | MainActivity.java

```java
package com.example.ta2_assignment;

import ...

public class MainActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        EdgeToEdge.enable( $this$enableEdgeToEdge: this);
        setContentView(R.layout.activity_main);
        ViewCompat.setOnApplyWindowInsetsListener(findViewById(R.id.main), (v, insets) -> {
            Insets systemBars = insets.getInsets(WindowInsetsCompat.Type.systemBars());
            v.setPadding(systemBars.left, systemBars.top, systemBars.right, systemBars.bottom);
            return insets;
        });
    }
}
```

Demonstration of Android Intent and Intent Filter

activity_main.xml | SecondActivity.java | AndroidManifest.xml | MainActivity.java

```xml
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    xmlns:tools="http://schemas.android.com/tools"
    package="com.example.ta2_assignment">

    <application
        android:allowBackup="true"
        android:dataExtractionRules="@xml/data_extraction_rules"
        android:fullBackupContent="@xml/backup_rules"
        android:icon="@mipmap/ic_launcher"
        android:label="@string/app_name"
        android:roundIcon="@mipmap/ic_launcher_round"
        android:supportsRtl="true"
        android:theme="@style/Theme.TA2_Assignment"
        tools:targetApi="31">

        <activity android:name=".SecondActivity" />

        <activity
            android:name=".MainActivity"
            android:exported="true">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```

activity_main.xml | SecondActivity.java | AndroidManifest.xml | MainActivity.java

```java
package com.example.ta2_assignment;

import android.os.Bundle;
import android.view.Gravity;
import android.widget.TextView;
import androidx.appcompat.app.AppCompatActivity;
import androidx.constraintlayout.widget.ConstraintLayout;

public class SecondActivity extends AppCompatActivity {

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        // Create a ConstraintLayout
        ConstraintLayout layout = new ConstraintLayout( context: this);
        layout.setLayoutParams(new ConstraintLayout.LayoutParams(
                ConstraintLayout.LayoutParams.MATCH_PARENT,
                ConstraintLayout.LayoutParams.MATCH_PARENT));

        // Create and set up a TextView
        TextView textView = new TextView( context: this);
        textView.setText("This is Second Activity");
        textView.setTextSize(22);
        textView.setGravity(Gravity.CENTER);

        // Set layout parameters to center the TextView
        ConstraintLayout.LayoutParams params = new ConstraintLayout.LayoutParams(
                ConstraintLayout.LayoutParams.WRAP_CONTENT,
                ConstraintLayout.LayoutParams.WRAP_CONTENT);
```

Demonstration of Android Content Provider

```
tools:targetApi="31" >
<provider
    android:name=".ContactsProvider"
    android:authorities="com.example.ta2_assignment.provider"
    android:exported="true" />
```

ContactsDbHelper.java | ContactsProvider.java | AndroidManifest.xml | MainActivity.java

```
public class ContactsDbHelper extends SQLiteOpenHelper {

    6 usages
    public static final String TABLE_NAME = "contacts";
    2 usages
    public static final String COL_ID = "_id";
    1 usage
    public static final String COL_NAME = "name";
    1 usage
    public static final String COL_EMAIL = "email";

    1 usage
    private static final String CREATE_TABLE = "CREATE TABLE " + TABLE_NAME + " (" +
            COL_ID + " INTEGER PRIMARY KEY AUTOINCREMENT, " +
            COL_NAME + " TEXT, " +
            COL_EMAIL + " TEXT);";

    1 usage
    public ContactsDbHelper(Context context) {
        super(context, DATABASE_NAME, factory: null, version: 1);
    }

    @Override
    public void onCreate(SQLiteDatabase db) {
        db.execSQL(CREATE_TABLE);

        // Insert sample data
        db.execSQL("INSERT INTO " + TABLE_NAME + " (name, email) VALUES ('Alice', 'alice@example
        db.execSQL("INSERT INTO " + TABLE_NAME + " (name, email) VALUES ('Bob', 'bob@example.com
    }

    10 usages
    @Override
```

Demonstration of Android Broadcast Receiver

```xml
<receiver android:name=".MyBroadcastReceiver">
    <intent-filter>
        <action android:name="com.example.ta2_assignment.ACTION_CUSTOM_BROADCAST" />
    </intent-filter>
</receiver>
```

MyBroadcastReceiver.java | ContactsProvider.java | AndroidManifest.xml | MainActivity.java

```java
package com.example.ta2_assignment;

import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.widget.Toast;

public class MyBroadcastReceiver extends BroadcastReceiver {

    @Override
    public void onReceive(Context context, Intent intent) {
        // Action matched, show a Toast
        Toast.makeText(context, text: "Broadcast Received!", Toast.LENGTH_SHORT).show();
    }
}
```

Demonstration of Android Security Permission Model

```
<uses-permission android:name="android.permission.CAMERA" />
```

MyBroadcastReceiver.java | ContactsProvider.java | AndroidManifest.xml | MainActivity.java

```
package com.example.ta2_assignment;

import android.Manifest;
import android.content.pm.PackageManager;
import android.os.Bundle;
import android.widget.Button;
import android.widget.Toast;
import androidx.annotation.NonNull;
import androidx.appcompat.app.AppCompatActivity;
import androidx.core.app.ActivityCompat;
import androidx.core.content.ContextCompat;
import androidx.constraintlayout.widget.ConstraintLayout;

public class MainActivity extends AppCompatActivity {

    2 usages
    private static final int REQUEST_CAMERA_PERMISSION = 100;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        // Create layout and button programmatically
```

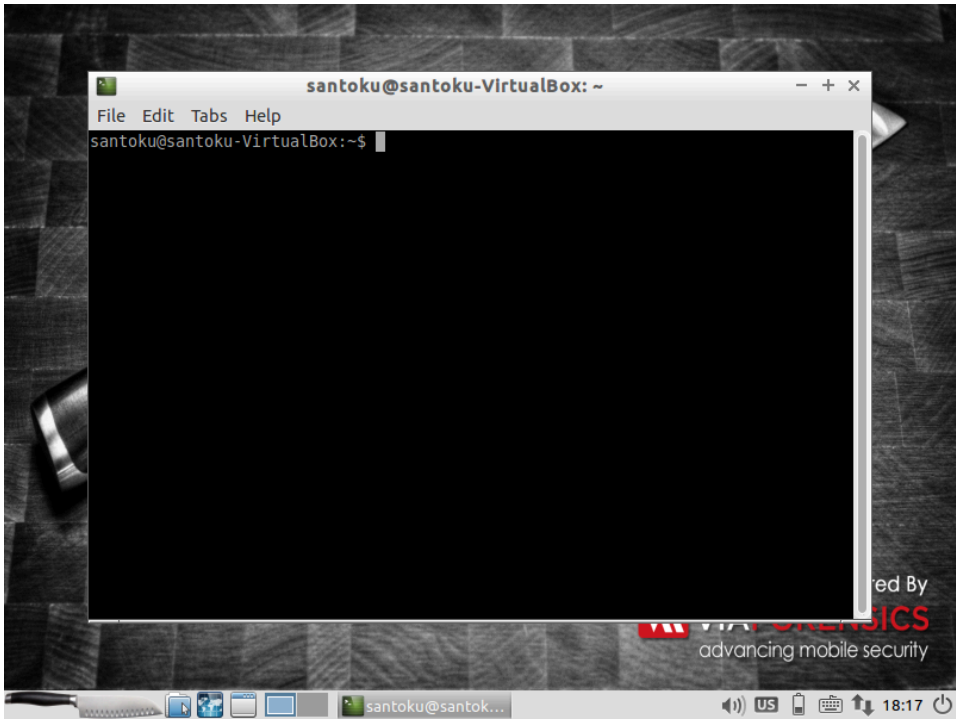
Demonstration of Android Services

```
        <service android:name=".MyService"
            android:exported="false" />
```

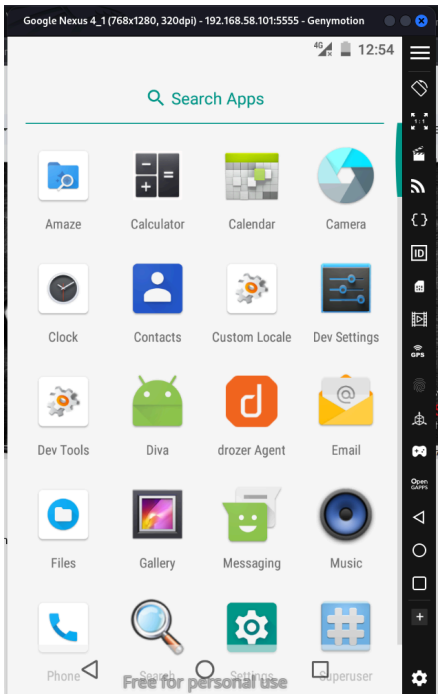
r.java | ContactsProvider.java | AndroidManifest.xml | MainActivity.java | MyService.java

```
package com.example.ta2_assignment;

import android.app.Service;
import android.content.Intent;
import android.os.IBinder;
import android.util.Log;

public class MyService extends Service {

    4 usages
    private static final String TAG = "MyService";

    @Override
    public void onCreate() {
        super.onCreate();
        Log.d(TAG, msg: "Service Created");
    }

    @Override
    public int onStartCommand(Intent intent, int flags, int startId) {
        Log.d(TAG, msg: "Service Started");

        // Simulate background task
        new Thread(() -> {
            for (int i = 1; i <= 5; i++) {
                try {
                    Thread.sleep( millis: 1000);
                    Log.d(TAG, msg: "Running task: " + i);
                } catch (InterruptedException e) {
                    e.printStackTrace();
                }
            }

            // Stop service once done
            stopSelf();
```

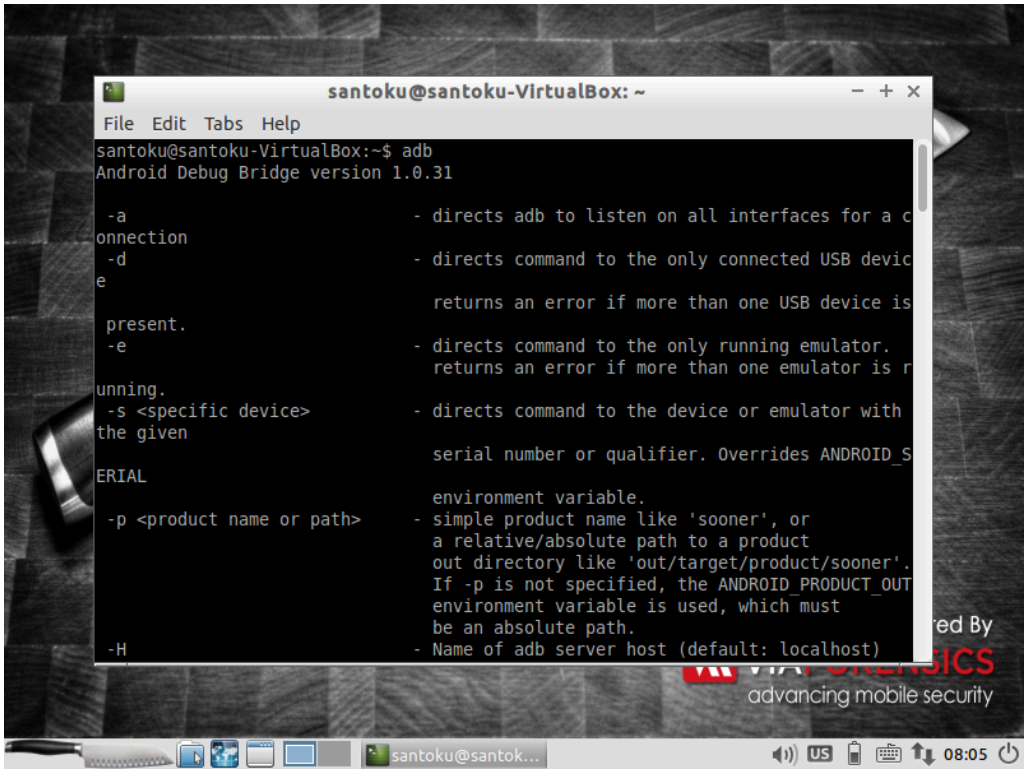
Configuration of Santoku OS

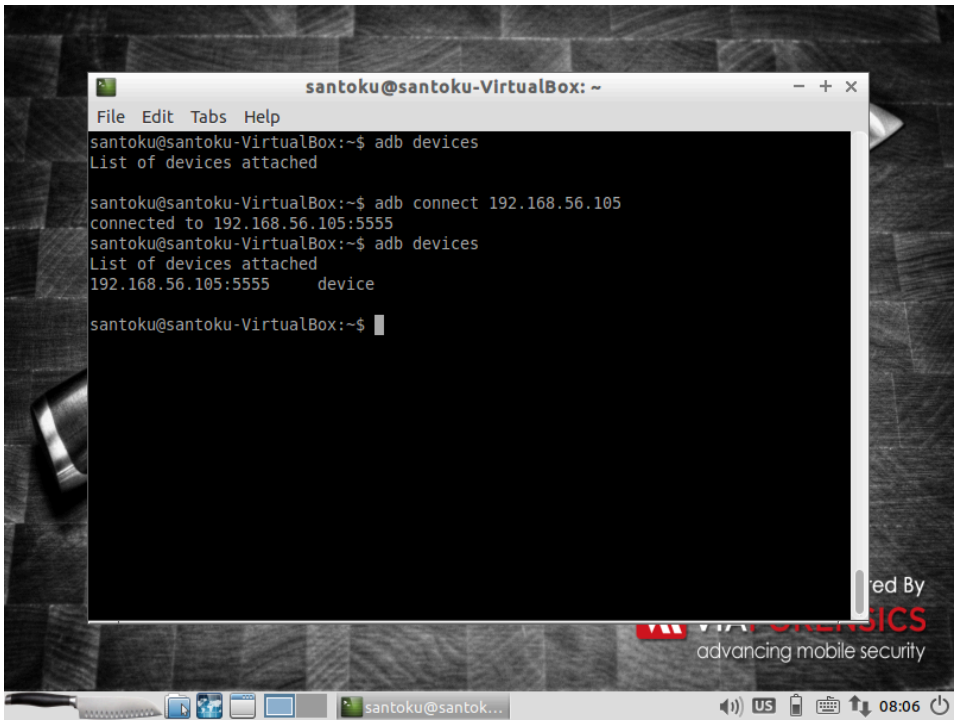


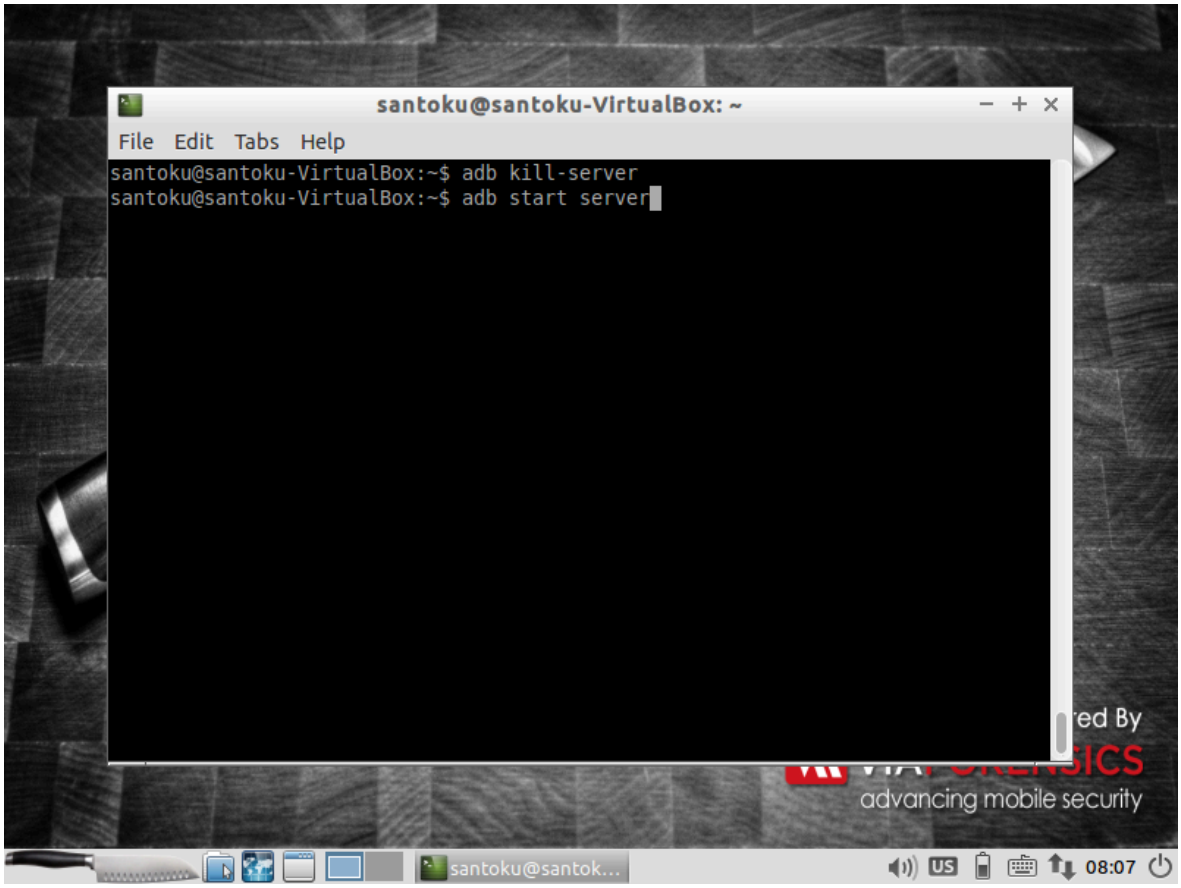
Configuration of Genymotion

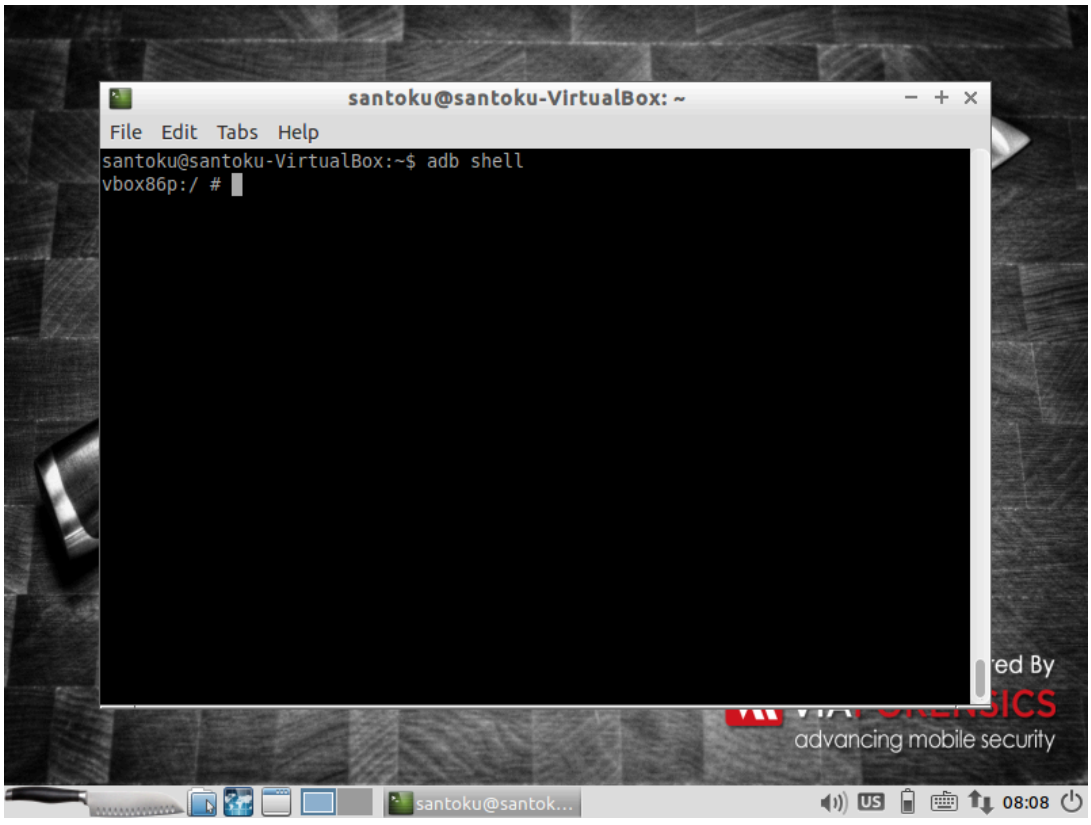


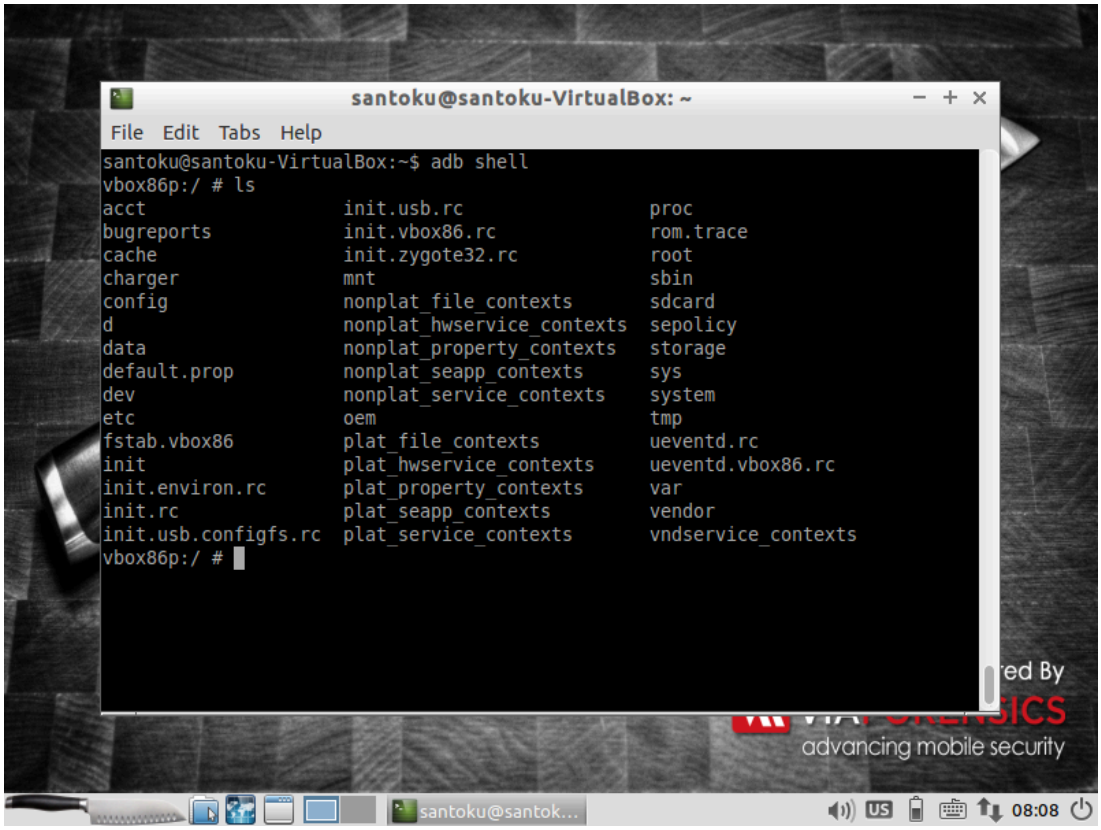
Demonstration of ADB commands

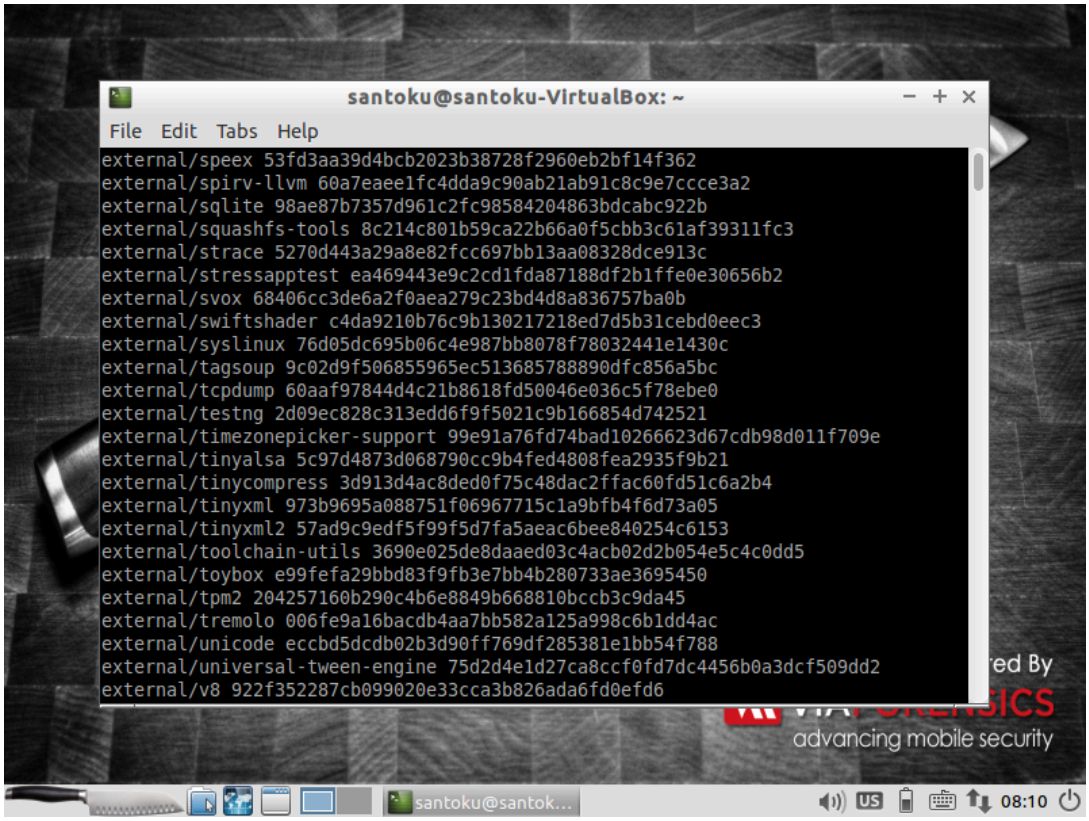


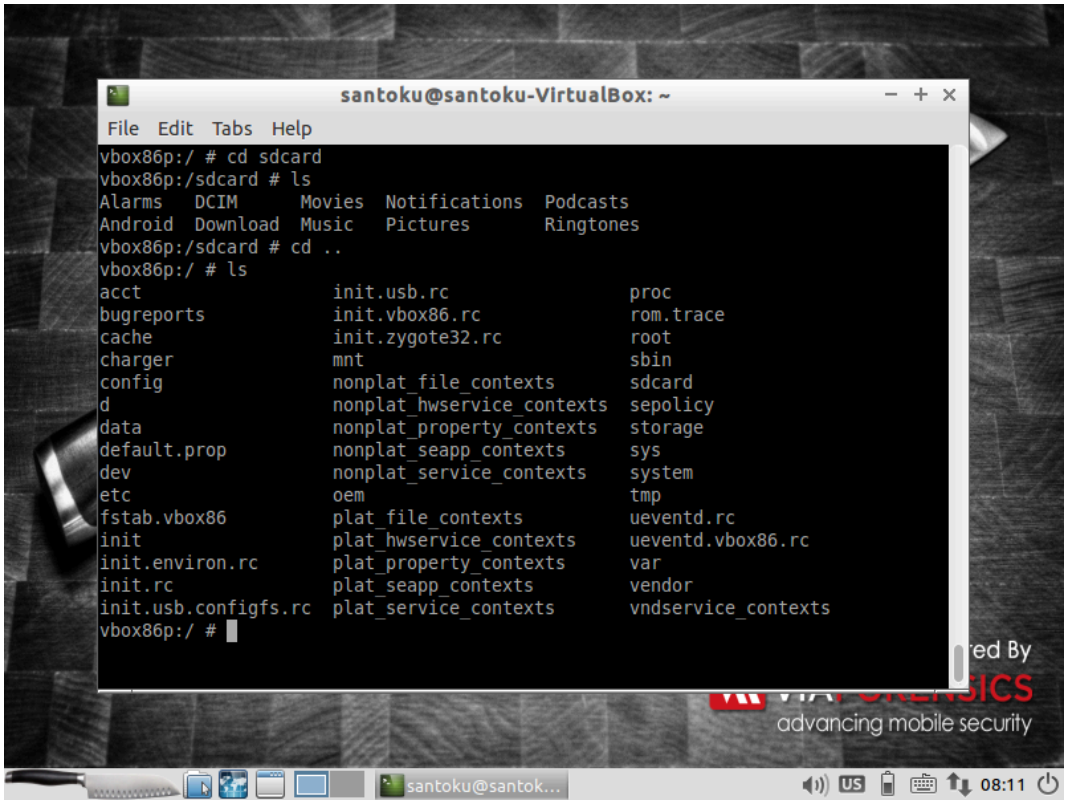


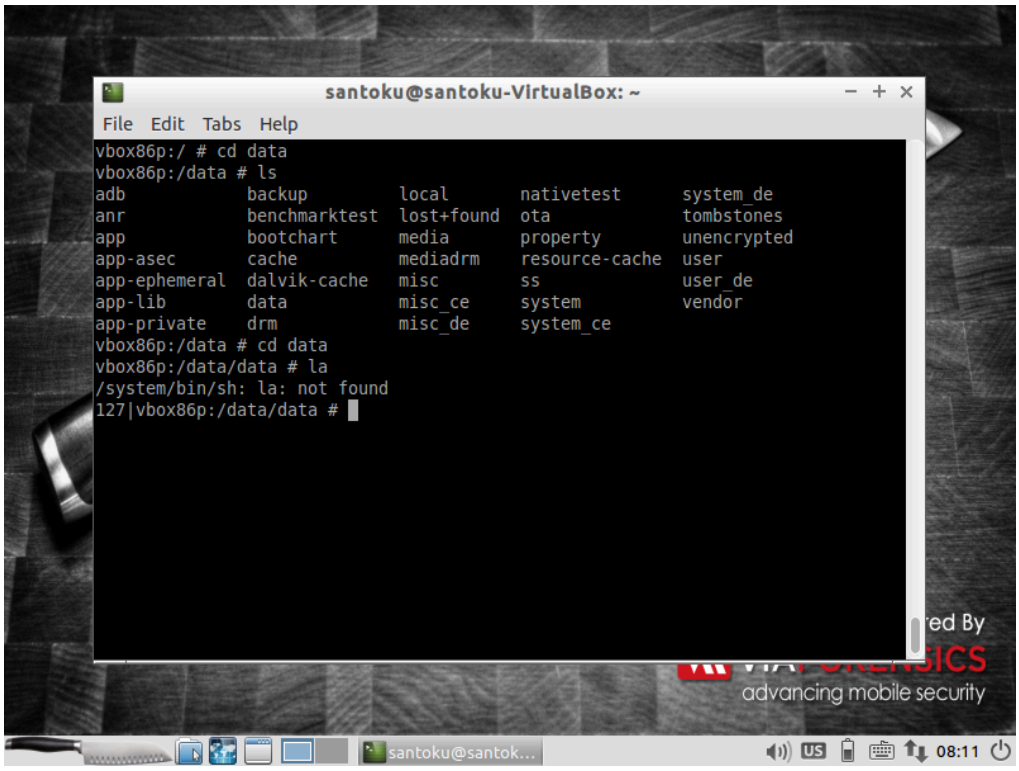

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb kill-server
santoku@santoku-VirtualBox:~$ adb start server
advancing mobile security
santoku@santok...
08:07

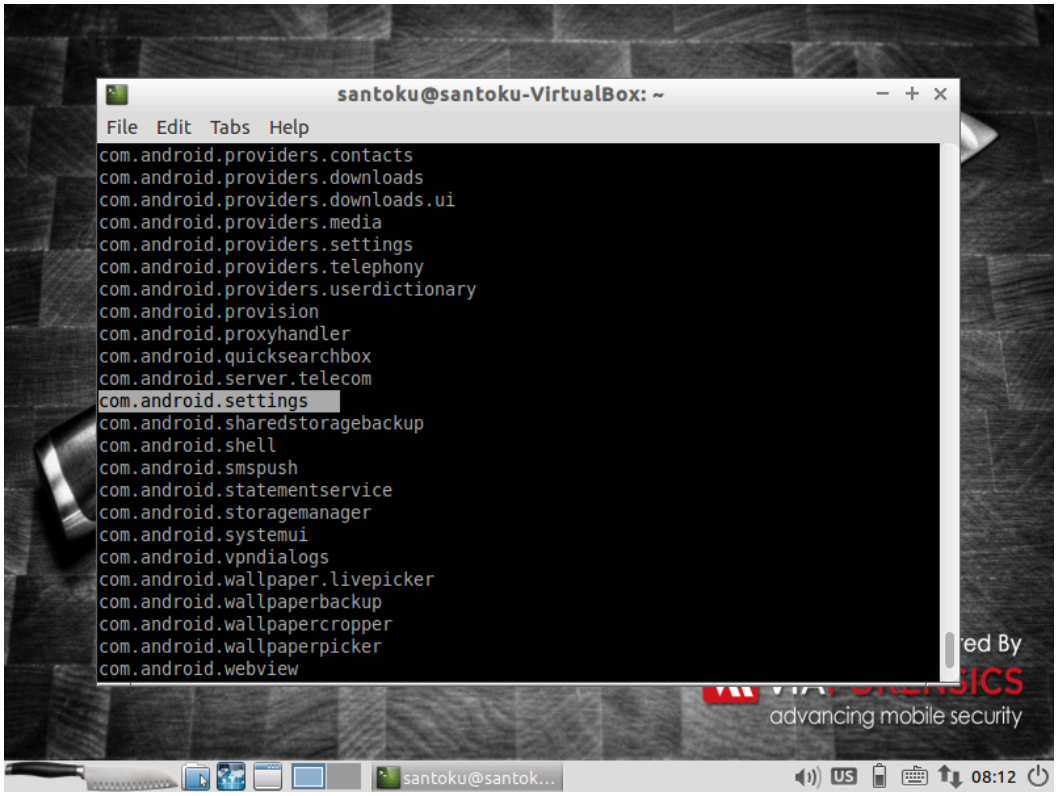

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ #
advancing mobile security
santoku@santok...
08:08

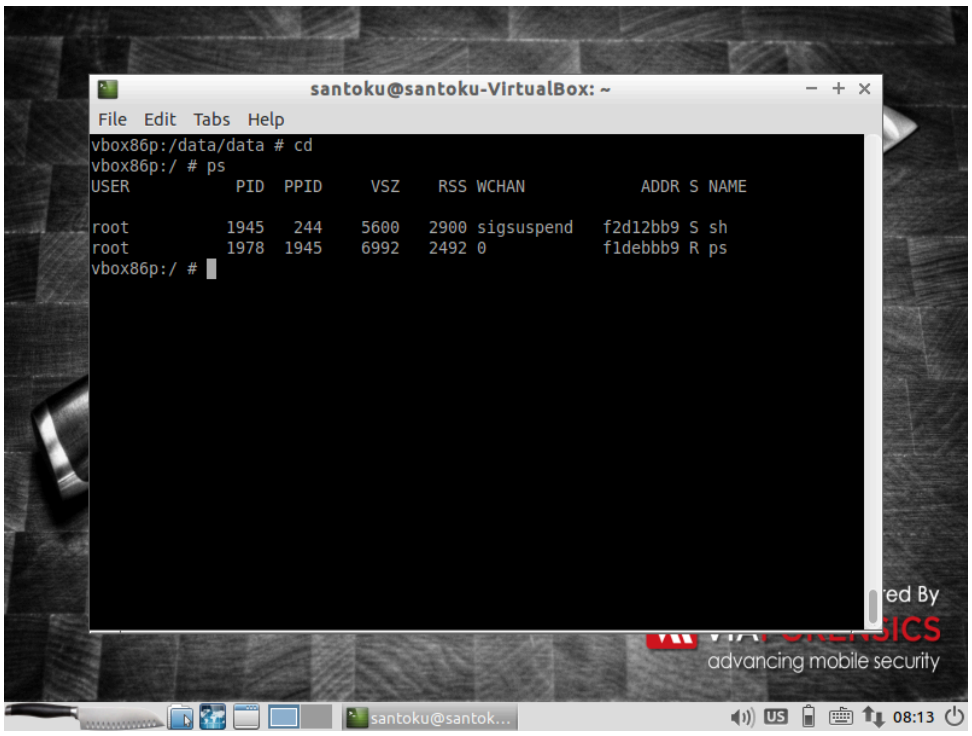

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ # ls
acct
bugreports
cache
charger
config
d
data
default.prop
dev
etc
fstab.vbox86
init
init.environ.rc
init.rc
init.usb.configfs.rc
init.usb.rc
init.vbox86.rc
init.zygote32.rc
mnt
nonplat_file_contexts
nonplat_hwservice_contexts
nonplat_property_contexts
nonplat_seapp_contexts
nonplat_service_contexts
oem
plat_file_contexts
plat_hwservice_contexts
plat_property_contexts
plat_seapp_contexts
plat_service_contexts
proc
rom.trace
root
sbin
sdcard
sepolicy
storage
sys
system
tmp
ueventd.rc
ueventd.vbox86.rc
var
vendor
vndservice_contexts
vbox86p:/ #
advancing mobile security
santoku@santok...
US
08:08

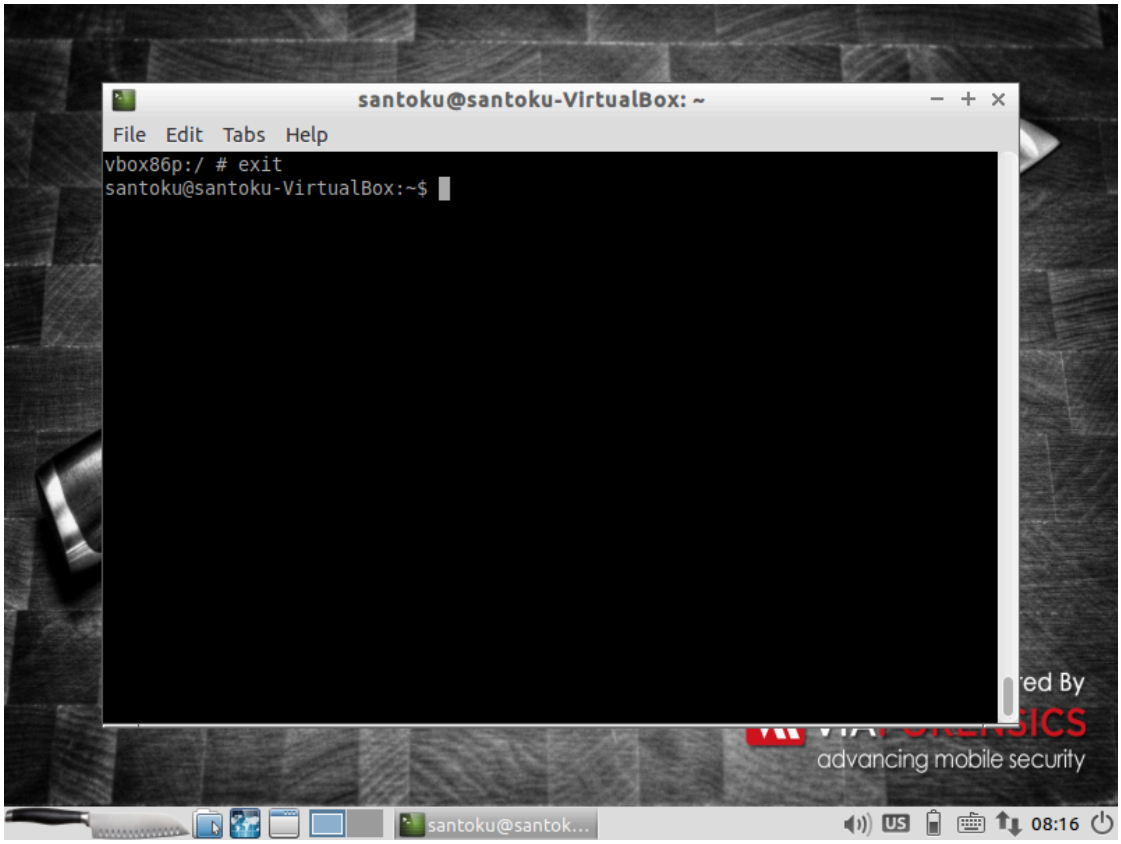

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
external/speex 53fd3aa39d4bcb2023b38728f2960eb2bf14f362
external/spirv-llvm 60a7eaee1fc4dda9c90ab21ab91c8c9e7ccce3a2
external/sqlite 98ae87b7357d961c2fc98584204863bdcabc922b
external/squashfs-tools 8c214c801b59ca22b66a0f5cbb3c61af39311fc3
external/strace 5270d443a29a8e82fcc697bb13aa08328dce913c
external/stressapptest ea469443e9c2cd1fda87188df2b1ffe0e30656b2
external/svox 68406cc3de6a2f0aea279c23bd4d8a836757ba0b
external/swiftshader c4da9210b76c9b130217218ed7d5b31cebd0eec3
external/syslinux 76d05dc695b06c4e987bb8078f78032441e1430c
external/tagsoup 9c02d9f506855965ec513685788890dfc856a5bc
external/tcpdump 60aaf97844d4c21b8618fd50046e036c5f78ebe0
external/testng 2d09ec828c313edd6f9f5021c9b166854d742521
external/timezonepicker-support 99e91a76fd74bad10266623d67cdb98d011f709e
external/tinyalsa 5c97d4873d068790cc9b4fed4808fea2935f9b21
external/tinycompress 3d913d4ac8ded0f75c48dac2ffac60fd51c6a2b4
external/tinyxml 973b9695a088751f06967715c1a9bfb4f6d73a05
external/tinyxml2 57ad9c9edf5f99f5d7fa5aeac6bee840254c6153
external/toolchain-utils 3690e025de8daaed03c4acb02d2b054e5c4c0dd5
external/toybox e99fefa29bbd83f9fb3e7bb4b280733ae3695450
external/tpm2 204257160b290c4b6e8849b668810bccb3c9da45
external/tremolo 006fe9a16bacdb4aa7bb582a125a998c6b1dd4ac
external/unicode eccbd5dcdb02b3d90ff769df285381e1bb54f788
external/universal-tween-engine 75d2d4e1d27ca8ccf0fd7dc4456b0a3dcf509dd2
external/v8 922f352287cb099020e33cca3b826ada6fd0efd6
advancing mobile security
santoku@santok...
US
08:10

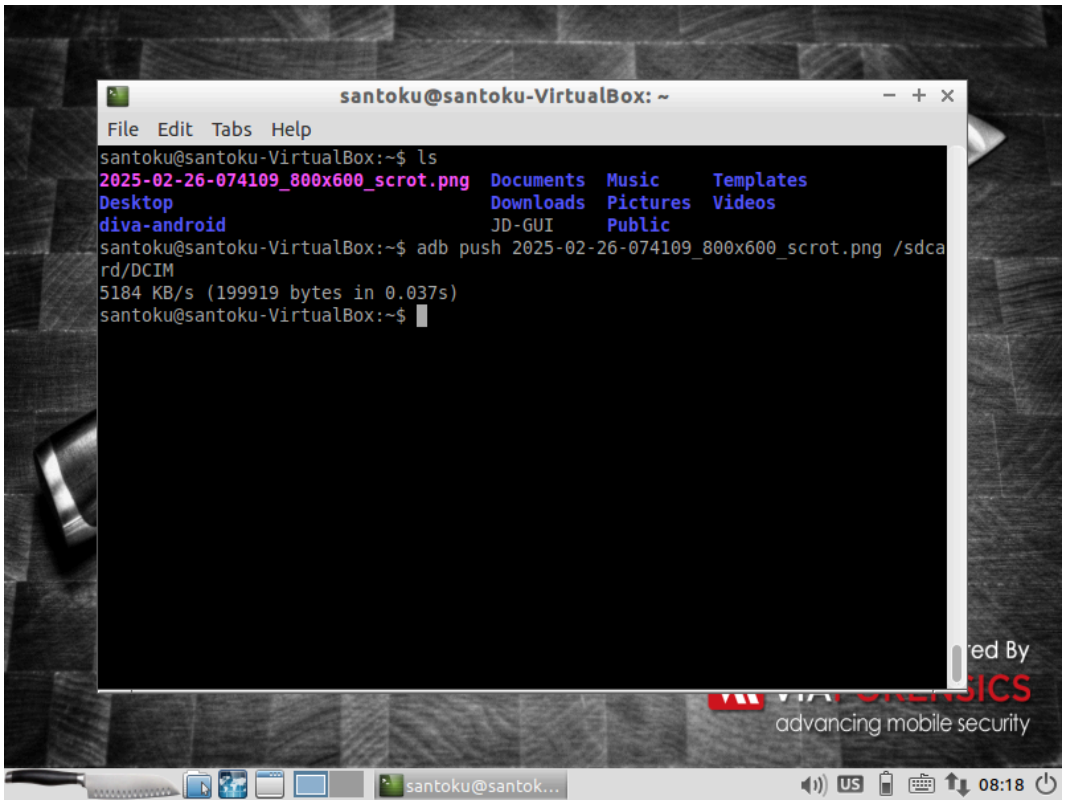

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd sdcard
vbox86p:/sdcard # ls
Alarms DCIM Movies Notifications Podcasts
Android Download Music Pictures Ringtones
vbox86p:/sdcard # cd ..
vbox86p:/ # ls
acct init.usb.rc proc
bugreports init.vbox86.rc rom.trace
cache init.zygote32.rc root
charger mnt sbin
config nonplat_file_contexts sdcard
d nonplat_hwservice_contexts sepolicy
data nonplat_property_contexts storage
default.prop nonplat_seapp_contexts sys
dev nonplat_service_contexts system
etc oem tmp
fstab.vbox86 plat_file_contexts ueventd.rc
init plat_hwservice_contexts ueventd.vbox86.rc
init.environ.rc plat_property_contexts var
init.rc plat_seapp_contexts vendor
init.usb.configfs.rc plat_service_contexts vndservice_contexts
vbox86p:/ #
advancing mobile security
santoku@santok...
08:11

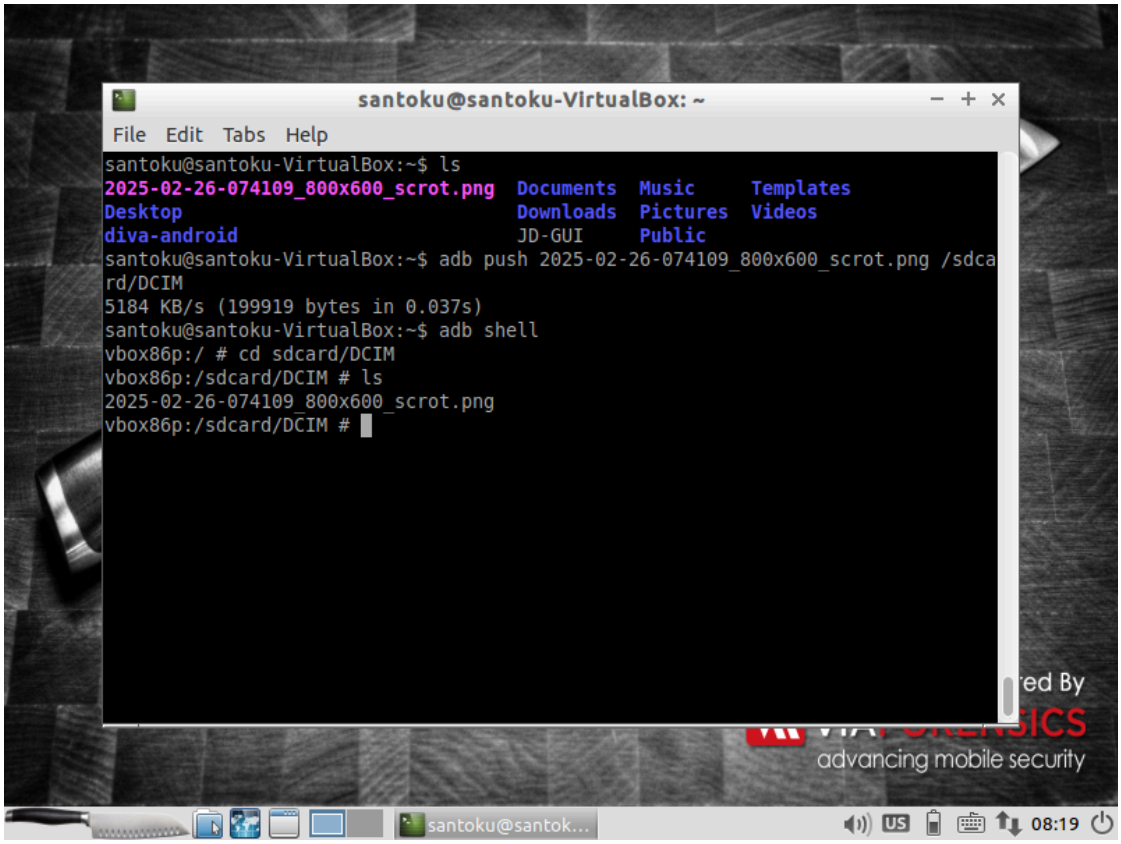

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd data
vbox86p:/data # ls
adb backup local nativetest system_de
anr benchmarktest lost+found ota tombstones
app bootchart media property unencrypted
app-asec cache mediadrm resource-cache user
app-ephemeral dalvik-cache misc ss user_de
app-lib data misc_ce system vendor
app-private drm misc_de system_ce
vbox86p:/data # cd data
vbox86p:/data/data # la
/system/bin/sh: la: not found
127|vbox86p:/data/data #
advancing mobile security
santoku@santok...
08:11

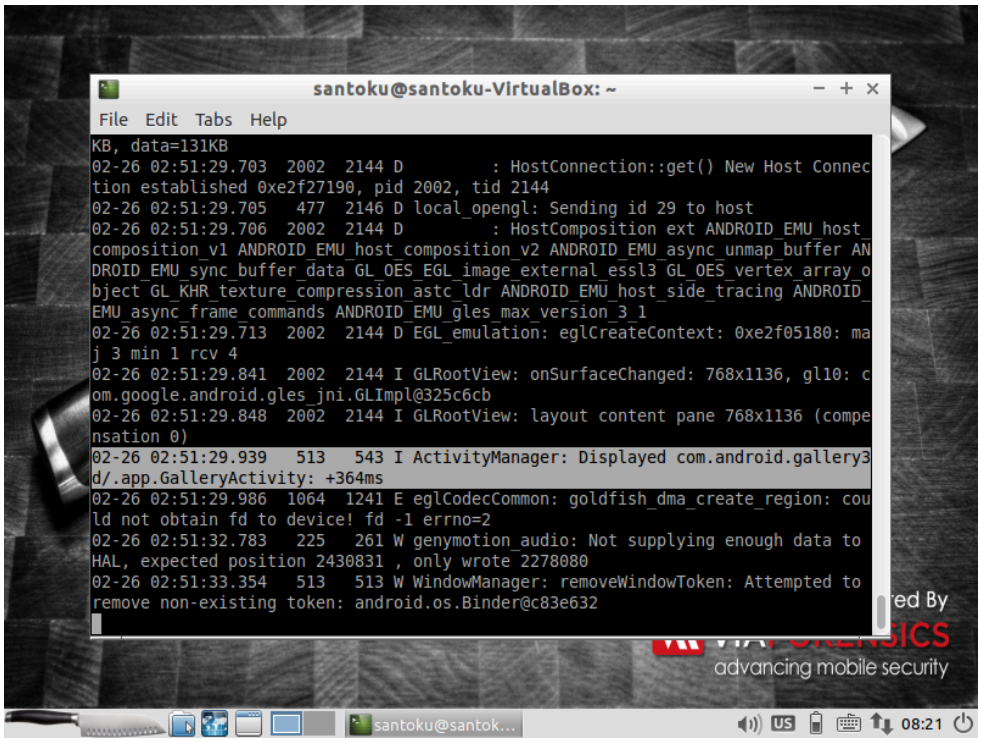

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
com.android.providers.contacts
com.android.providers.downloads
com.android.providers.downloads.ui
com.android.providers.media
com.android.providers.settings
com.android.providers.telephony
com.android.providers.userdictionary
com.android.provision
com.android.proxyhandler
com.android.quicksearchbox
com.android.server.telecom
com.android.settings
com.android.sharedstoragebackup
com.android.shell
com.android.smspush
com.android.statementservice
com.android.storagemanager
com.android.systemui
com.android.vpndialogs
com.android.wallpaper.livepicker
com.android.wallpaperbackup
com.android.wallpapercropper
com.android.wallpaperpicker
com.android.webview
advancing mobile security
santoku@santok...
08:12

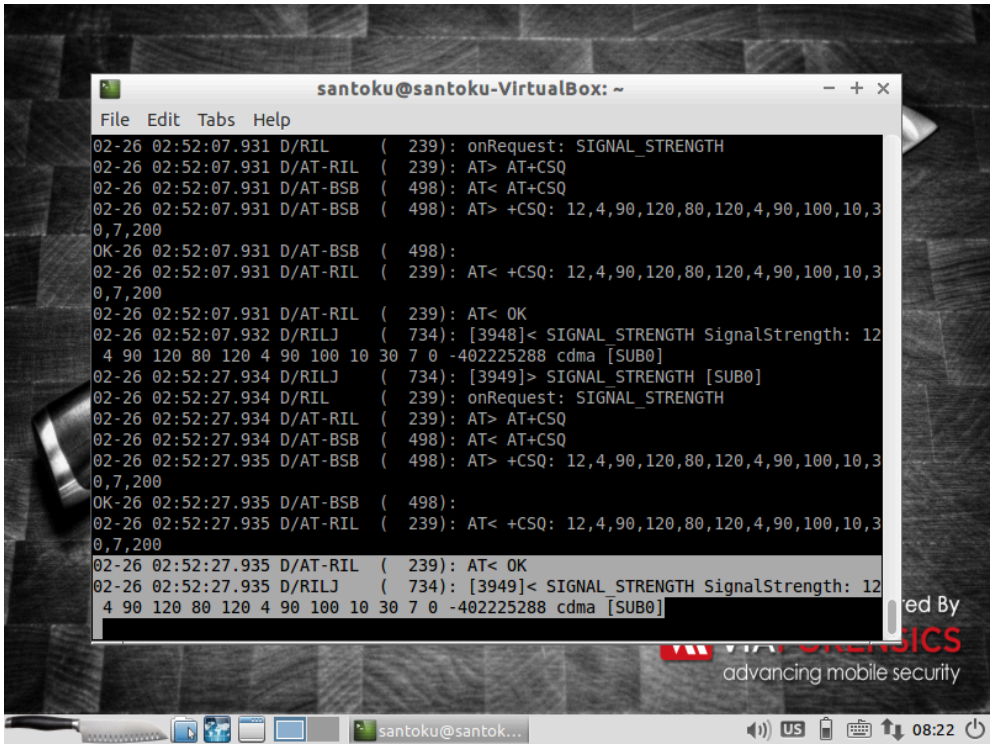

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/data/data # cd
vbox86p:/ # ps
USER PID PPID VSZ RSS WCHAN ADDR S NAME
root 1945 244 5600 2900 sigsuspend f2d12bb9 S sh
root 1978 1945 6992 2492 0 f1debbb9 R ps
vbox86p:/ #
advancing mobile security
santoku@santok...
08:13

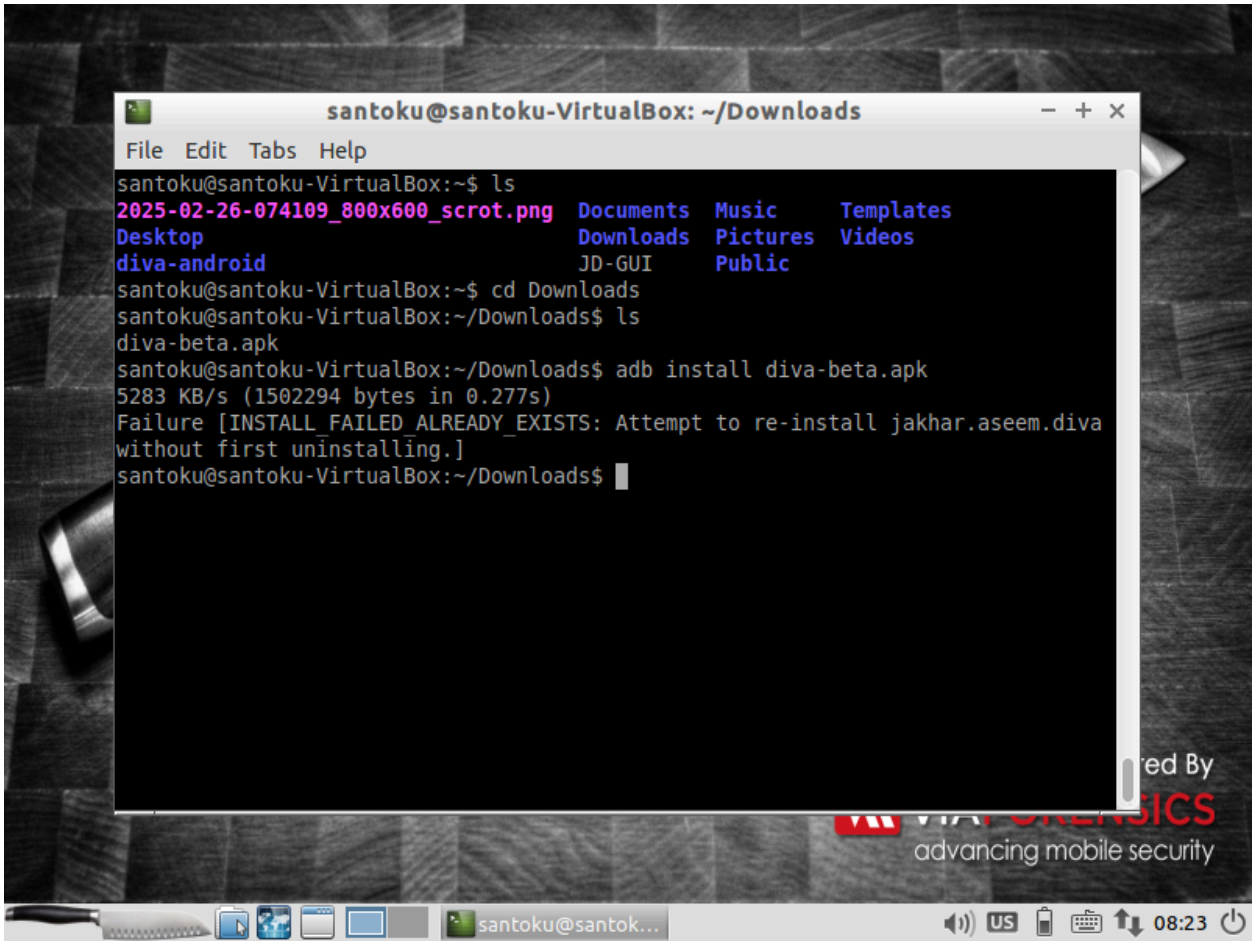

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # exit
santoku@santoku-VirtualBox:~$
advancing mobile security
santoku@santok...
08:16


santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ ls
2025-02-26-074109_800x600_scrot.png Documents Music Templates
Desktop Downloads Pictures Videos
diva-android JD-GUI Public
santoku@santoku-VirtualBox:~$ adb push 2025-02-26-074109_800x600_scrot.png /sdca
rd/DCIM
5184 KB/s (199919 bytes in 0.037s)
santoku@santoku-VirtualBox:~$
advancing mobile security
santoku@santok...
08:18

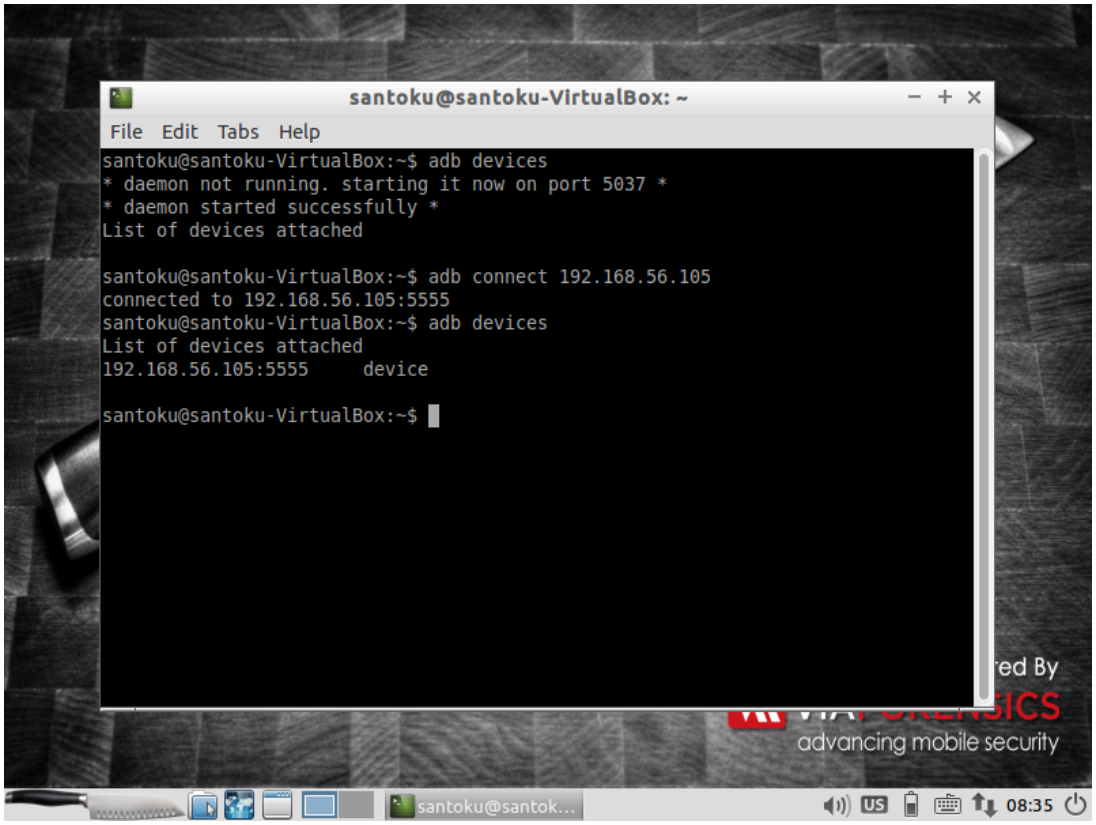

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ ls
2025-02-26-074109_800x600_scrot.png Documents Music Templates
Desktop Downloads Pictures Videos
diva-android JD-GUI Public
santoku@santoku-VirtualBox:~$ adb push 2025-02-26-074109_800x600_scrot.png /sdcard/DCIM
5184 KB/s (199919 bytes in 0.037s)
santoku@santoku-VirtualBox:~$ adb shell
vbox86p:/ # cd sdcard/DCIM
vbox86p:/sdcard/DCIM # ls
2025-02-26-074109_800x600_scrot.png
vbox86p:/sdcard/DCIM #
advancing mobile security
santoku@santok...
08:19

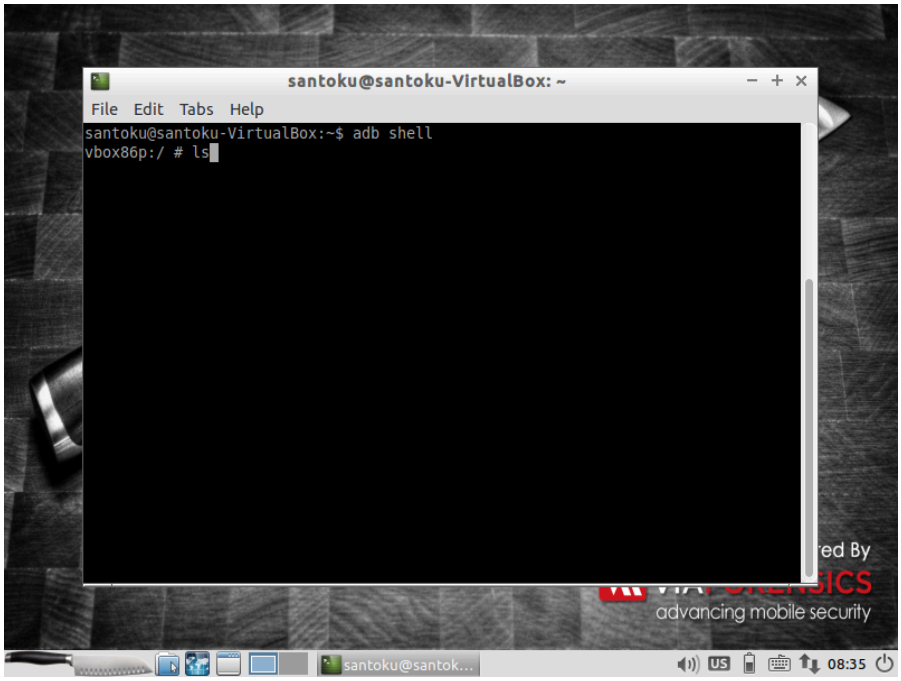

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
KB, data=131KB
02-26 02:51:29.703 2002 2144 D : HostConnection::get() New Host Connection established 0xe2f27190, pid 2002, tid 2144
02-26 02:51:29.705 477 2146 D local_opengl: Sending id 29 to host
02-26 02:51:29.706 2002 2144 D : HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_async_unmap_buffer ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_async_frame_commands ANDROID_EMU_gles_max_version_3_1
02-26 02:51:29.713 2002 2144 D EGL_emulation: eglCreateContext: 0xe2f05180: maj 3 min 1 rcv 4
02-26 02:51:29.841 2002 2144 I GLRootView: onSurfaceChanged: 768x1136, gl10: com.google.android.gles_jni.GLImpl@325c6cb
02-26 02:51:29.848 2002 2144 I GLRootView: layout content pane 768x1136 (compensation 0)
02-26 02:51:29.939 513 543 I ActivityManager: Displayed com.android.gallery3d/.app.GalleryActivity: +364ms
02-26 02:51:29.986 1064 1241 E eglCodecCommon: goldfish_dma_create_region: could not obtain fd to device! fd -1 errno=2
02-26 02:51:32.783 225 261 W genymotion_audio: Not supplying enough data to HAL, expected position 2430831 , only wrote 2278080
02-26 02:51:33.354 513 513 W WindowManager: removeWindowToken: Attempted to remove non-existing token: android.os.Binder@c83e632
advancing mobile security
santoku@santok...
08:21

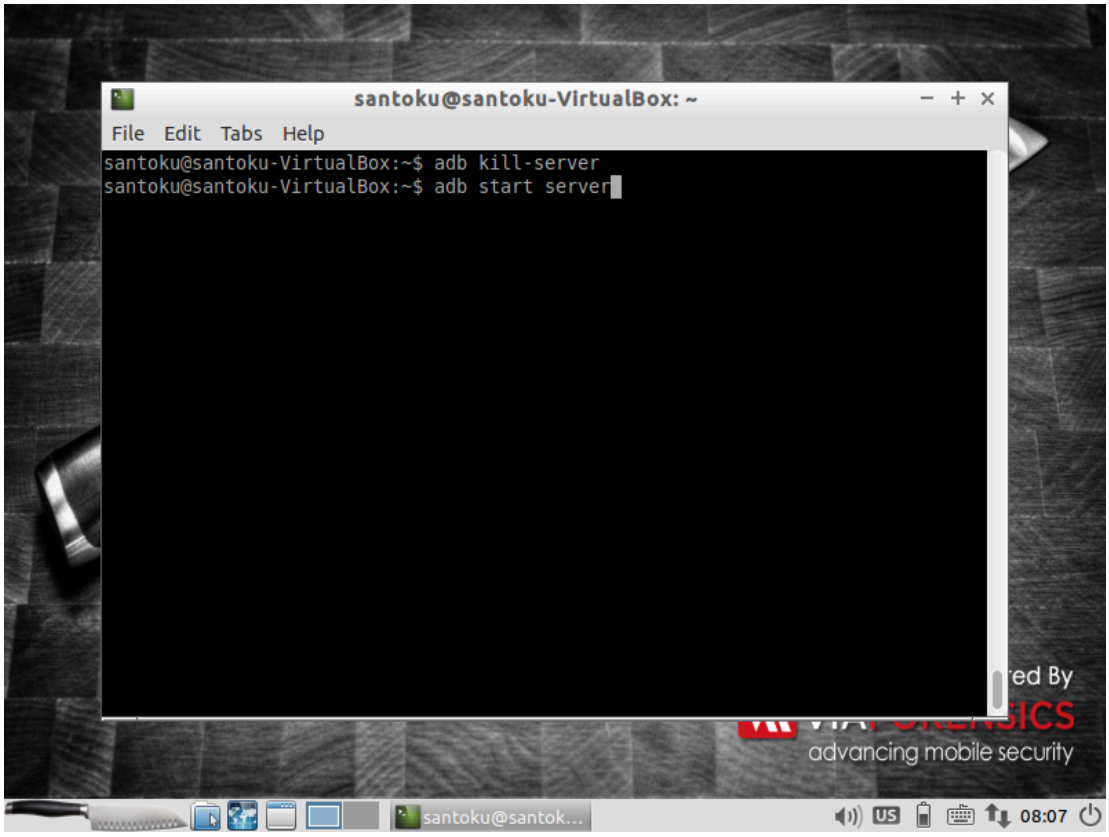

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
02-26 02:52:07.931 D/RIL (239): onRequest: SIGNAL_STRENGTH
02-26 02:52:07.931 D/AT-RIL (239): AT> AT+CSQ
02-26 02:52:07.931 D/AT-BSB (498): AT< AT+CSQ
02-26 02:52:07.931 D/AT-BSB (498): AT> +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
OK-26 02:52:07.931 D/AT-BSB (498):
02-26 02:52:07.931 D/AT-RIL (239): AT< +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
02-26 02:52:07.931 D/AT-RIL (239): AT< OK
02-26 02:52:07.932 D/RILJ (734): [3948]< SIGNAL_STRENGTH SignalStrength: 12
4 90 120 80 120 4 90 100 10 30 7 0 -402225288 cdma [SUB0]
02-26 02:52:27.934 D/RILJ (734): [3949]> SIGNAL_STRENGTH [SUB0]
02-26 02:52:27.934 D/RIL (239): onRequest: SIGNAL_STRENGTH
02-26 02:52:27.934 D/AT-RIL (239): AT> AT+CSQ
02-26 02:52:27.934 D/AT-BSB (498): AT< AT+CSQ
02-26 02:52:27.935 D/AT-BSB (498): AT> +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
OK-26 02:52:27.935 D/AT-BSB (498):
02-26 02:52:27.935 D/AT-RIL (239): AT< +CSQ: 12,4,90,120,80,120,4,90,100,10,3
0,7,200
02-26 02:52:27.935 D/AT-RIL (239): AT< OK
02-26 02:52:27.935 D/RILJ (734): [3949]< SIGNAL_STRENGTH SignalStrength: 12
4 90 120 80 120 4 90 100 10 30 7 0 -402225288 cdma [SUB0]
ed By
advancing mobile security
santoku@santok...
08:22

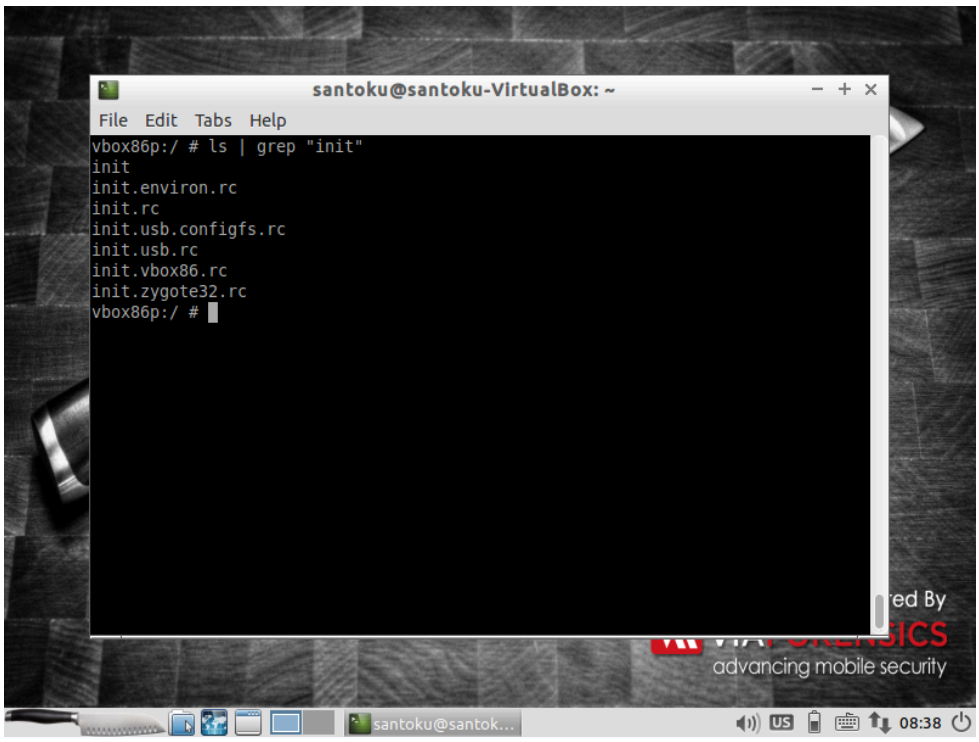

santoku@santoku-VirtualBox: ~/Downloads
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ ls
2025-02-26-074109_800x600_scrot.png Documents Music Templates
Desktop Downloads Pictures Videos
diva-android JD-GUI Public
santoku@santoku-VirtualBox:~$ cd Downloads
santoku@santoku-VirtualBox:~/Downloads$ ls
diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ adb install diva-beta.apk
5283 KB/s (1502294 bytes in 0.277s)
Failure [INSTALL_FAILED_ALREADY_EXISTS: Attempt to re-install jakhar.aseem.diva
without first uninstalling.]
santoku@santoku-VirtualBox:~/Downloads$
ed By
advancing mobile security
santoku@santok...
08:23

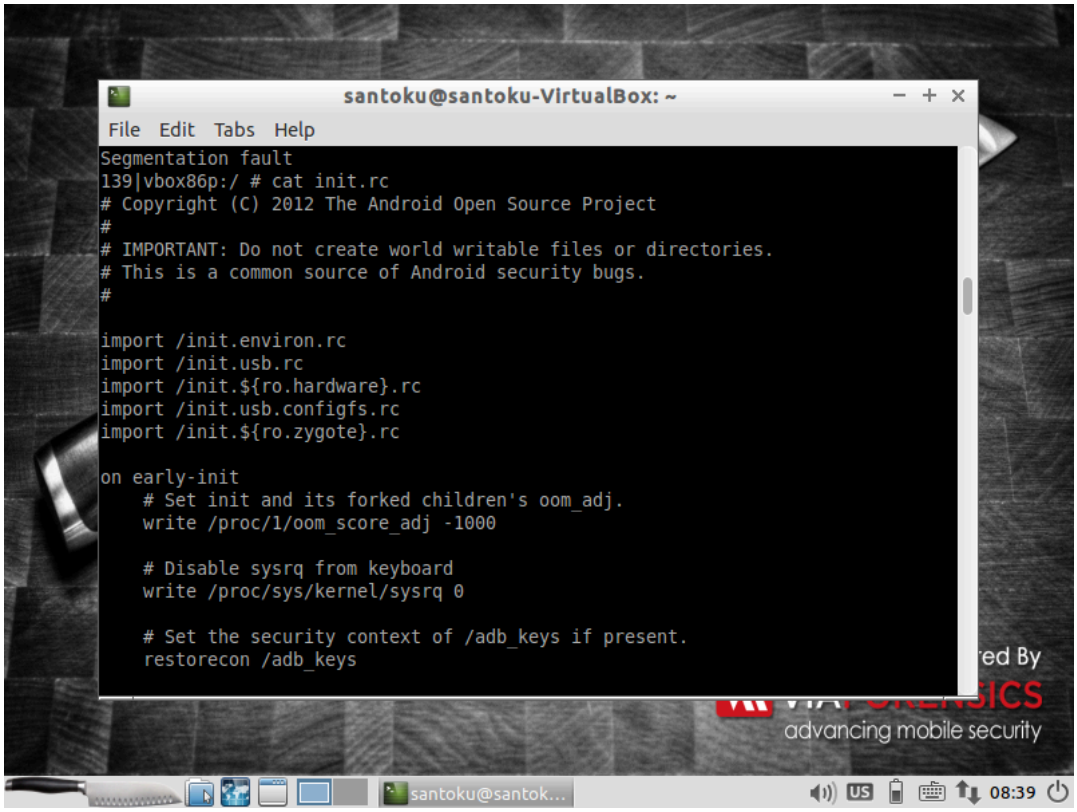
Demonstration of Android Boot Process using ADB

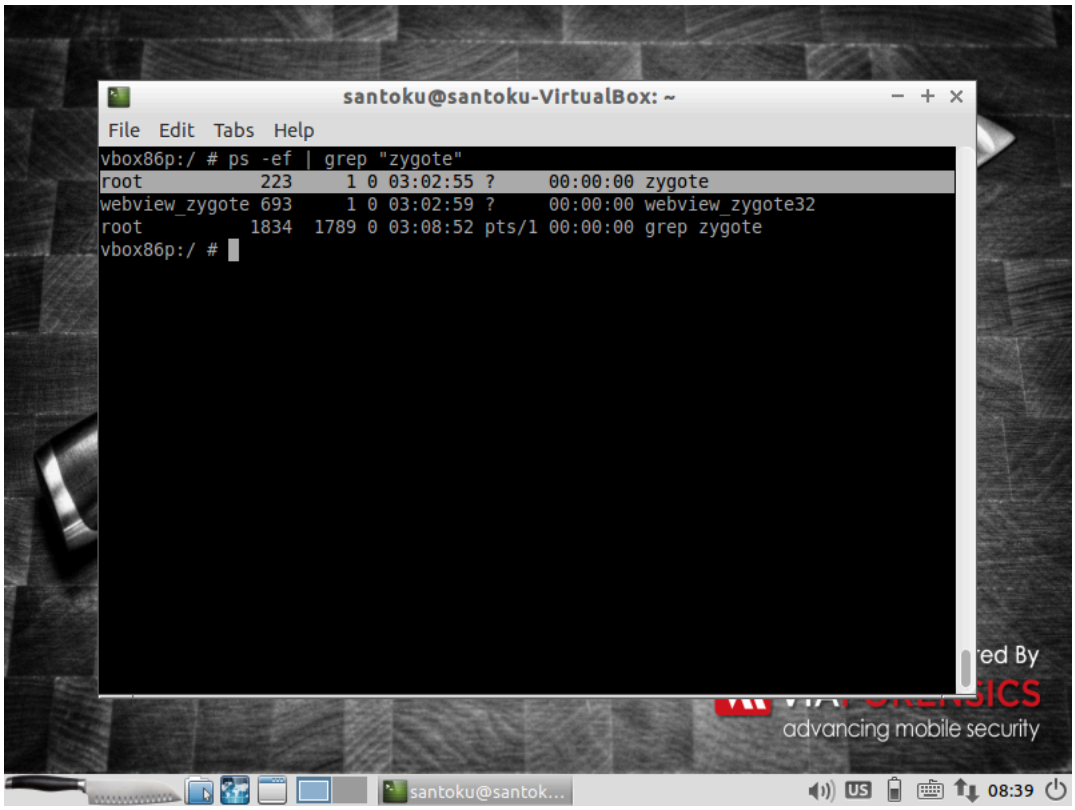




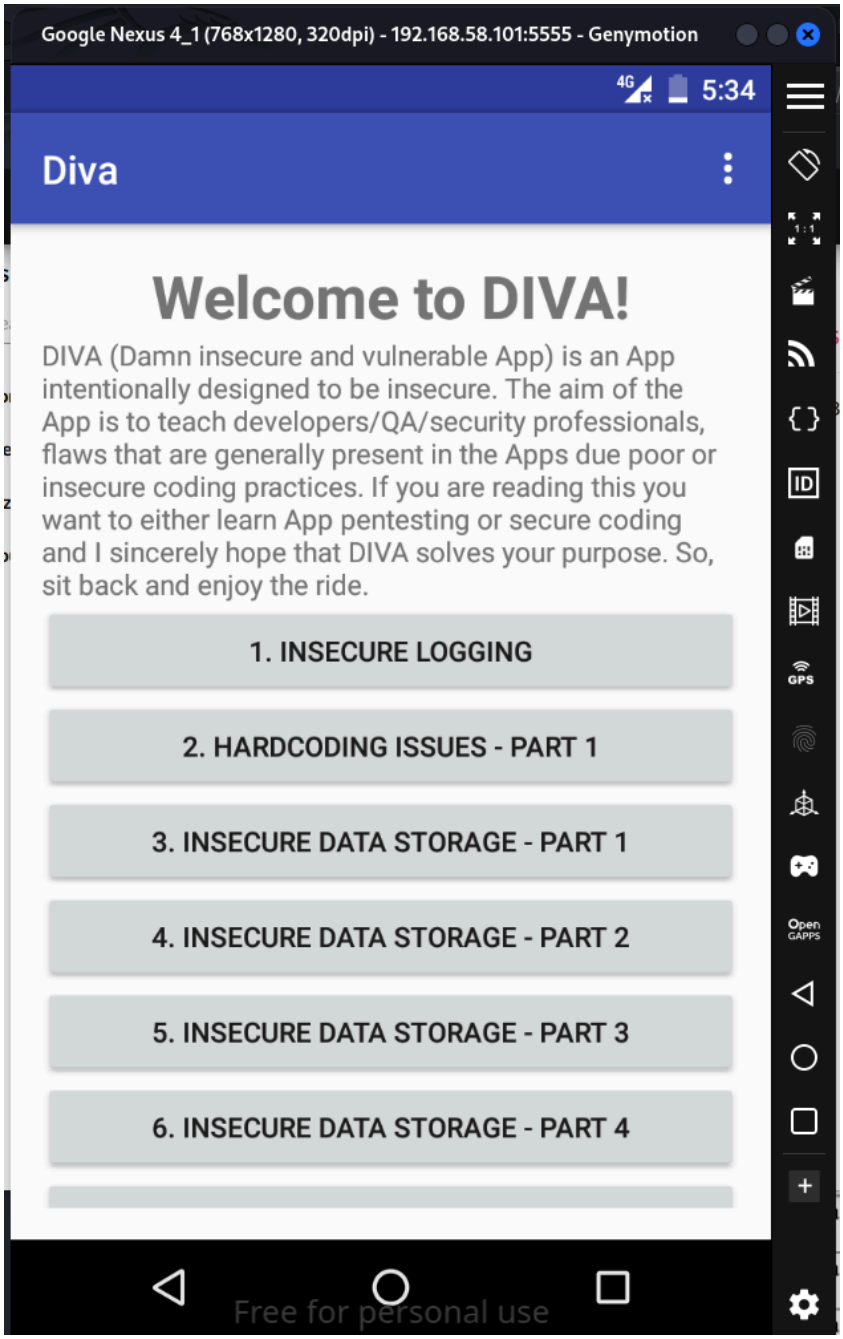

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
santoku@santoku-VirtualBox:~$ adb kill-server
santoku@santoku-VirtualBox:~$ adb start server
advancing mobile security
santoku@santok...
US
08:07


santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # ls | grep "init"
init
init.environ.rc
init.rc
init.usb.configfs.rc
init.usb.rc
init.vbox86.rc
init.zygote32.rc
vbox86p:/ #
advancing mobile security
santoku@santok...
US
08:38

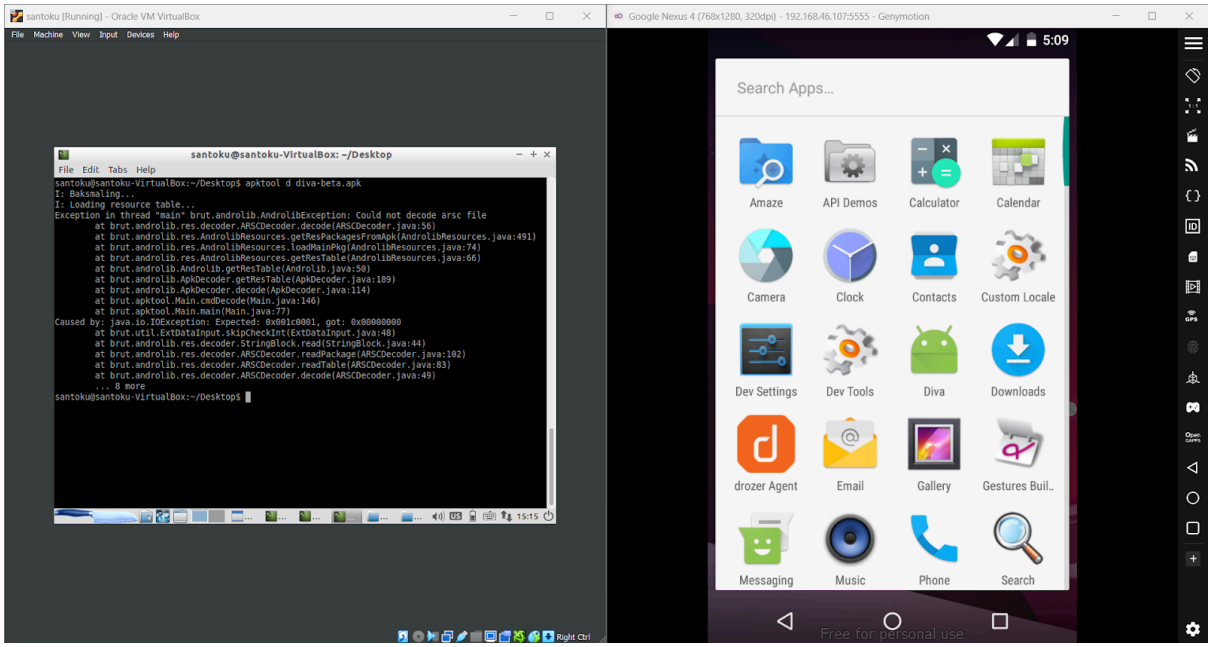

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
Segmentation fault
139|vbox86p:/ # cat init.rc
Copyright (C) 2012 The Android Open Source Project
#
IMPORTANT: Do not create world writable files or directories.
This is a common source of Android security bugs.
#
import /init.environ.rc
import /init.usb.rc
import /init.${ro.hardware}.rc
import /init.usb.configfs.rc
import /init.${ro.zygote}.rc
on early-init
Set init and its forked children's oom_adj.
write /proc/1/oom_score_adj -1000
Disable sysrq from keyboard
write /proc/sys/kernel/sysrq 0
Set the security context of /adb_keys if present.
restorecon /adb_keys
advancing mobile security
08:39

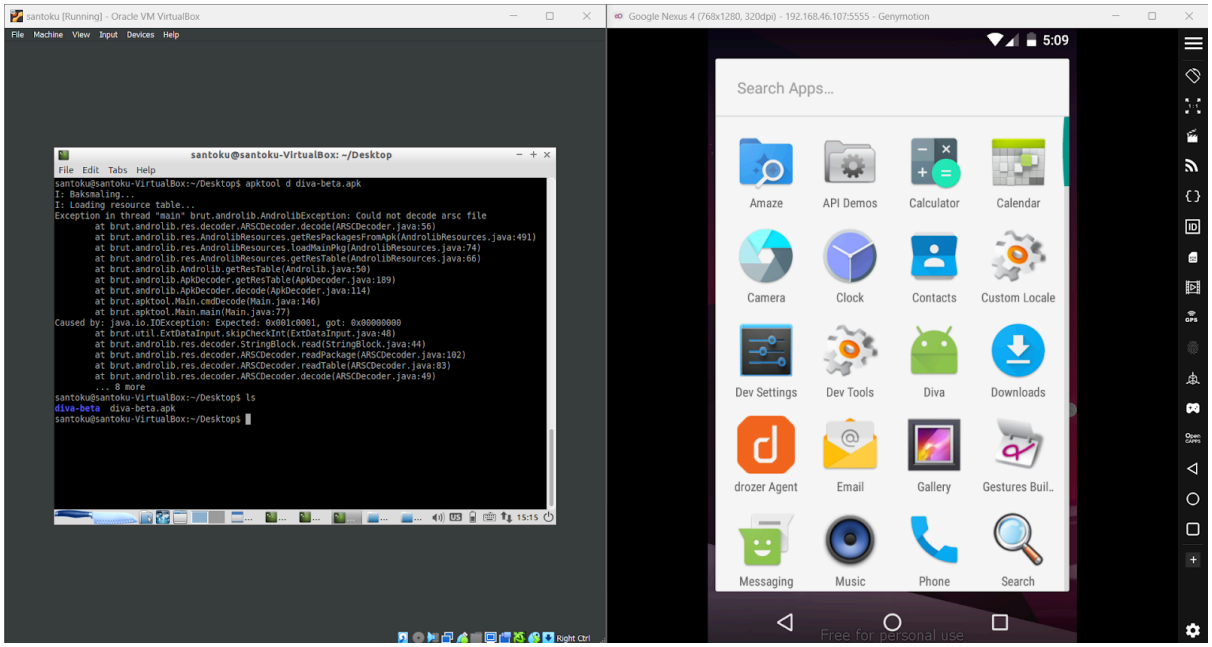

santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # ps -ef | grep "zygote"
root 223 1 0 03:02:55 ? 00:00:00 zygote
webview_zygote 693 1 0 03:02:59 ? 00:00:00 webview_zygote32
root 1834 1789 0 03:08:52 pts/1 00:00:00 grep zygote
vbox86p:/ #
advancing mobile security
08:39

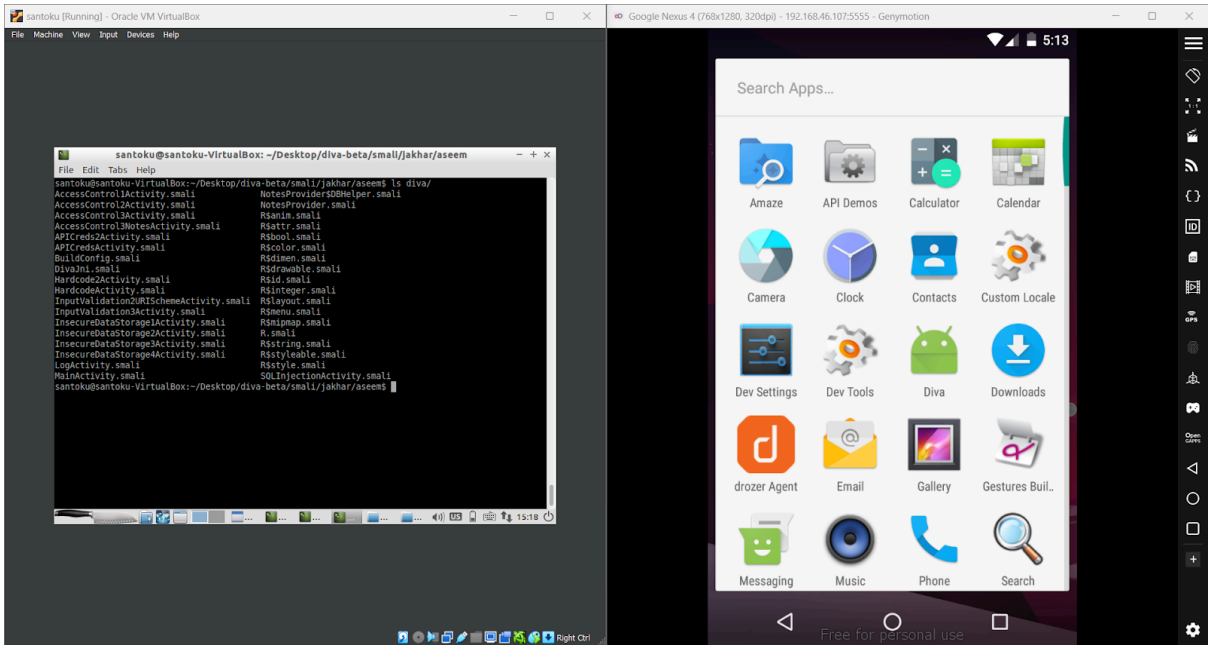
Configuration of DIVA



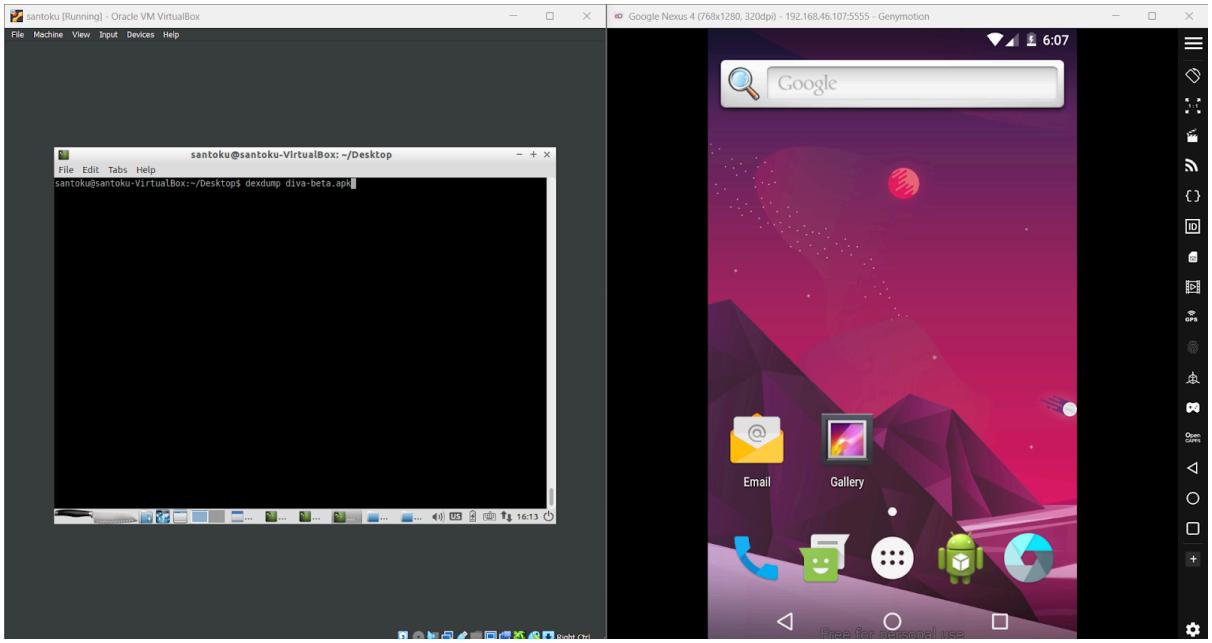
Reverse Engineering using APKTools

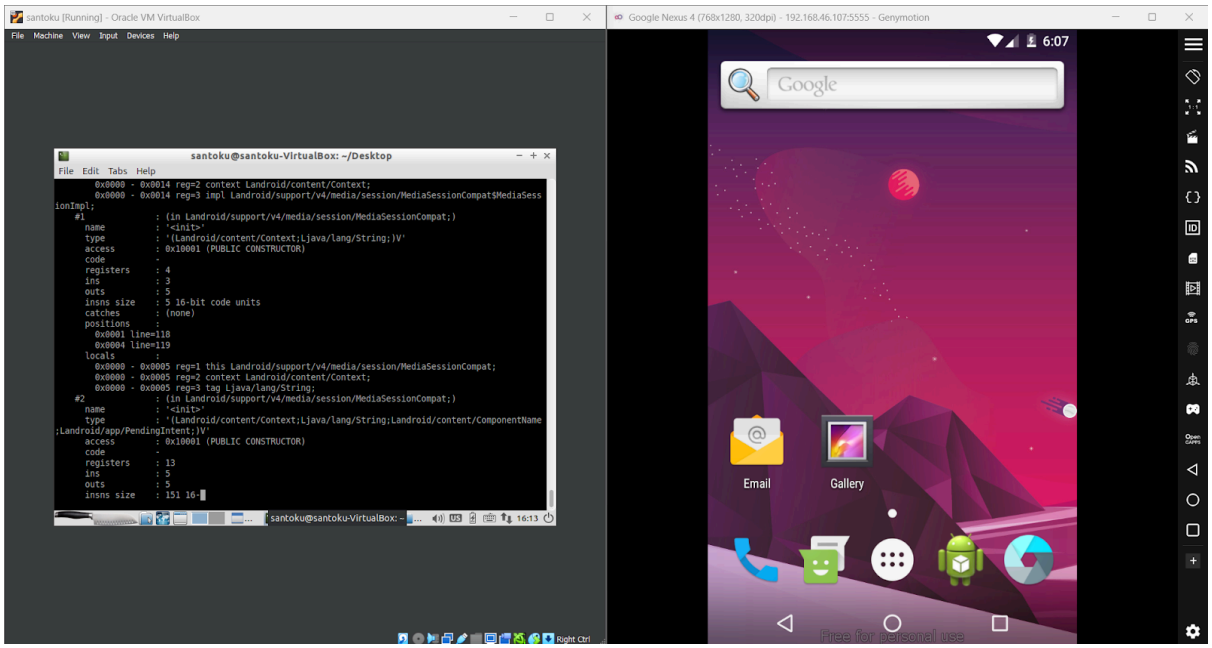


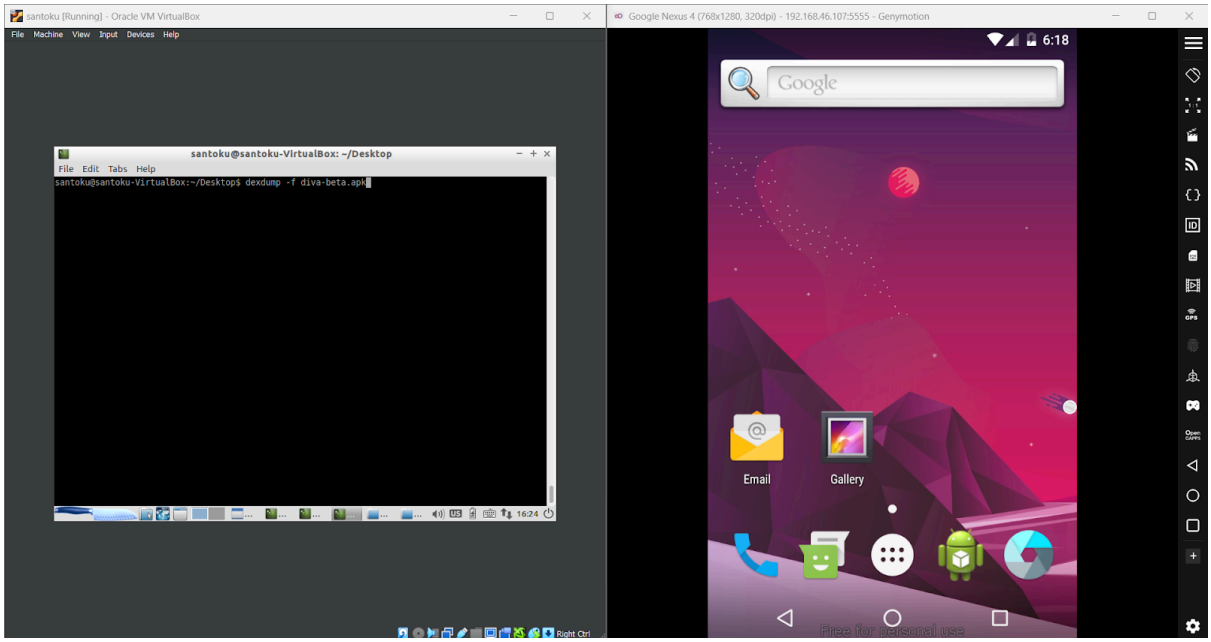


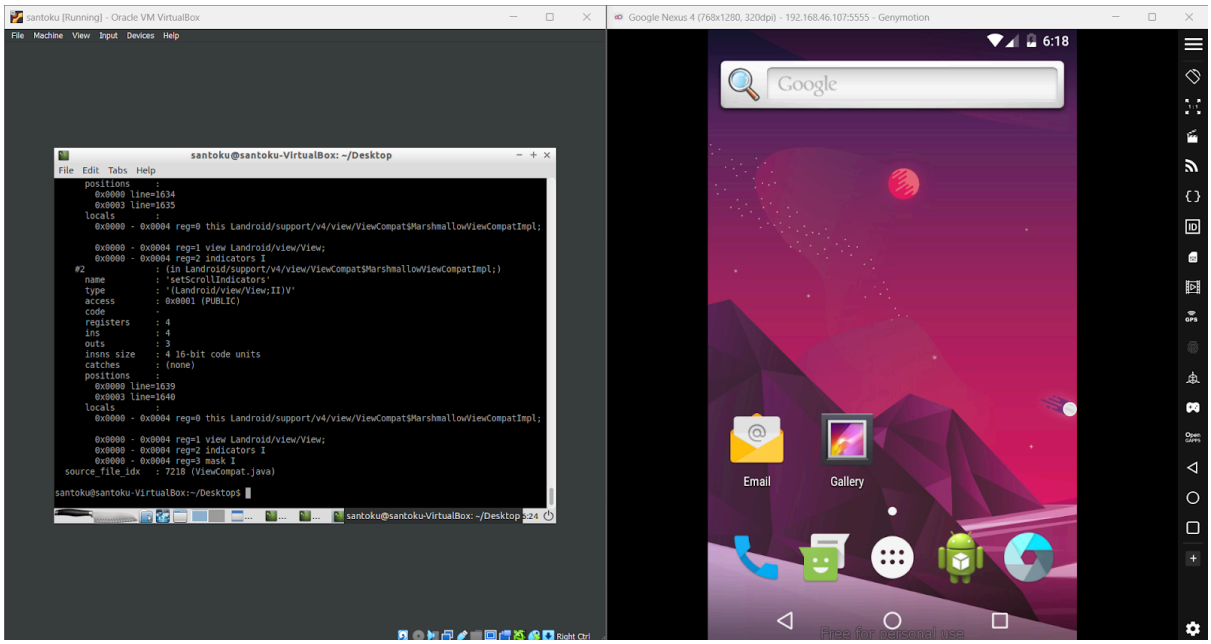

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop/diva-beta/small/jakhar/aseem
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Desktop/diva-beta/smali/jakhar/aseem$ ls diva/
AccessControl1Activity.smali
AccessControl2Activity.smali
AccessControl3Activity.smali
AccessControl3NotesActivity.smali
APICreds2Activity.smali
APICredsActivity.smali
BuildConfig.smali
DivaJni.smali
Hardcode2Activity.smali
HardcodeActivity.smali
InputValidation2URISchemeActivity.smali
InputValidation3Activity.smali
InsecureDataStorage1Activity.smali
InsecureDataStorage2Activity.smali
InsecureDataStorage3Activity.smali
InsecureDataStorage4Activity.smali
LogActivity.smali
MainActivity.smali
NotesProvider$DBHelper.smali
NotesProvider.smali
R$anim.smali
R$attr.smali
R$bool.smali
R$color.smali
R$dimen.smali
R$drawable.smali
R$id.smali
R$integer.smali
R$layout.smali
R$menu.smali
R$mipmap.smali
R.smali
R$string.smali
R$styleable.smali
R$style.smali
SQLInjectionActivity.smali
santoku@santoku-VirtualBox:~/Desktop/diva-beta/smali/jakhar/aseem$
15:18
Right Ctrl
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
5:13
Search Apps...
Amaze
API Demos
Calculator
Calendar
Camera
Clock
Contacts
Custom Locale
Dev Settings
Dev Tools
Diva
Downloads
drozer Agent
Email
Gallery
Gestures Buil..
Messaging
Music
Phone
Search
Free for personal use

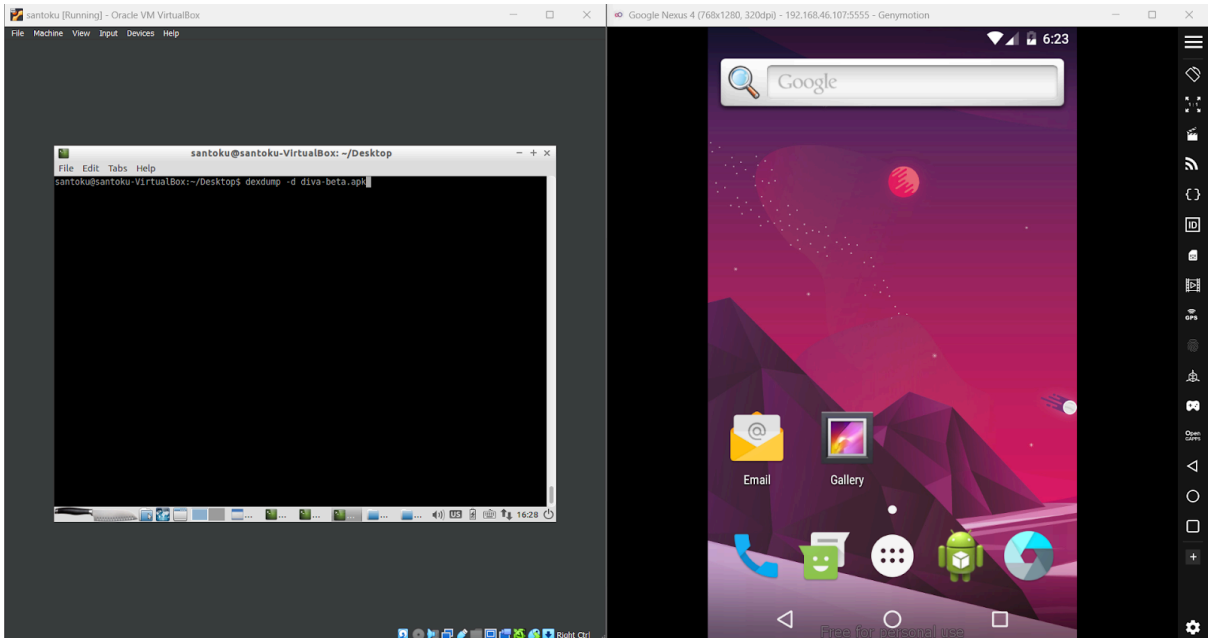
Reverse Engineering using Haxdump Dex Dump and d2j

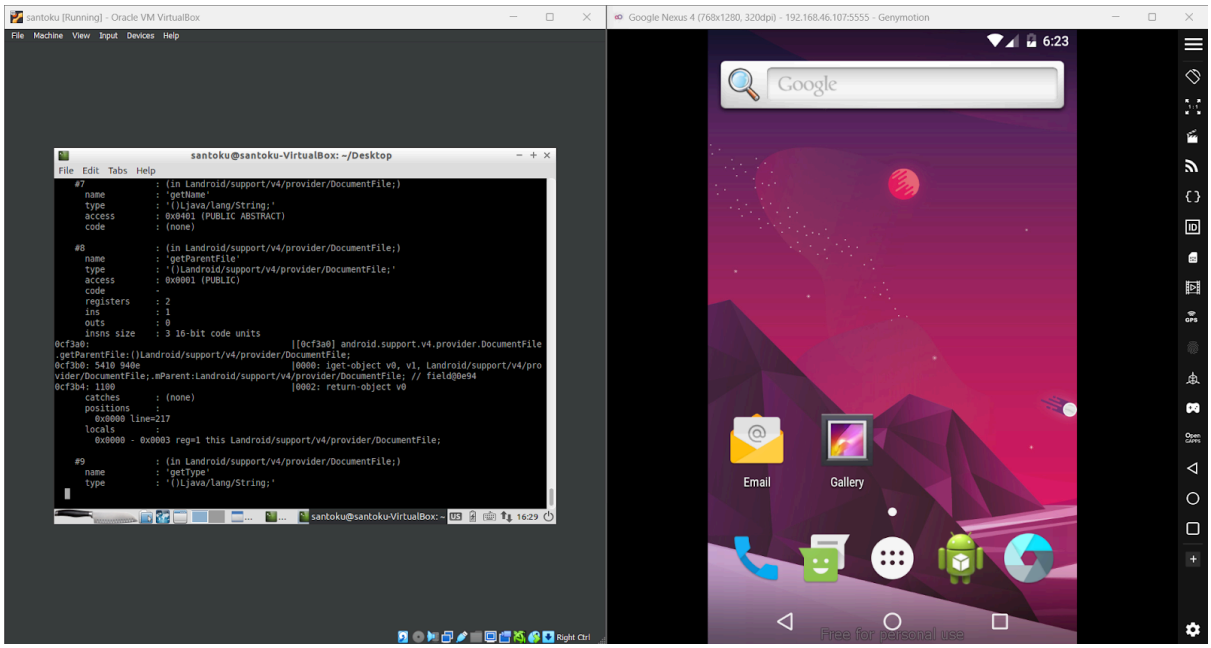




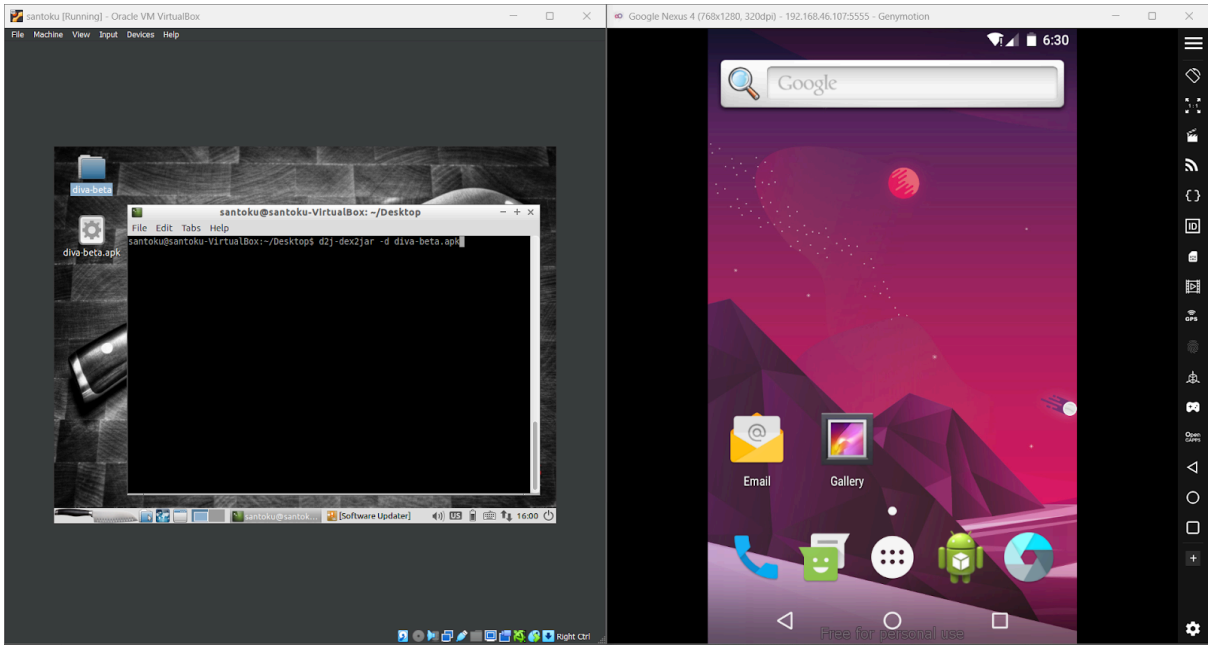

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Desktop$ dexdump -f diva-beta.apk
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:18
Google
Email
Gallery
Free for personal use

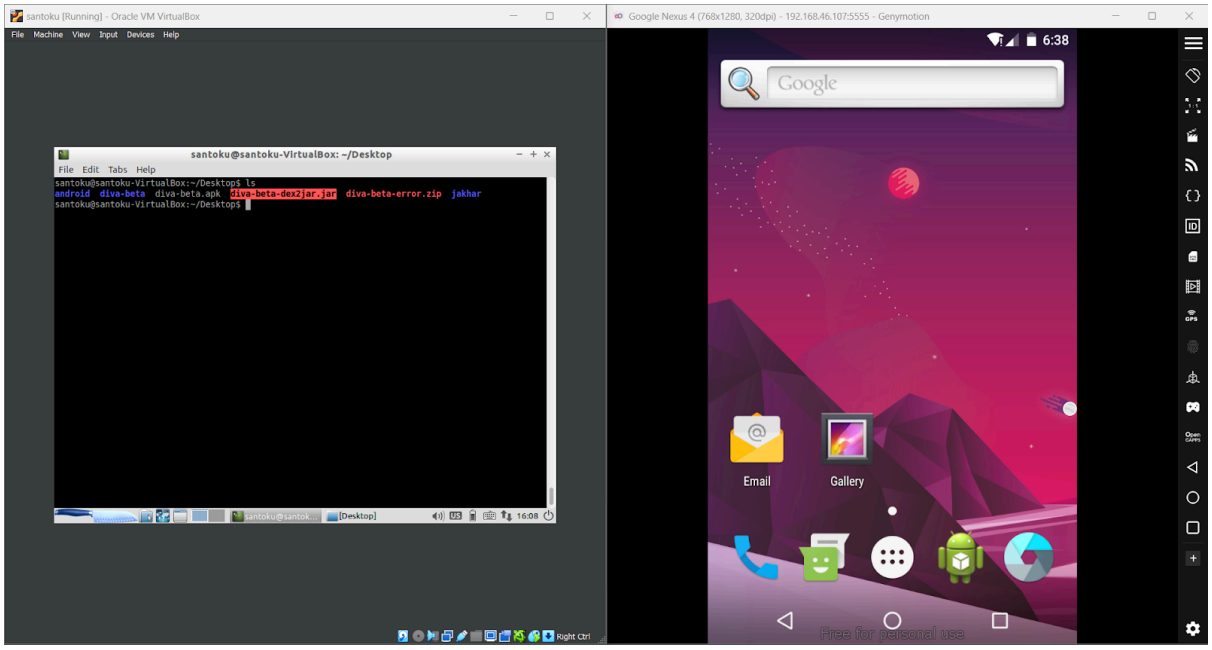

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop
File Edit Tabs Help
positions : 0x0000 line=1634 0x0003 line=1635
locals : 0x0000 - 0x0004 reg=0 this Landroid/support/v4/view/ViewCompat$MarshmallowViewCompatImpl;
0x0000 - 0x0004 reg=1 view Landroid/view/View;
0x0000 - 0x0004 reg=2 indicators I
#2 : (in Landroid/support/v4/view/ViewCompat$MarshmallowViewCompatImpl;)
name : 'setScrollIndicators'
type : '(Landroid/view/View;II)V'
access : 0x0001 (PUBLIC)
code -
registers : 4
ins : 4
outs : 3
insns size : 4 16-bit code units
catches : (none)
positions : 0x0000 line=1639 0x0003 line=1640
locals : 0x0000 - 0x0004 reg=0 this Landroid/support/v4/view/ViewCompat$MarshmallowViewCompatImpl;
0x0000 - 0x0004 reg=1 view Landroid/view/View;
0x0000 - 0x0004 reg=2 indicators I
0x0000 - 0x0004 reg=3 mask I
source_file_idx : 7218 (ViewCompat.java)
santoku@santoku-VirtualBox:~/Desktop$
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:18
Google
Email
Gallery
Free for personal use

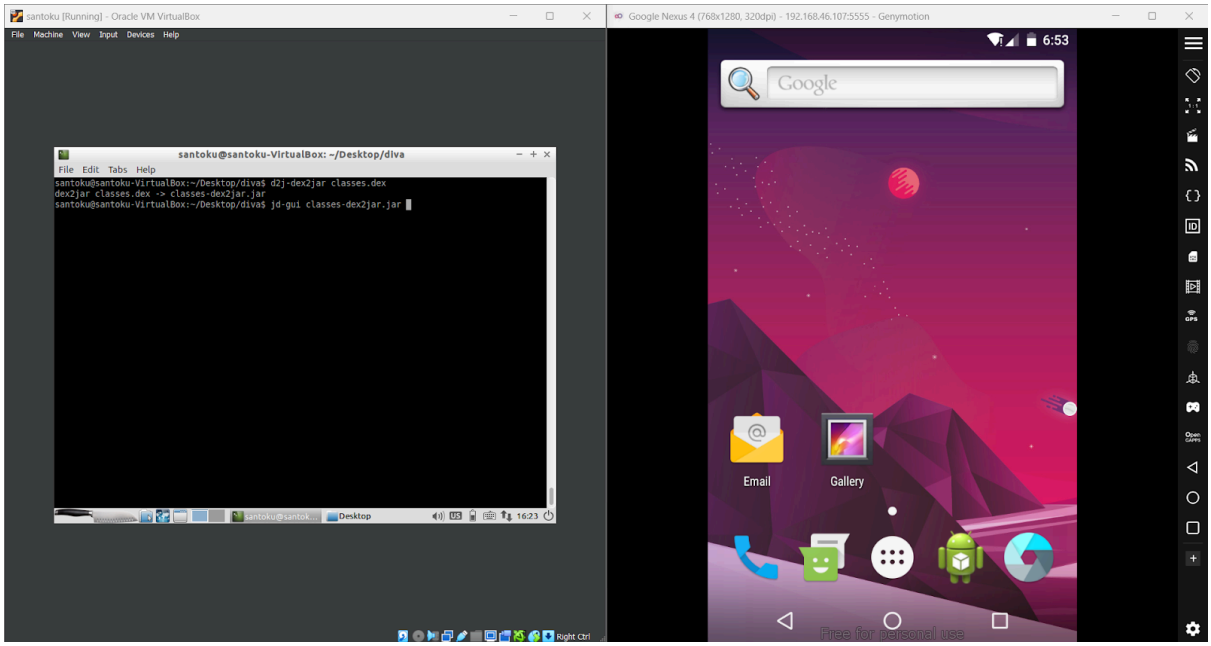

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Desktop$ dexdump -d diva-beta.apk
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:23
Google
Email
Gallery
Free for personal use

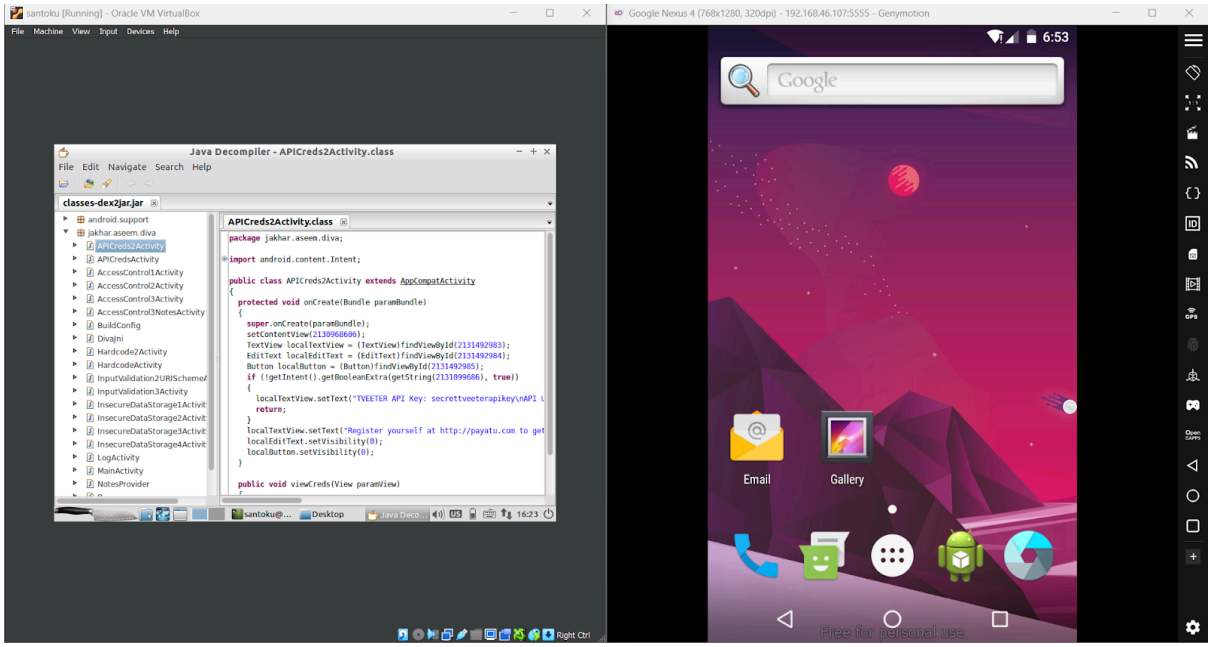

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop
File Edit Tabs Help
#7 : (in Landroid/support/v4/provider/DocumentFile;)
name : 'getName'
type : '()Ljava/lang/String;'
access : 0x0401 (PUBLIC ABSTRACT)
code : (none)
#8 : (in Landroid/support/v4/provider/DocumentFile;)
name : 'getParentFile'
type : '()Landroid/support/v4/provider/DocumentFile;'
access : 0x0001 (PUBLIC)
code -
registers : 2
ins : 1
outs : 0
insns size : 3 16-bit code units
0cf3a0: |[0cf3a0] android.support.v4.provider.DocumentFile
.getParentFile:()Landroid/support/v4/provider/DocumentFile;
0cf3b0: 5410 940e |0000: iget-object v0, v1, Landroid/support/v4/pro
vider/DocumentFile;.mParent:Landroid/support/v4/provider/DocumentFile; // field@0e94
0cf3b4: 1100 |0002: return-object v0
catches : (none)
positions :
0x0000 line=217
locals :
0x0000 - 0x0003 reg=1 this Landroid/support/v4/provider/DocumentFile;
#9 : (in Landroid/support/v4/provider/DocumentFile;)
name : 'getType'
type : '()Ljava/lang/String;'
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:23
Google
Email
Gallery
Free for personal use

Reverse Engineering using dex2jar and JDGUI

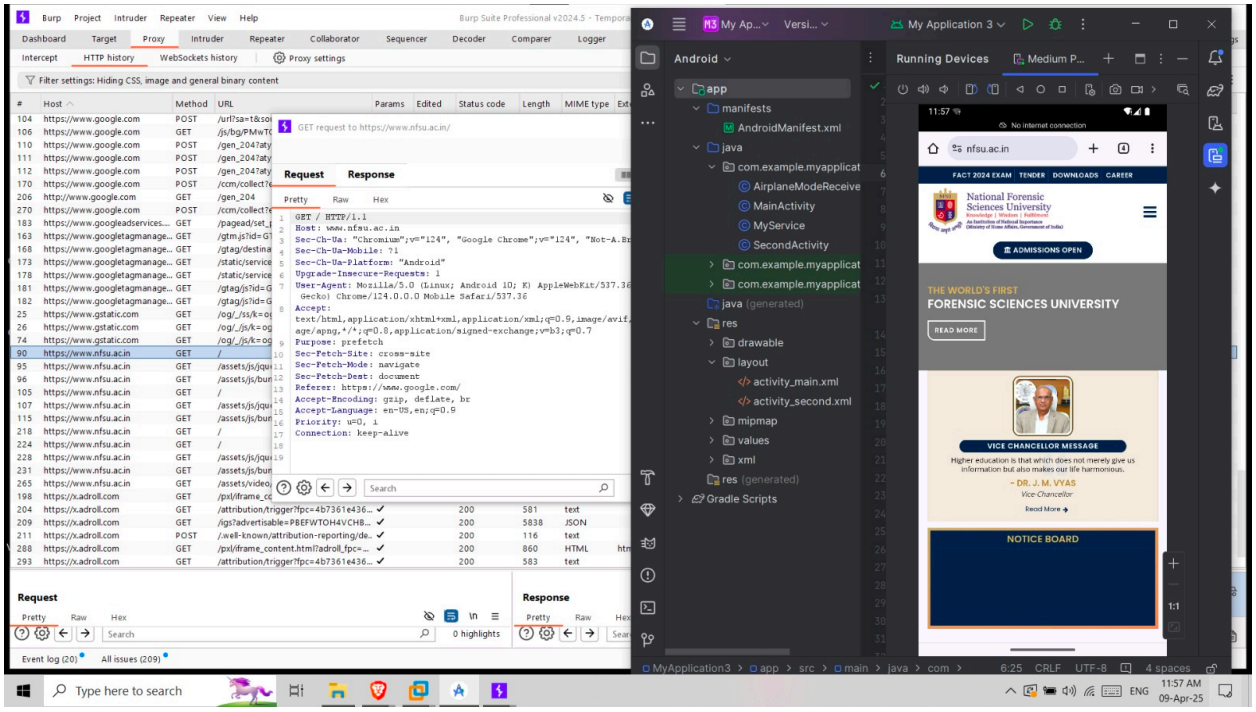





santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
santoku@santoku-VirtualBox: ~/Desktop/diva
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Desktop/diva$ d2j-dex2jar classes.dex
dex2jar classes.dex -> classes-dex2jar.jar
santoku@santoku-VirtualBox:~/Desktop/diva$ jd-gui classes-dex2jar.jar
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:53
Google
Email
Gallery
Free for personal use

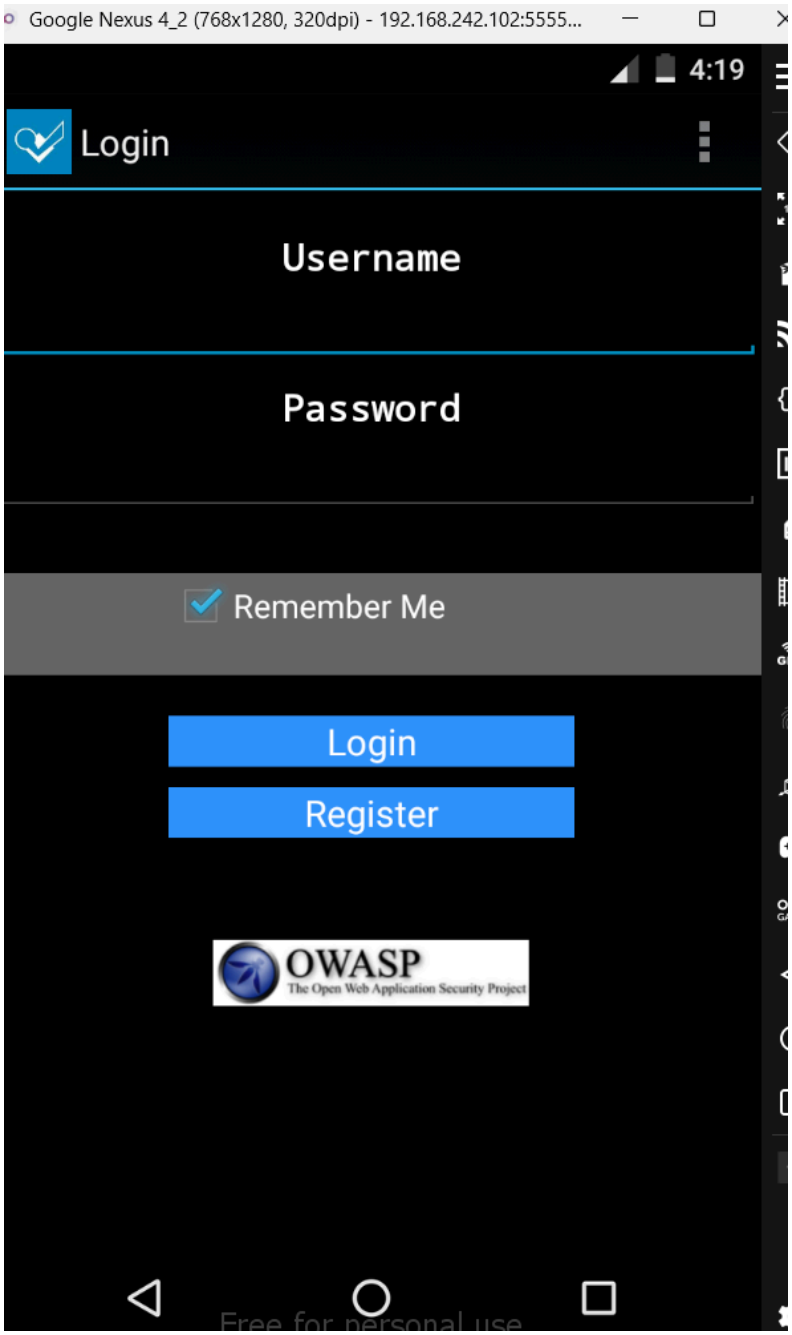

santoku [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Java Decompiler - APICreds2Activity.class
File Edit Navigate Search Help
classes-dex2jar.jar
APICreds2Activity.class
package jakhar.aseem.diva;
import android.content.Intent;
public class APICreds2Activity extends AppCompatActivity
Google Nexus 4 (768x1280, 320dpi) - 192.168.46.107:5555 - Genymotion
6:53
Google
Email
Gallery
Free for personal use

Request interception using BurpSuit

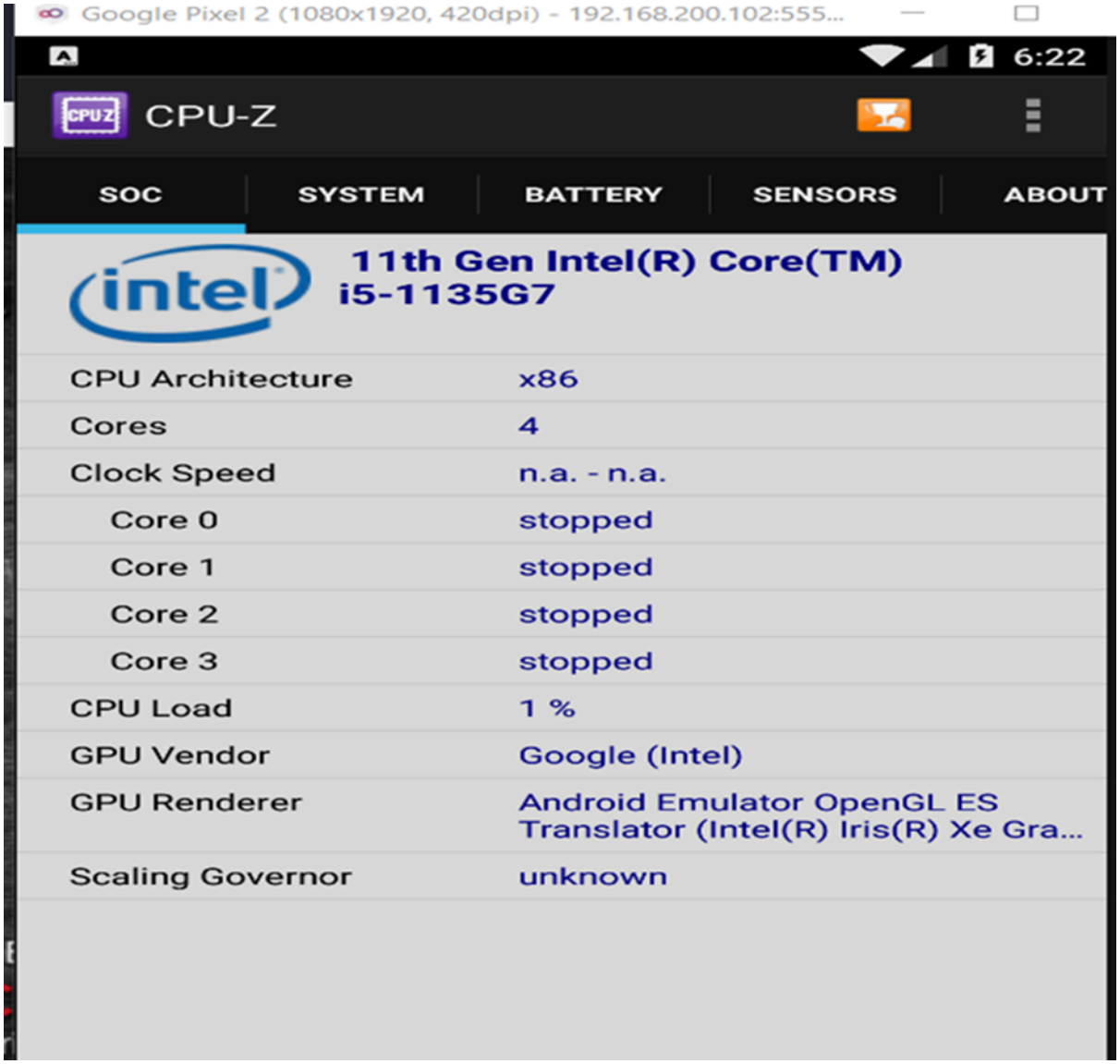


Configuration of Insecure Bank2

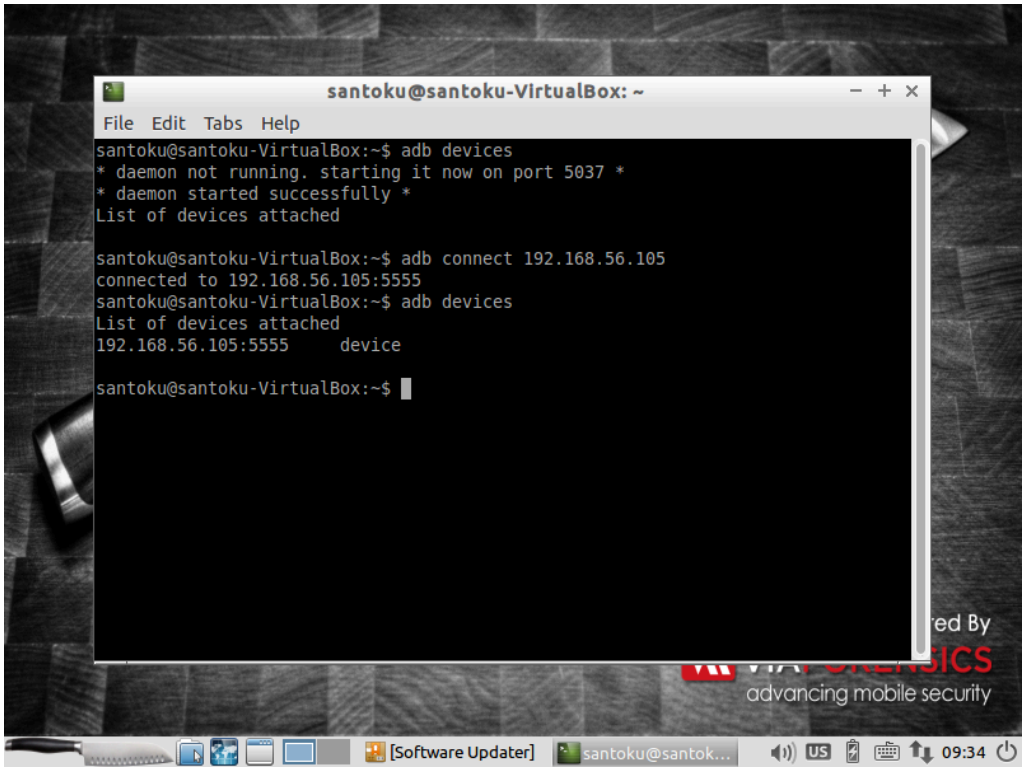
Configuration of OWASP GoatDroid

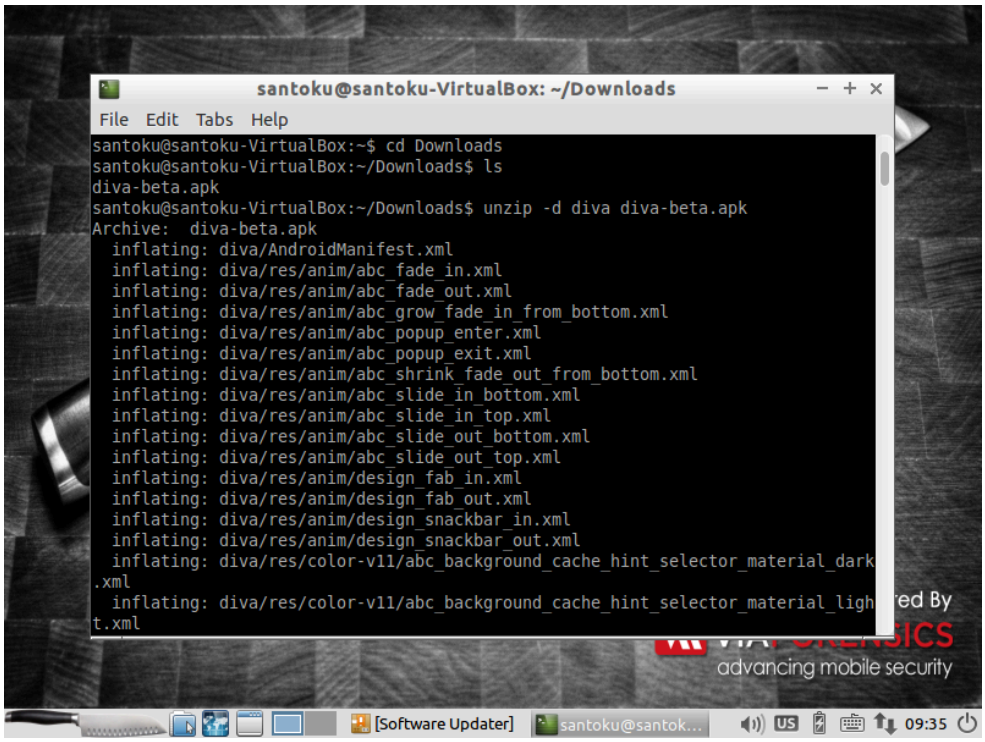


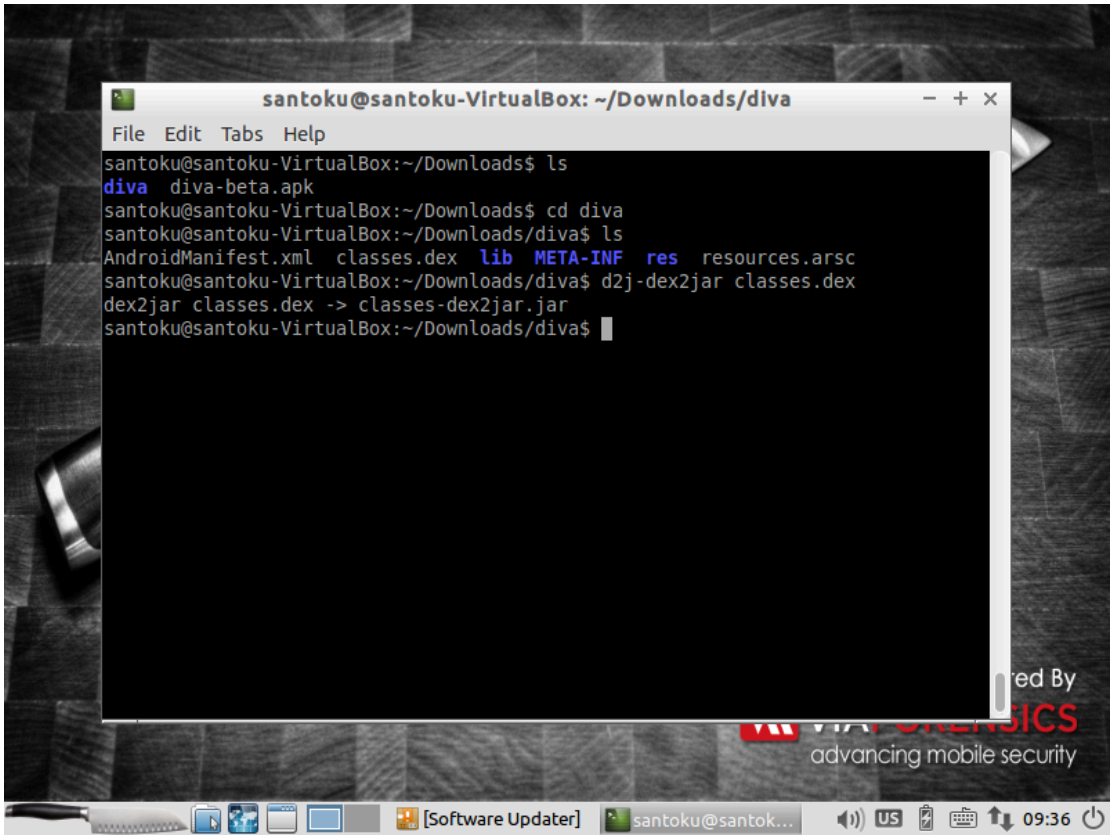
Configuration of Open GApps

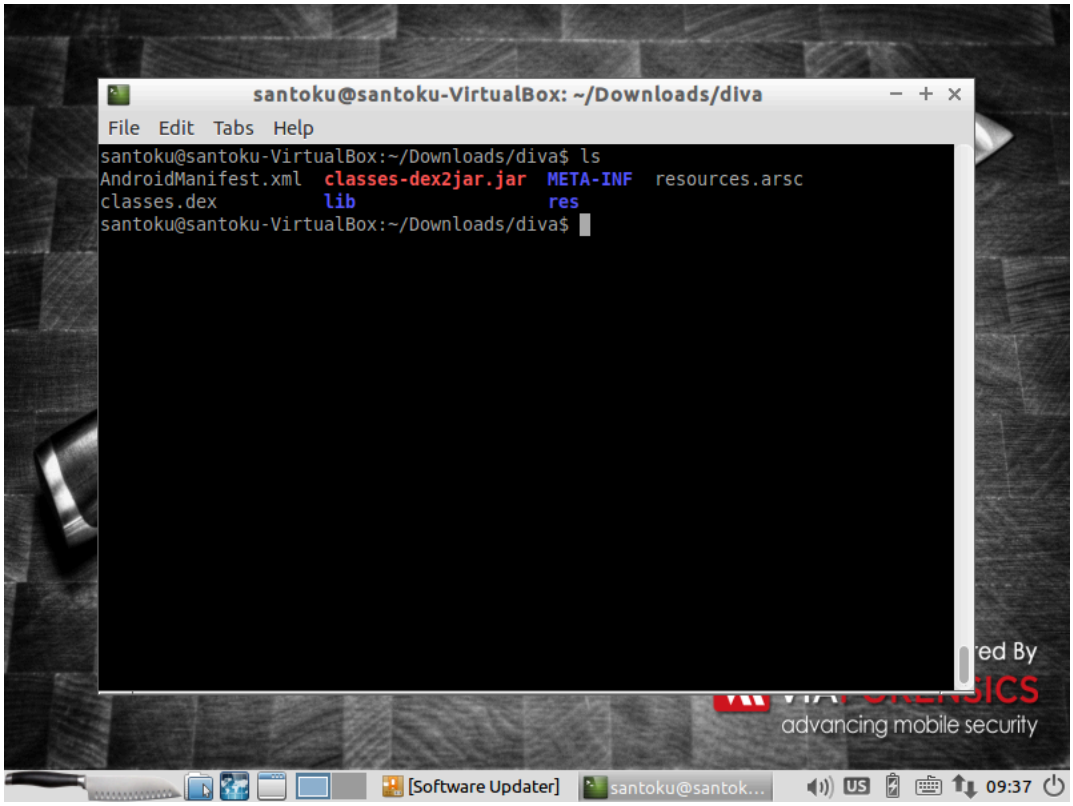


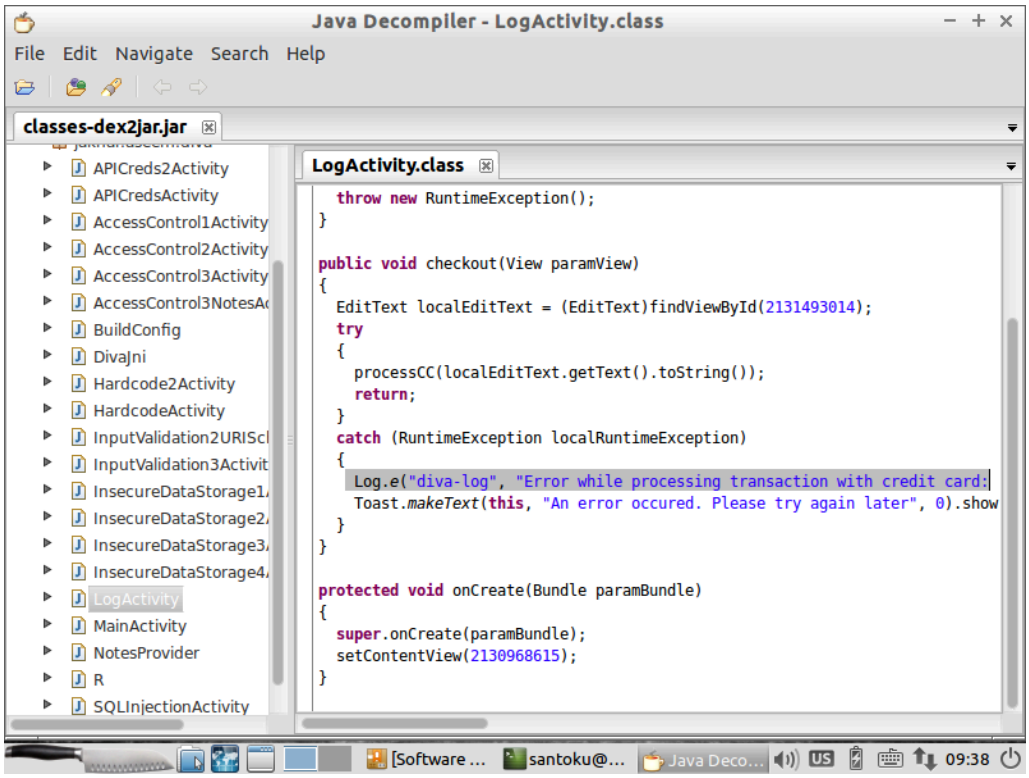
Insecure Logging – Vulnerability

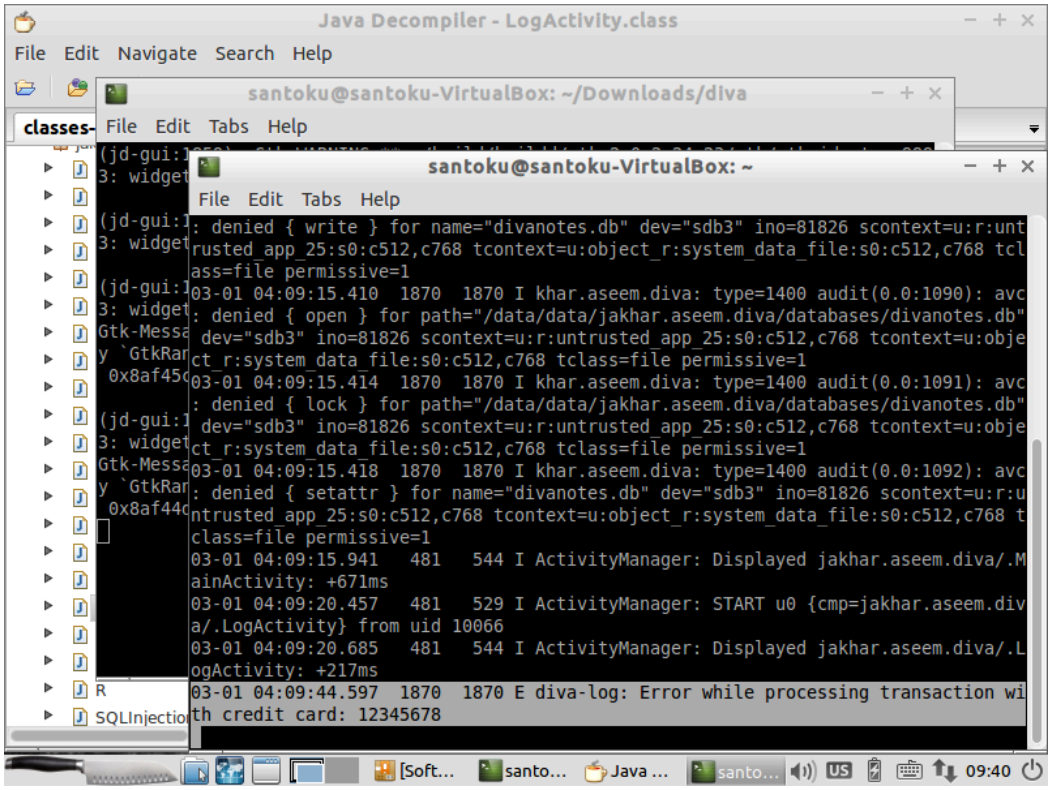


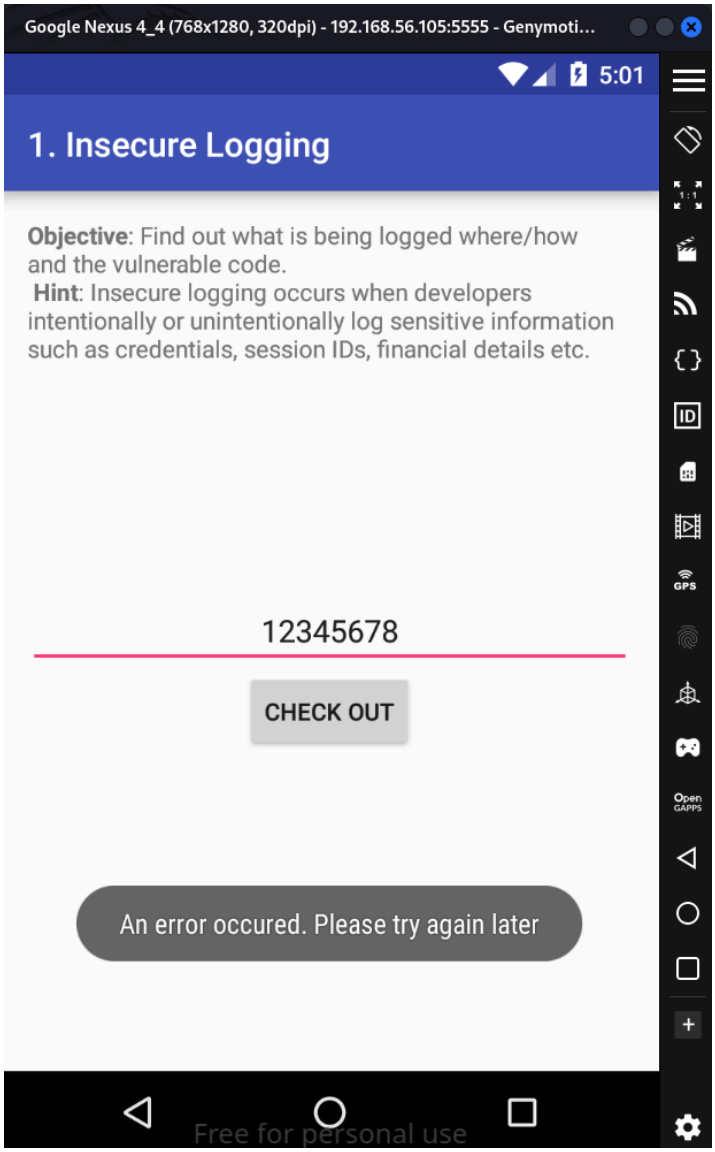



santoku@santoku-VirtualBox: ~/Downloads/diva
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads$ ls
diva diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ cd diva
santoku@santoku-VirtualBox:~/Downloads/diva$ ls
AndroidManifest.xml classes.dex lib META-INF res resources.arsc
santoku@santoku-VirtualBox:~/Downloads/diva$ d2j-dex2jar classes.dex
dex2jar classes.dex -> classes-dex2jar.jar
santoku@santoku-VirtualBox:~/Downloads/diva$
ed By
advancing mobile security
[Software Updater]
santoku@santok...
US
09:36

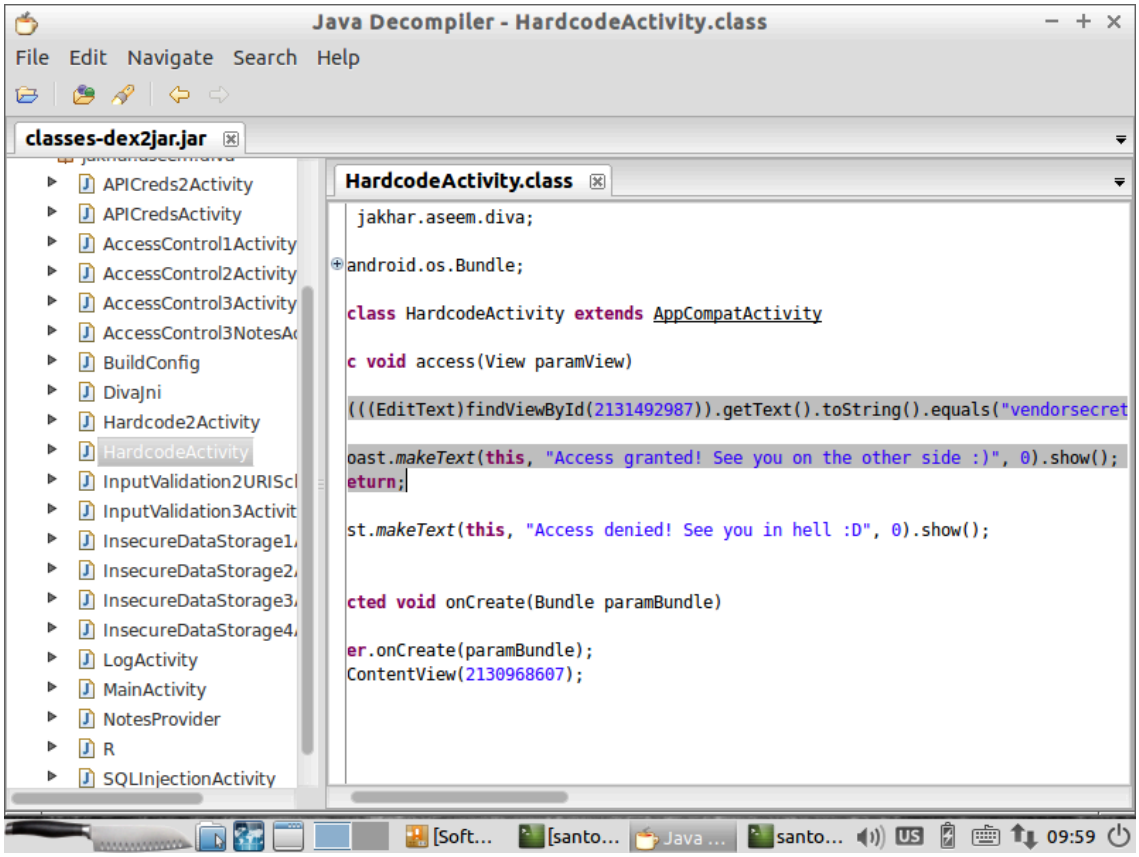

santoku@santoku-VirtualBox: ~/Downloads/diva
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/diva$ ls
AndroidManifest.xml classes-dex2jar.jar META-INF resources.arsc
classes.dex lib res
santoku@santoku-VirtualBox:~/Downloads/diva$
advancing mobile security
[Software Updater]
santoku@santok...
09:37

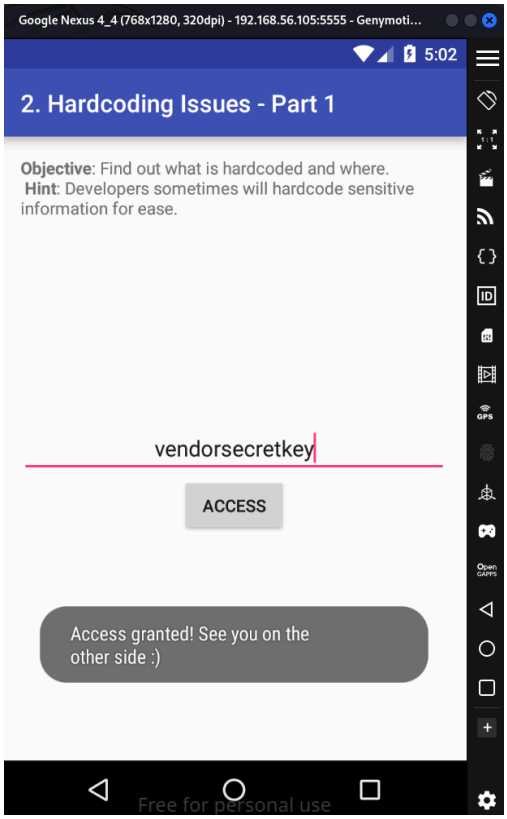

Java Decompiler - LogActivity.class
File Edit Navigate Search Help
classes-dex2jar.jar
APICreds2Activity
APICredsActivity
AccessControl1Activity
AccessControl2Activity
AccessControl3Activity
BuildConfig
DivaJni
Hardcode2Activity
HardcodeActivity
LogActivity
MainActivity
NotesProvider
R
SQLInjectionActivity
LogActivity.class
throw new RuntimeException();
}
public void checkout(View paramView)
{
EditText localEditText = (EditText)findViewById(2131493014);
try
{
processCC(localEditText.getText().toString());
return;
}
catch (RuntimeException localRuntimeException)
{
Log.e("diva-log", "Error while processing transaction with credit card:
Toast.makeText(this, "An error occured. Please try again later", 0).show
}
}
protected void onCreate(Bundle paramBundle)
{
super.onCreate(paramBundle);
setContentView(2130968615);
}
[Software ...
santoku@...
Java Deco...
09:38


Java Decompiler - LogActivity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~/Downloads/diva
File Edit Tabs Help
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
: denied { write } for name="divanotes.db" dev="sdb3" ino=81826 scontext=u:r:unt
rusted_app_25:s0:c512,c768 tcontext=u:object_r:system_data_file:s0:c512,c768 tcl
ass=file permissive=1
03-01 04:09:15.410 1870 1870 I khar.aseem.diva: type=1400 audit(0.0:1090): avc
: denied { open } for path="/data/data/jakhar.aseem.diva/databases/divanotes.db"
dev="sdb3" ino=81826 scontext=u:r:untrusted_app_25:s0:c512,c768 tcontext=u:obje
ct_r:system_data_file:s0:c512,c768 tclass=file permissive=1
03-01 04:09:15.414 1870 1870 I khar.aseem.diva: type=1400 audit(0.0:1091): avc
: denied { lock } for path="/data/data/jakhar.aseem.diva/databases/divanotes.db"
dev="sdb3" ino=81826 scontext=u:r:untrusted_app_25:s0:c512,c768 tcontext=u:obje
ct_r:system_data_file:s0:c512,c768 tclass=file permissive=1
03-01 04:09:15.418 1870 1870 I khar.aseem.diva: type=1400 audit(0.0:1092): avc
: denied { setattr } for name="divanotes.db" dev="sdb3" ino=81826 scontext=u:r:u
ntrusted_app_25:s0:c512,c768 tcontext=u:object_r:system_data_file:s0:c512,c768 t
class=file permissive=1
03-01 04:09:15.941 481 544 I ActivityManager: Displayed jakhar.aseem.diva/.M
ainActivity: +671ms
03-01 04:09:20.457 481 529 I ActivityManager: START u0 {cmp=jakhar.aseem.div
a/.LogActivity} from uid 10066
03-01 04:09:20.685 481 544 I ActivityManager: Displayed jakhar.aseem.diva/.L
ogActivity: +217ms
03-01 04:09:44.597 1870 1870 E diva-log: Error while processing transaction wi
th credit card: 12345678
09:40

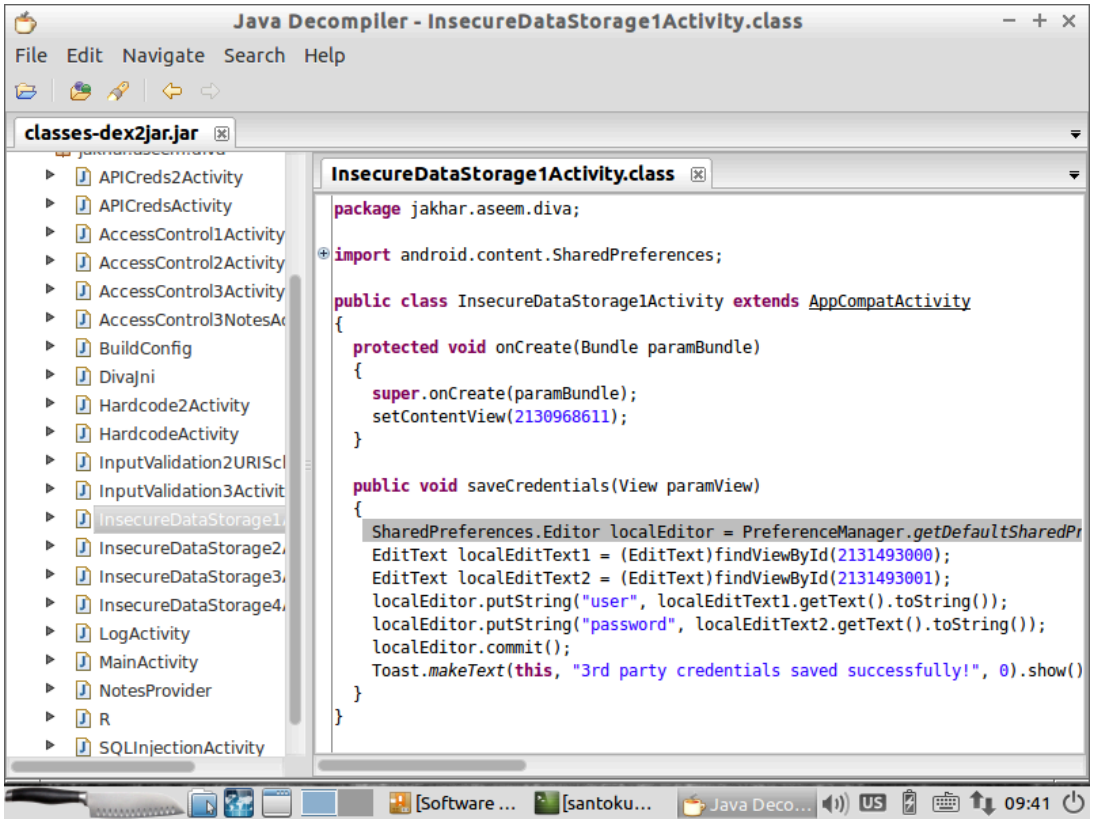

Google Nexus 4_4 (768x1280, 320dpi) - 192.168.56.105:5555 - Genymoti...
5:01
1. Insecure Logging
Objective: Find out what is being logged where/how and the vulnerable code.
Hint: Insecure logging occurs when developers intentionally or unintentionally log sensitive information such as credentials, session IDs, financial details etc.
12345678
CHECK OUT
An error occured. Please try again later
Free for personal use

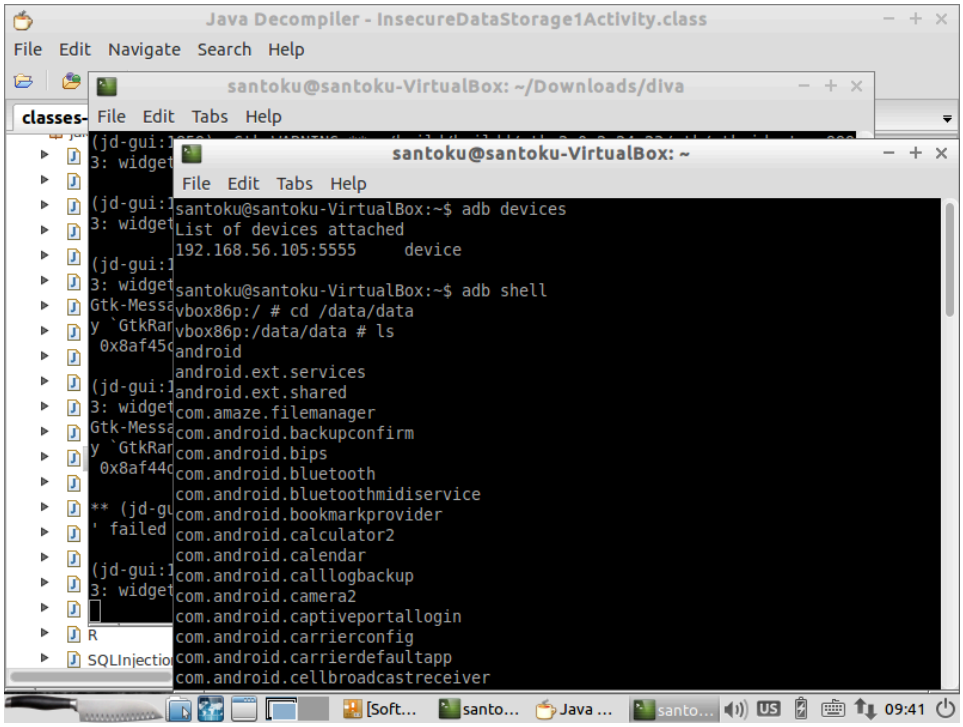
Hard Coding Issue – Vulnerability

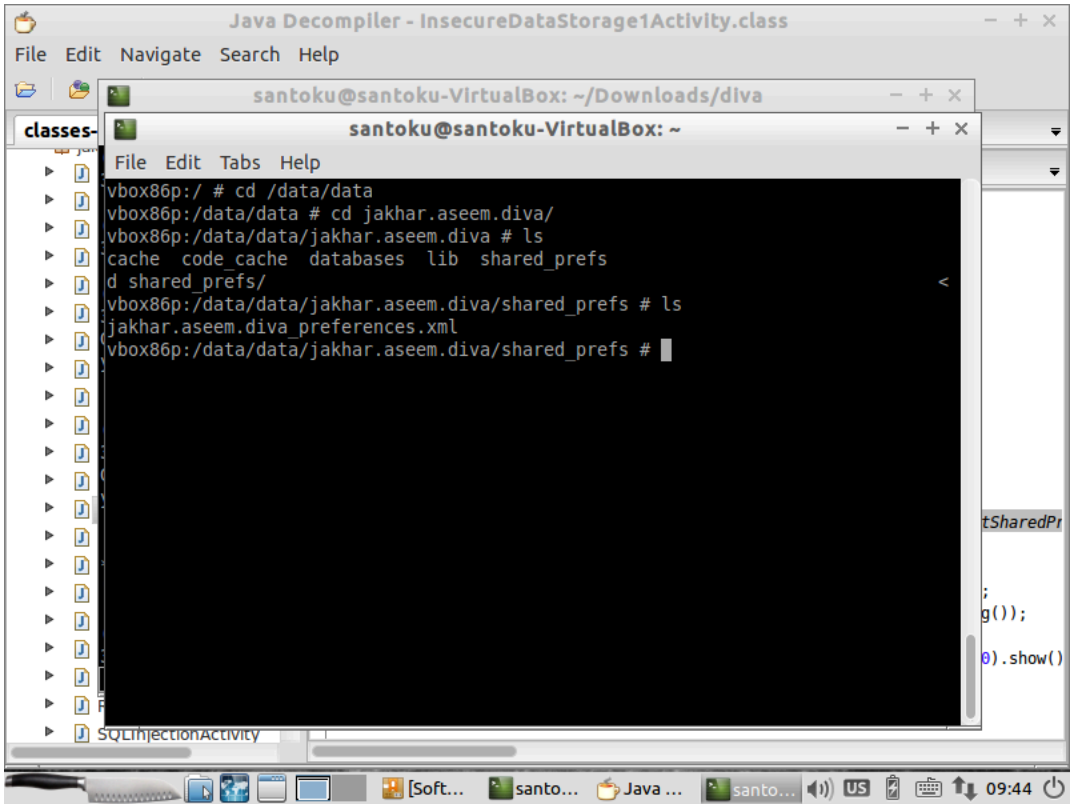


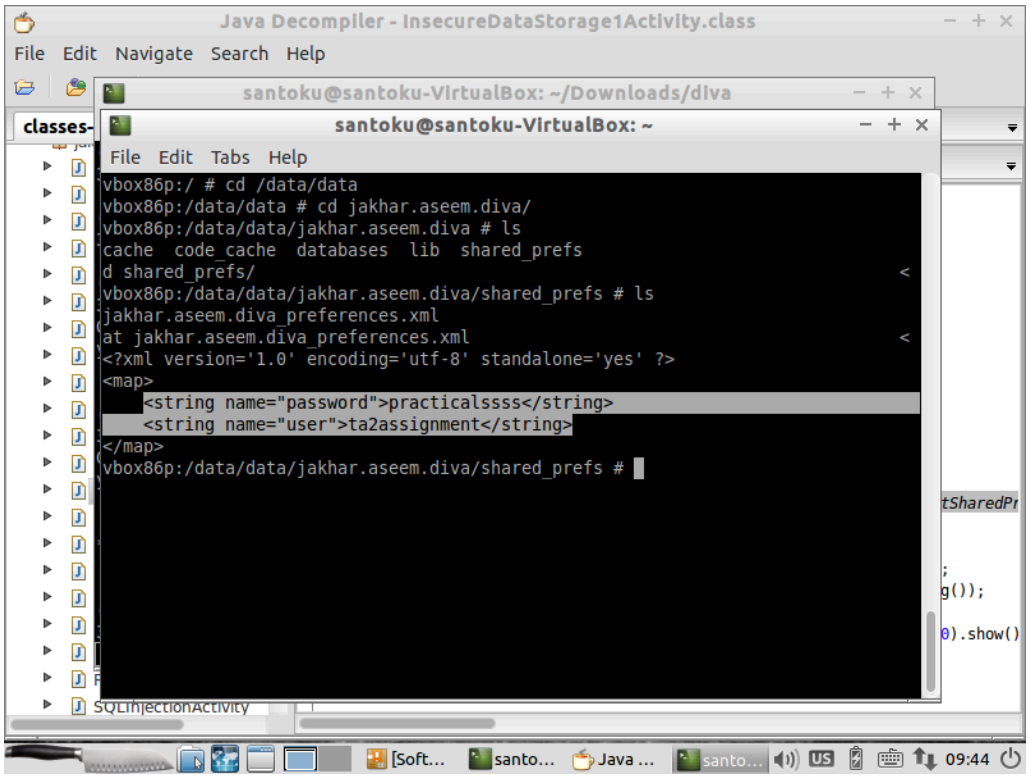


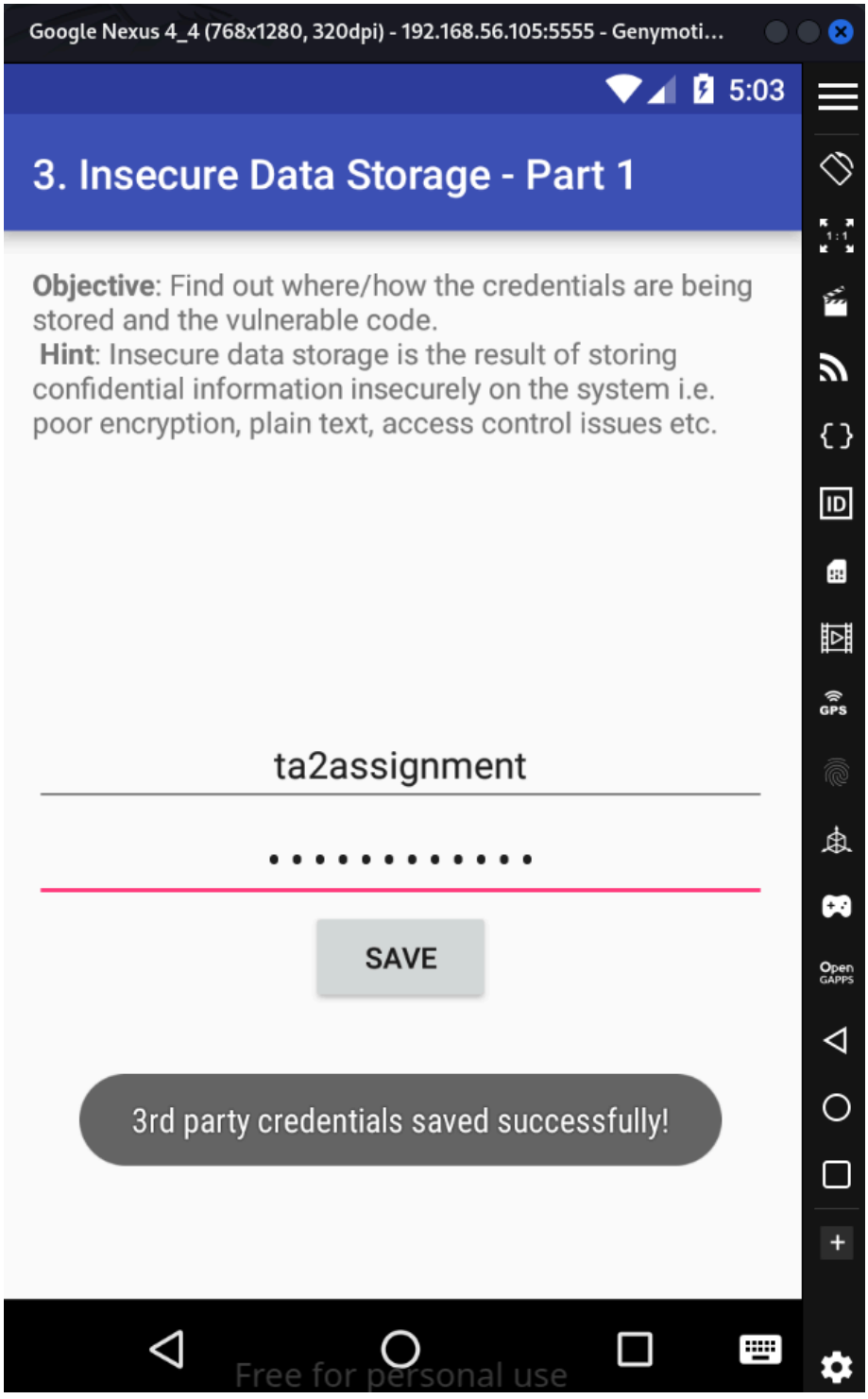
Insecure Data Storage (Shared Preference) –Vulnerability



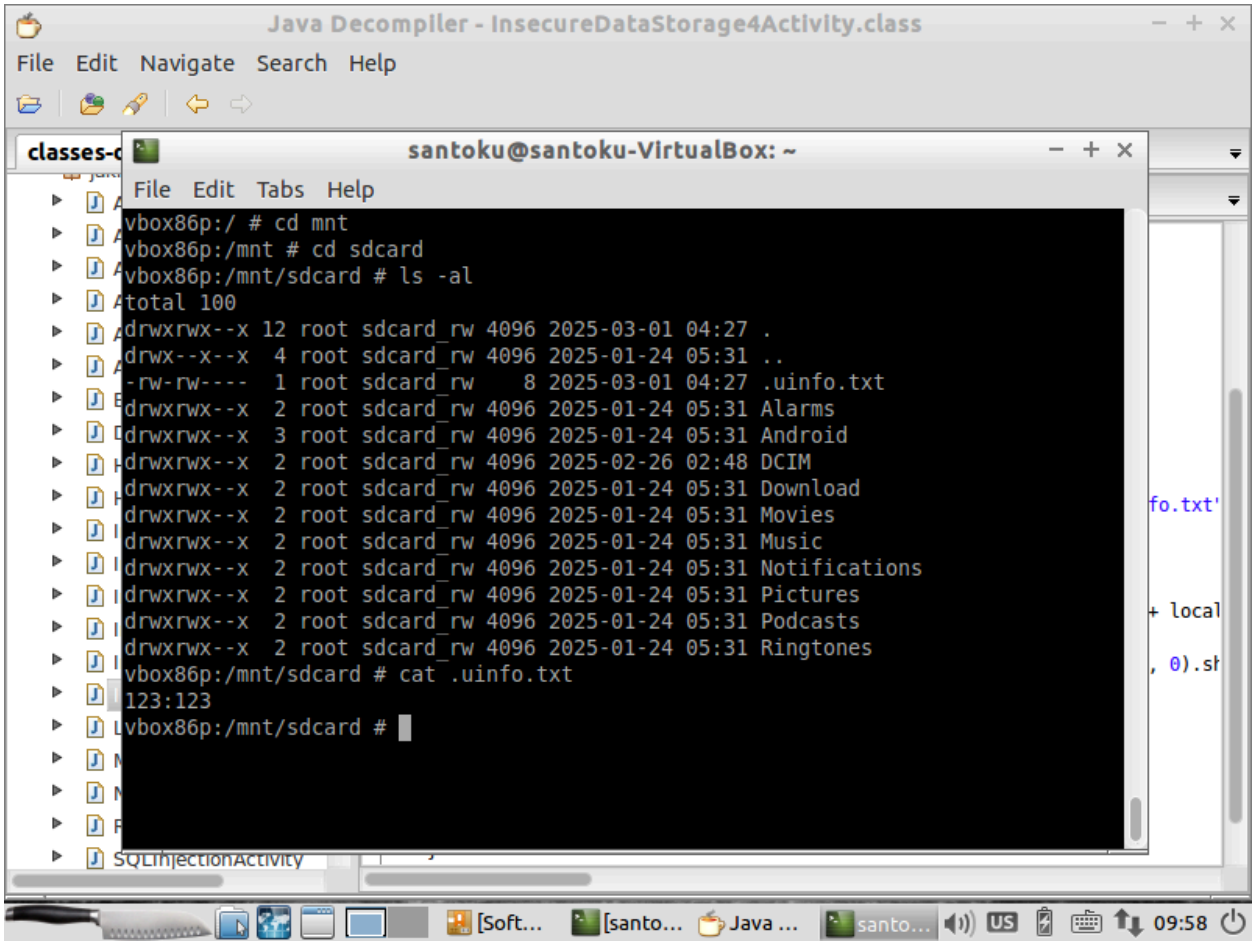



Java Decompiler - InsecureDataStorage1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~/Downloads/diva
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd /data/data
vbox86p:/data/data # cd jakhar.aseem.diva/
vbox86p:/data/data/jakhar.aseem.diva # ls
cache code_cache databases lib shared_prefs
d shared_prefs/
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs #
SQLInjectionActivity
09:44

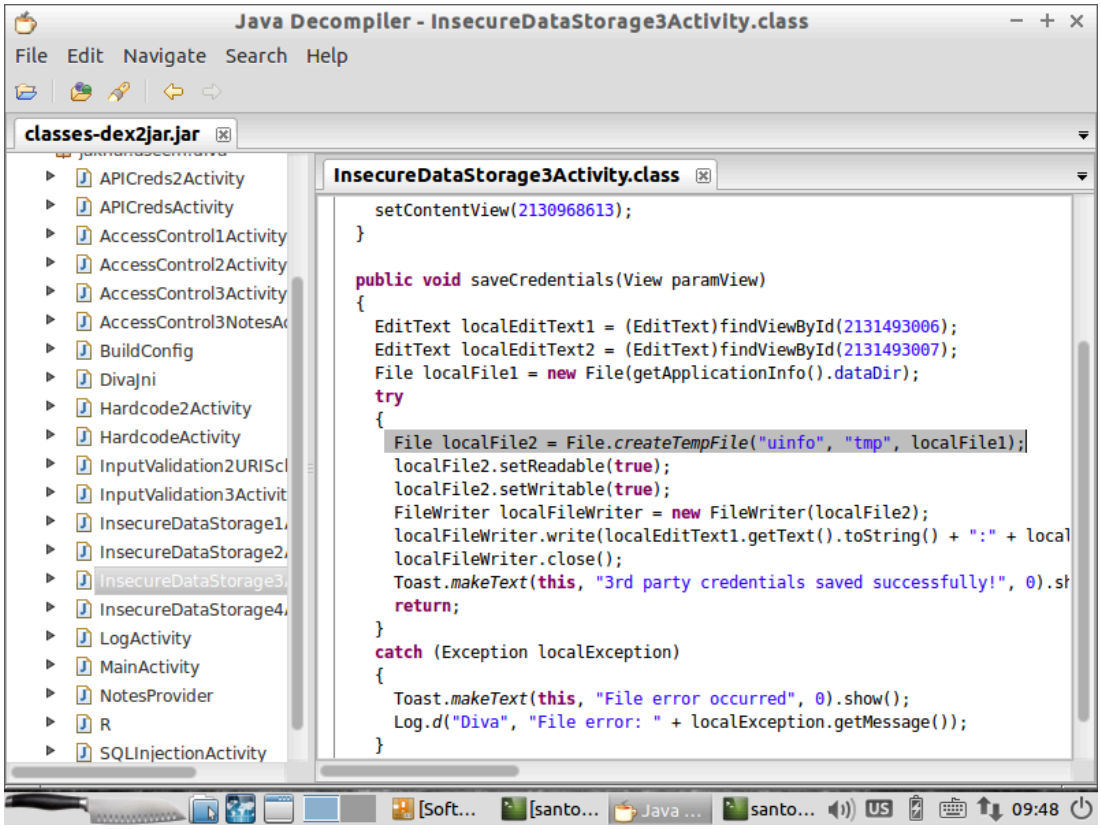

Java Decompiler - InsecureDataStorage1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~/Downloads/diva
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
vbox86p:/ # cd /data/data
vbox86p:/data/data # cd jakhar.aseem.diva/
vbox86p:/data/data/jakhar.aseem.diva # ls
cache code_cache databases lib shared_prefs
d shared_prefs/
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs # ls
jakhar.aseem.diva_preferences.xml
at jakhar.aseem.diva_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<string name="password">practicalssss</string>
<string name="user">ta2assignment</string>
</map>
vbox86p:/data/data/jakhar.aseem.diva/shared_prefs #
SQLInjectionActivity
09:44

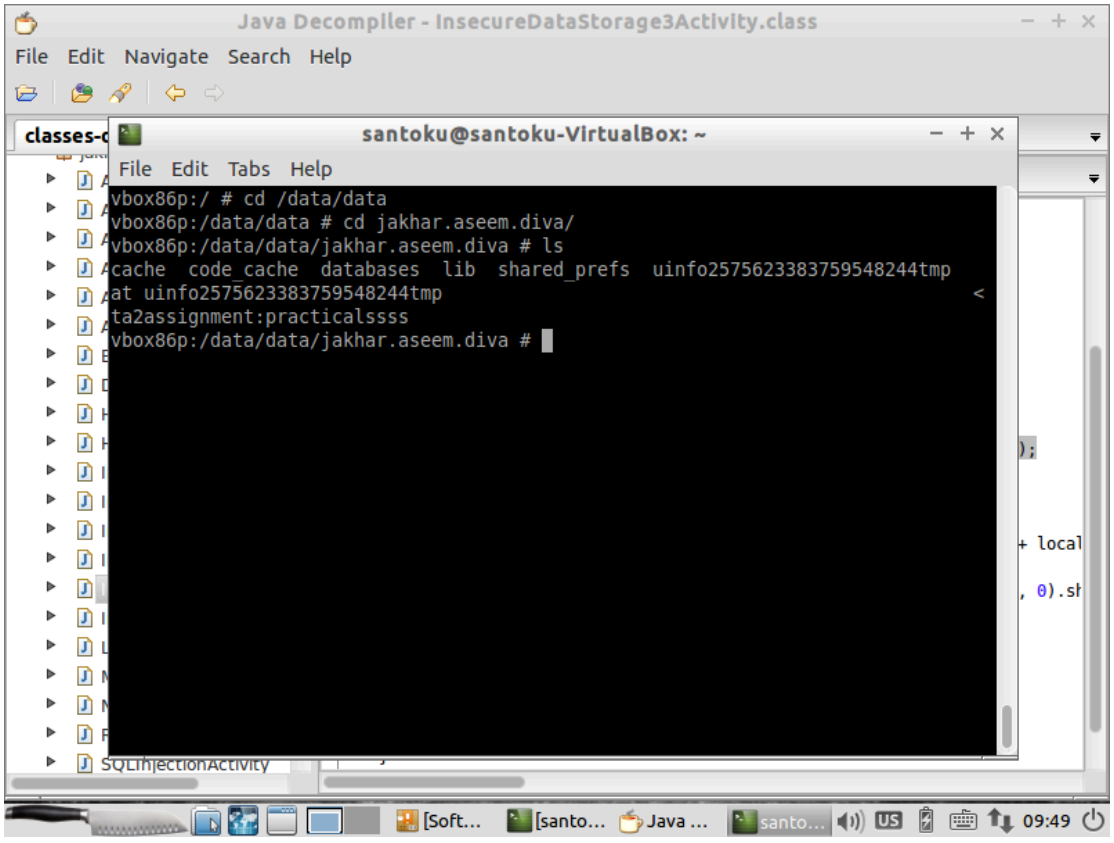

Google Nexus 4_4 (768x1280, 320dpi) - 192.168.56.105:5555 - Genymoti...
5:03
3. Insecure Data Storage - Part 1
Objective: Find out where/how the credentials are being stored and the vulnerable code.
Hint: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.
ta2assignment
SAVE
3rd party credentials saved successfully!
Free for personal use

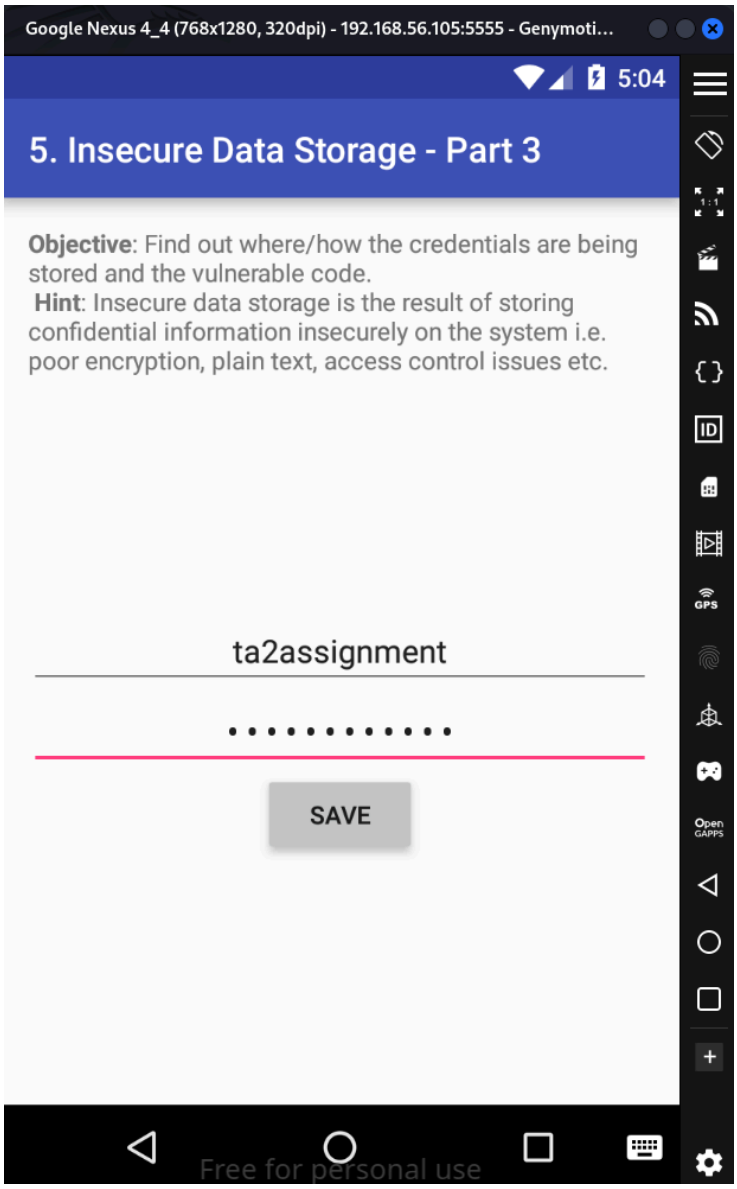
Insecure Data Storage (SD Card) –Vulnerability



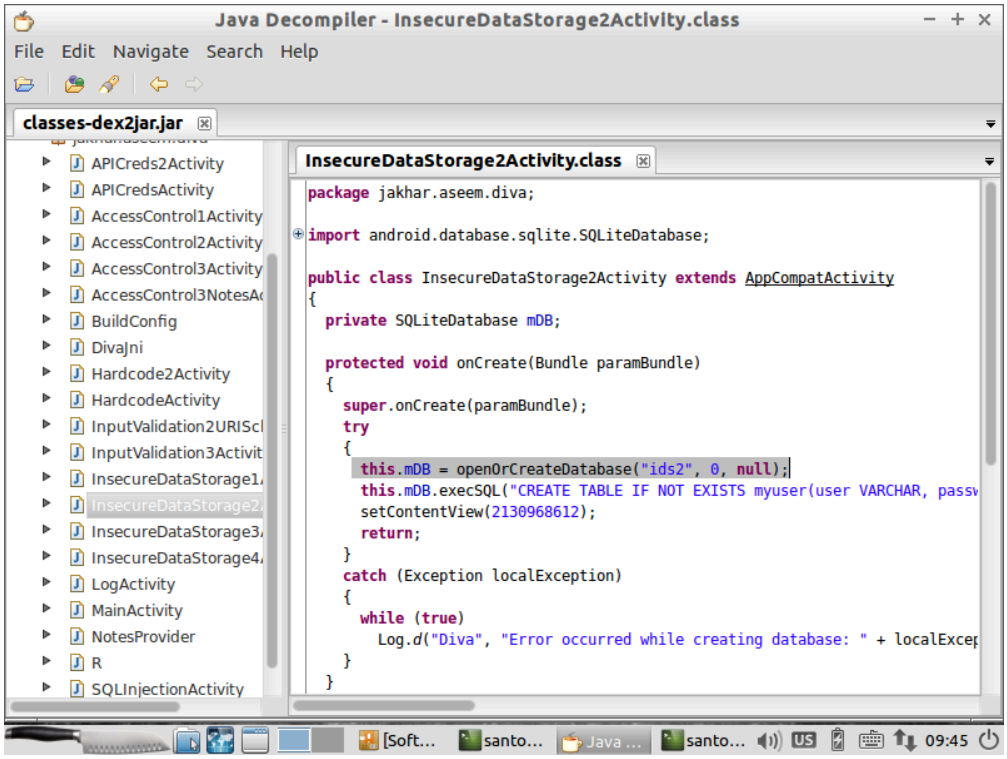
Insecure Data Storage (Temp File) –Vulnerability

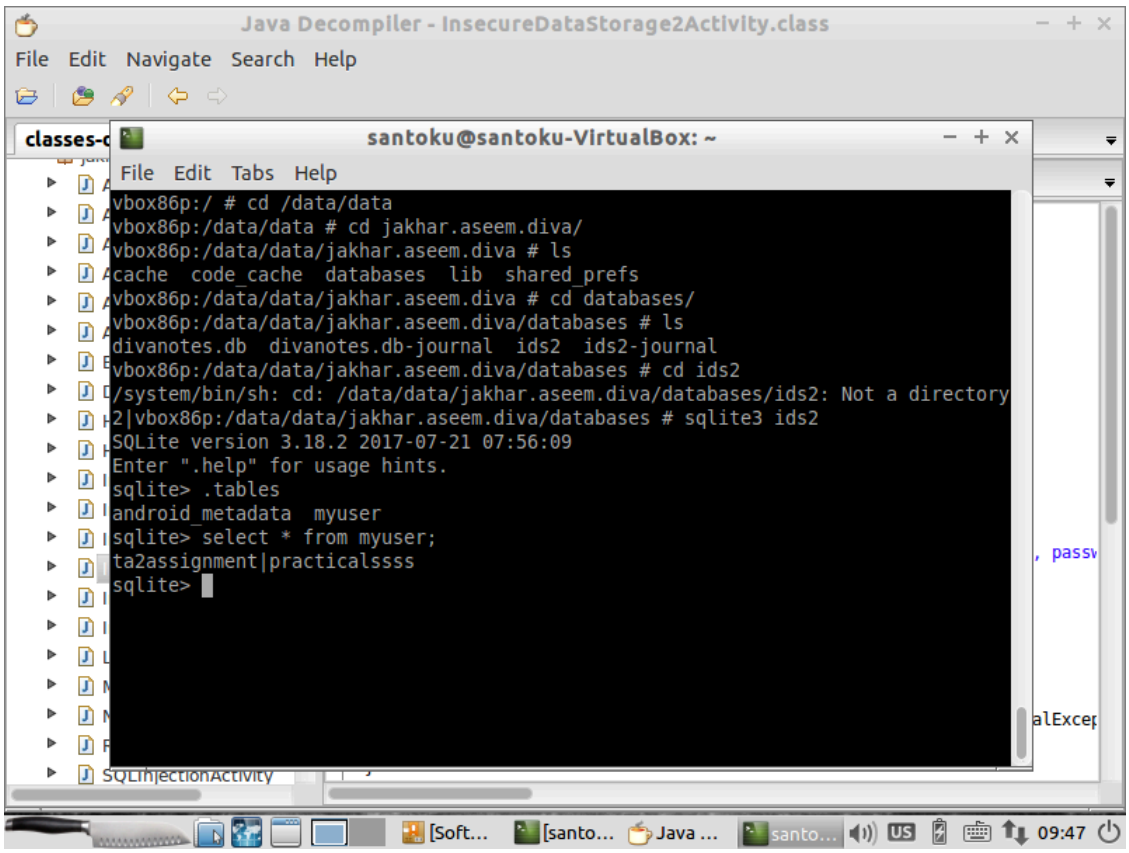


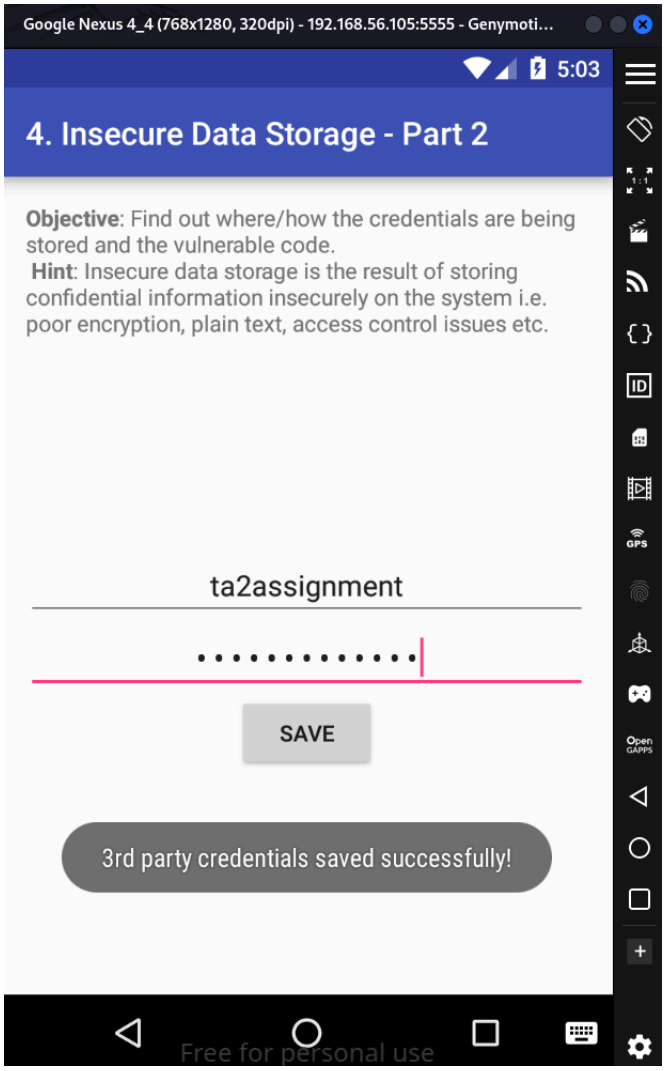



Google Nexus 4_4 (768x1280, 320dpi) - 192.168.56.105:5555 - Genymoti...
5:04
5. Insecure Data Storage - Part 3
Objective: Find out where/how the credentials are being stored and the vulnerable code.
Hint: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.
ta2assignment
SAVE
Free for personal use

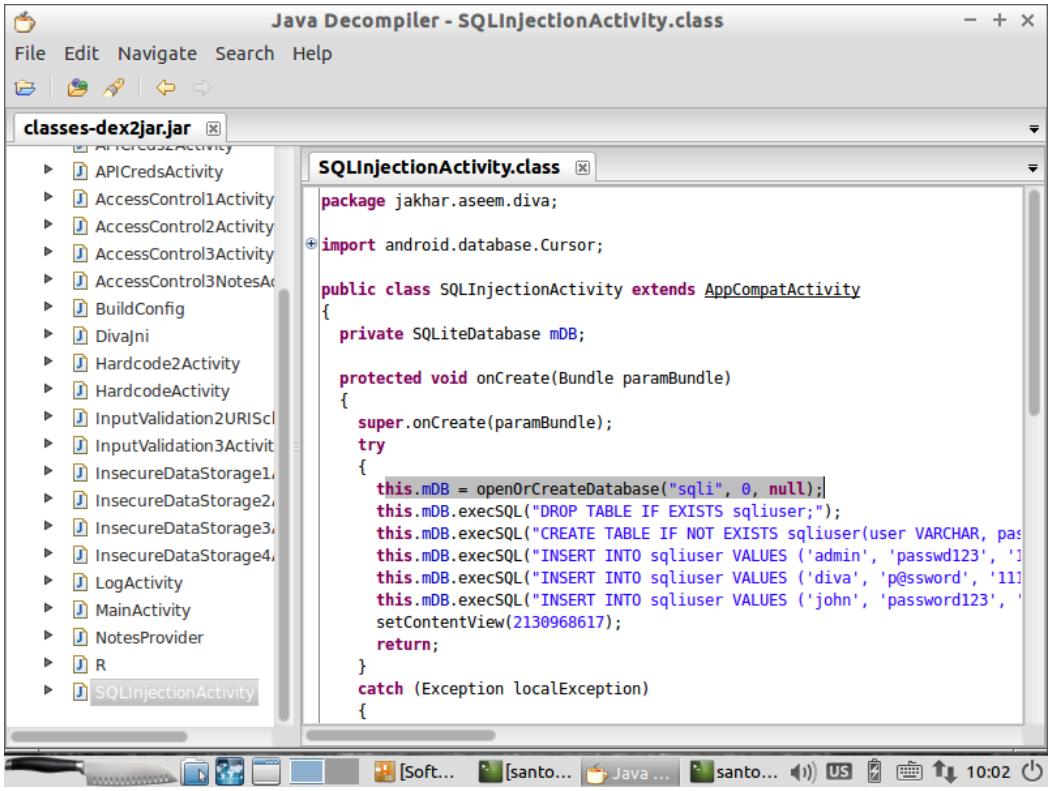
Insecure Data Storage (SQLight Database) –Vulnerability

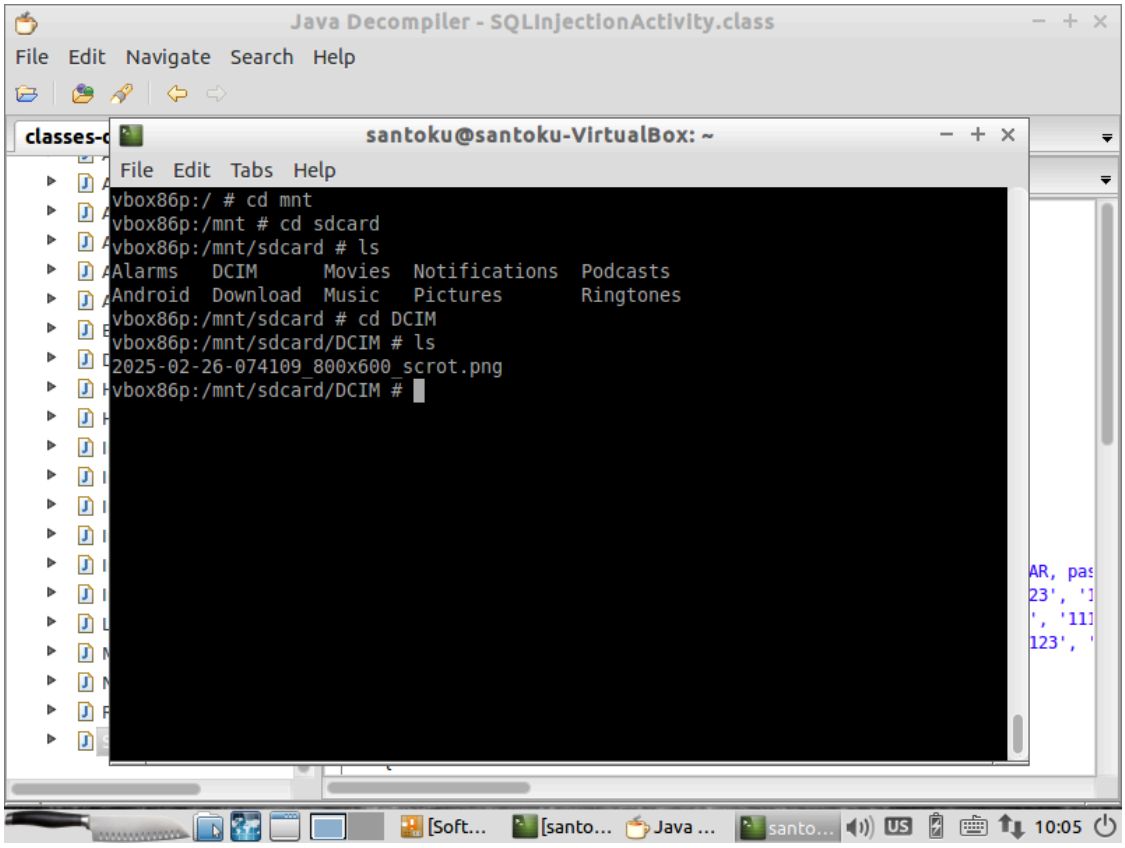




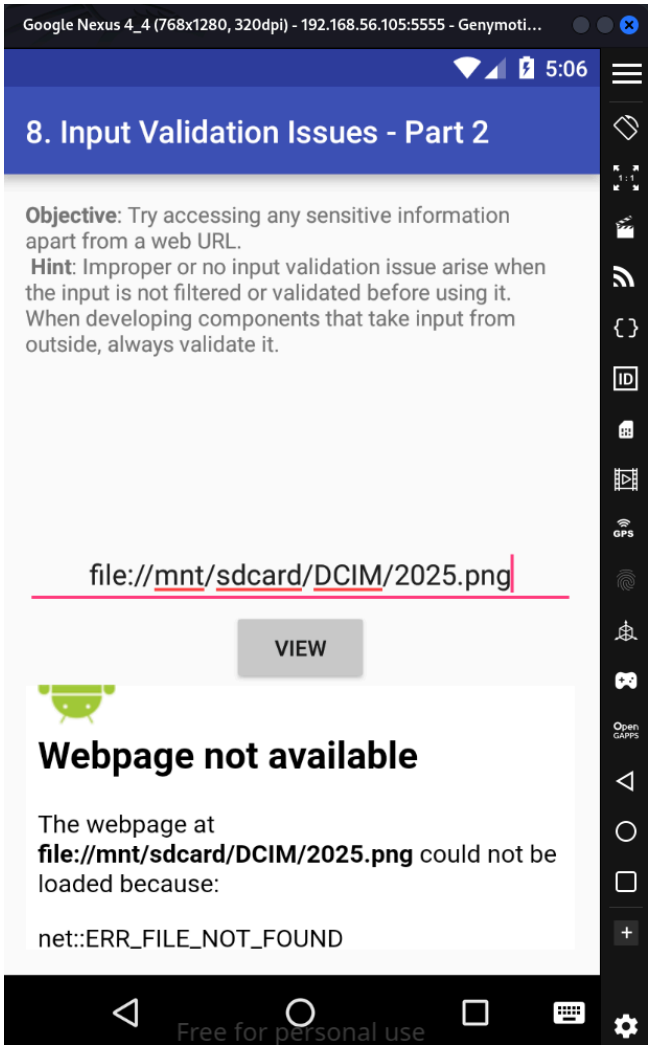

Google Nexus 4_4 (768x1280, 320dpi) - 192.168.56.105:5555 - Genymoti...
5:03
4. Insecure Data Storage - Part 2
Objective: Find out where/how the credentials are being stored and the vulnerable code.
Hint: Insecure data storage is the result of storing confidential information insecurely on the system i.e. poor encryption, plain text, access control issues etc.
ta2assignment
SAVE
3rd party credentials saved successfully!
Free for personal use

Input Validation and Data Sanitization (SQLInjection) – Vulnerability

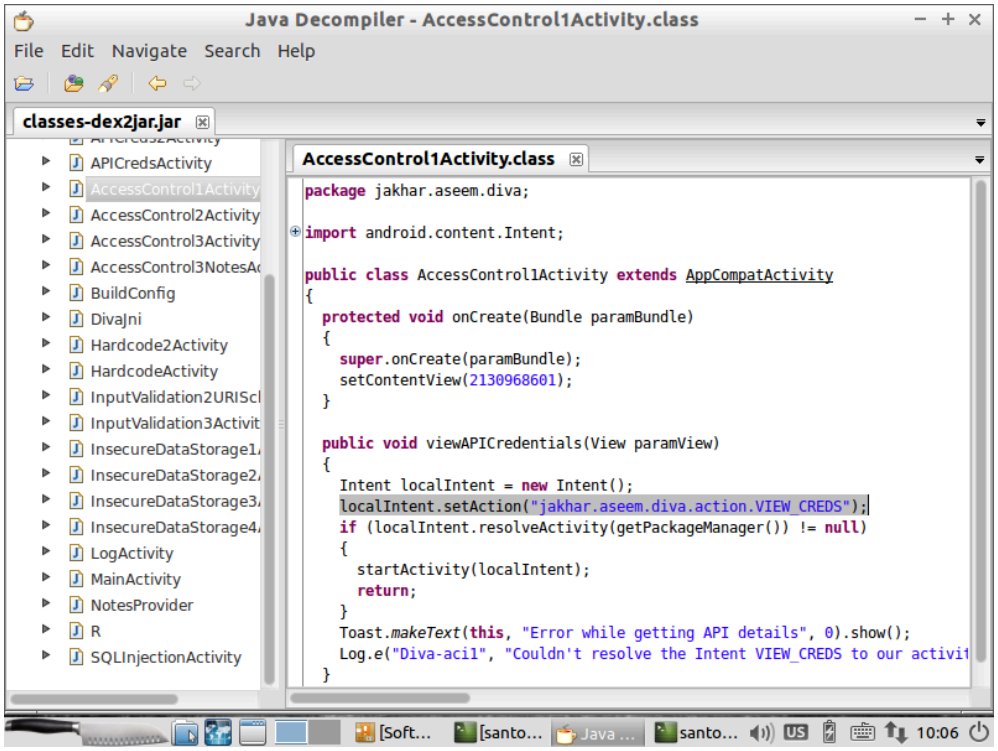


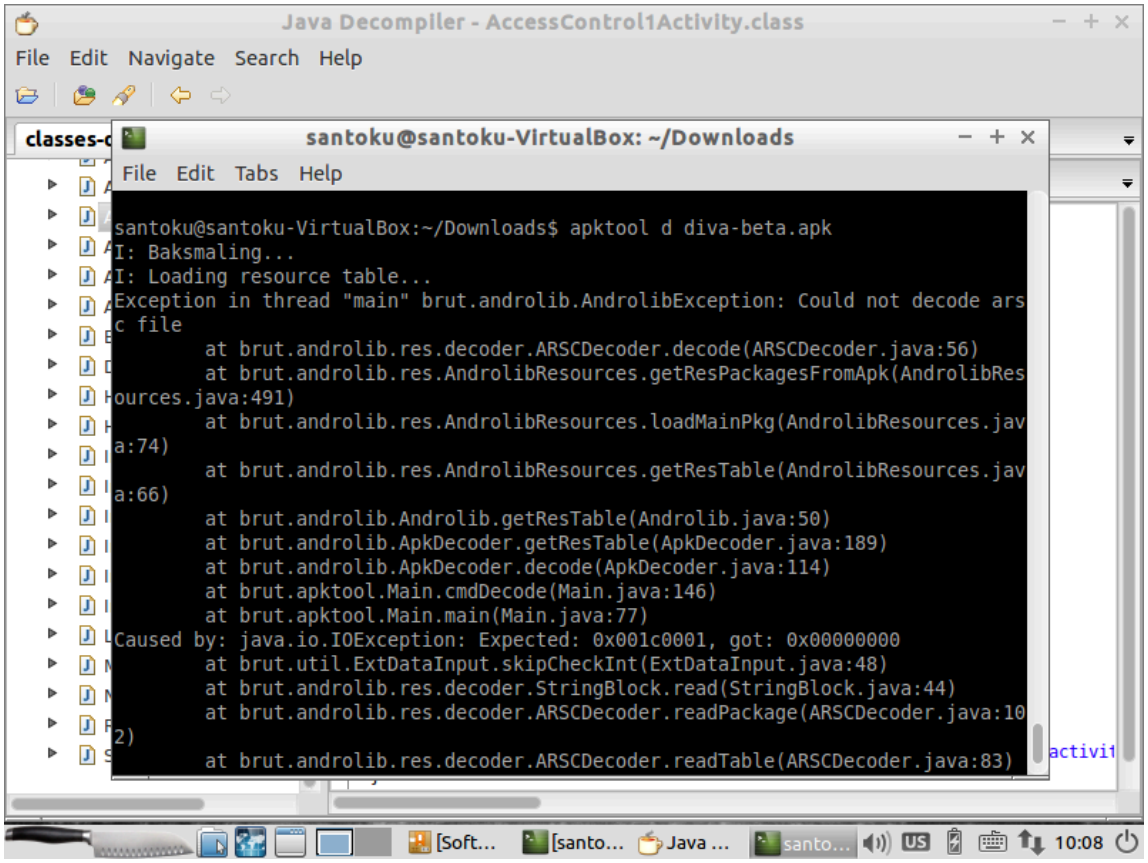


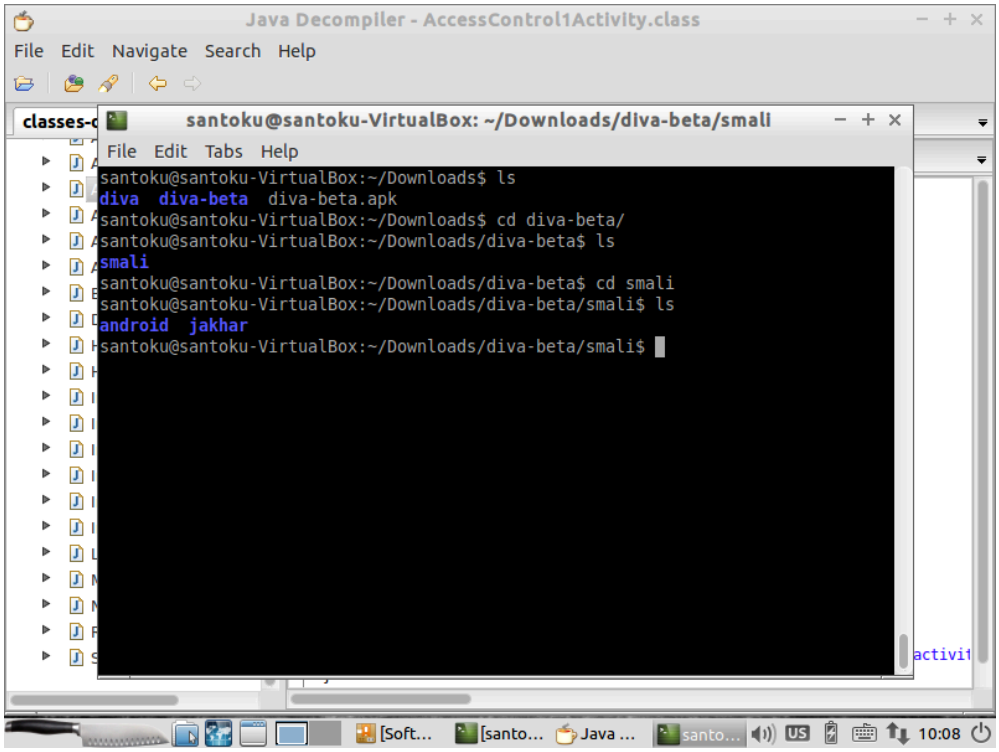
Input Validation and Data Sanitization (WebView) – Vulnerability

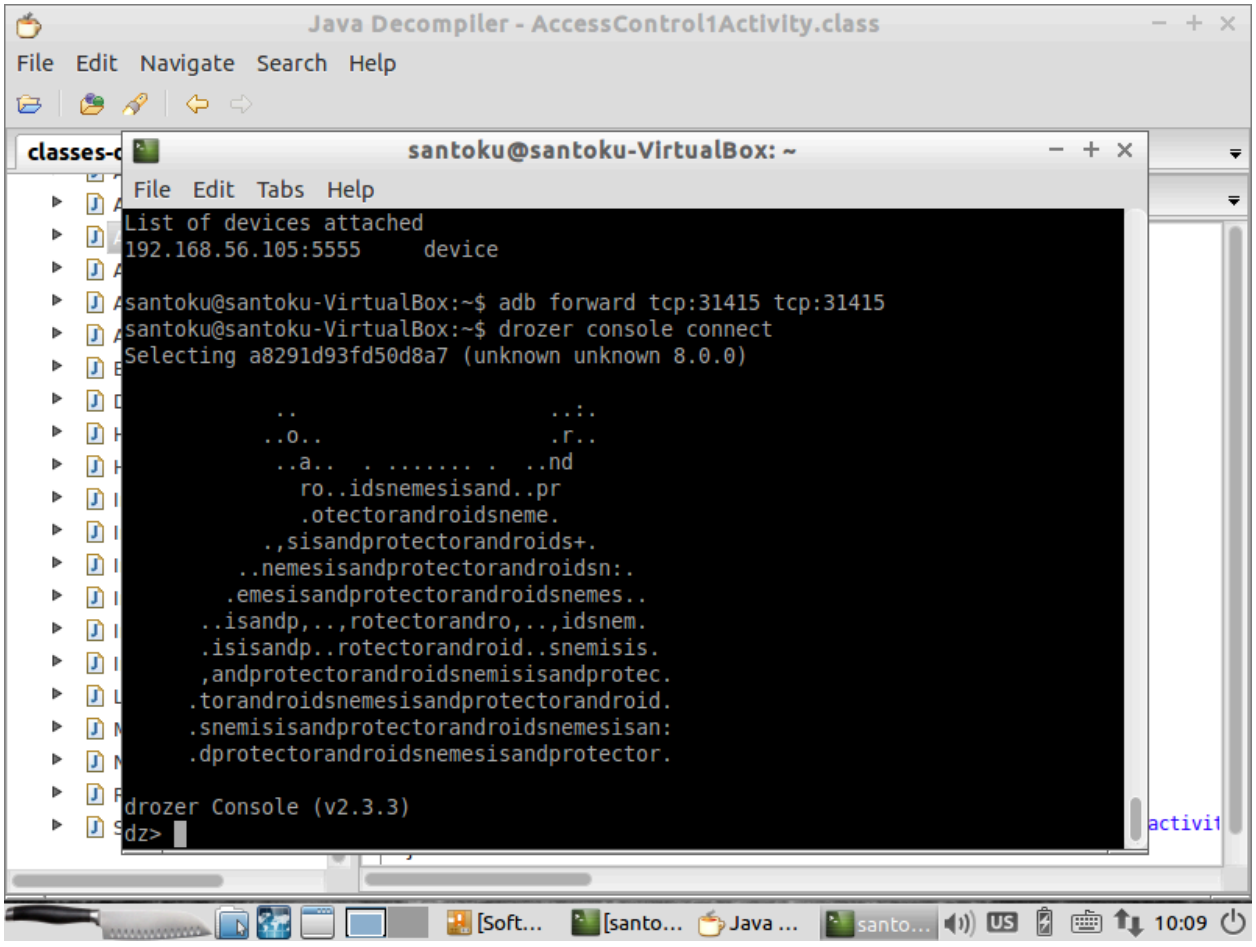


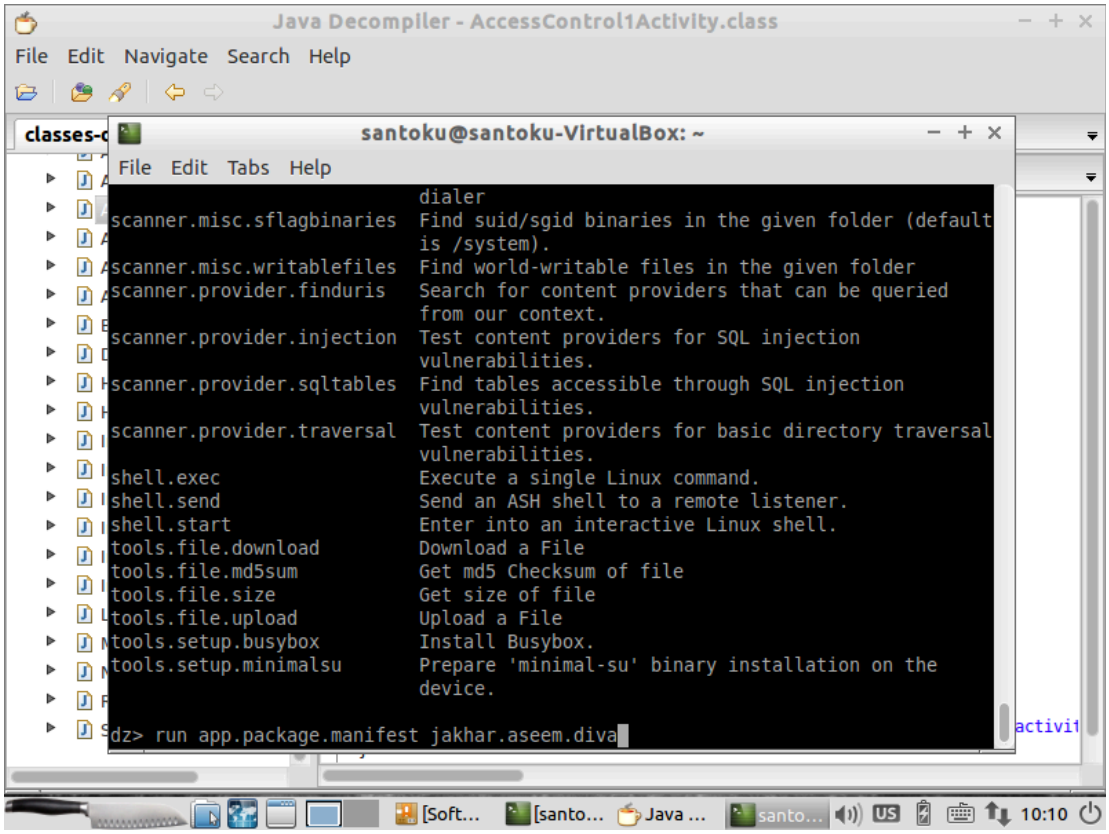
Access Control Issue – Vulnerability

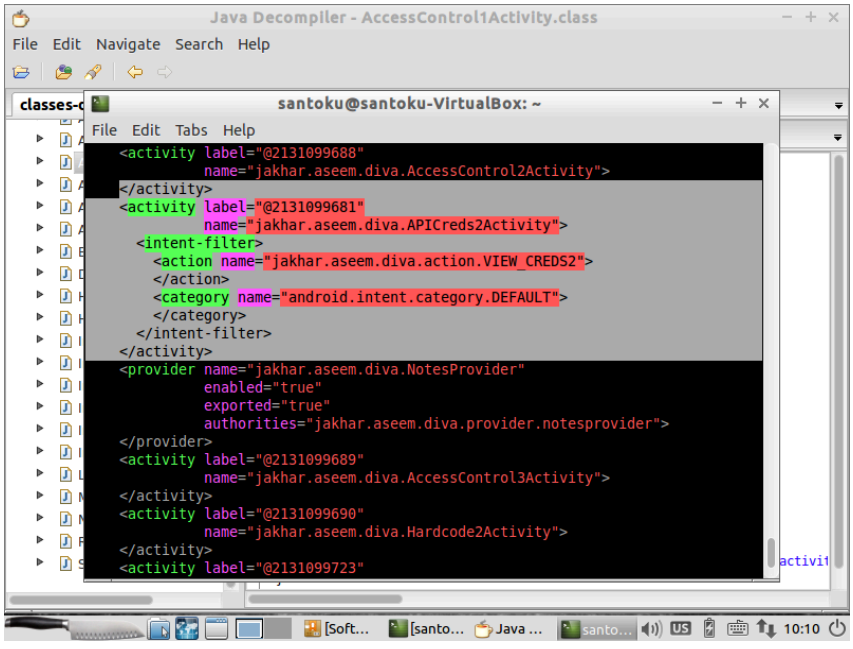


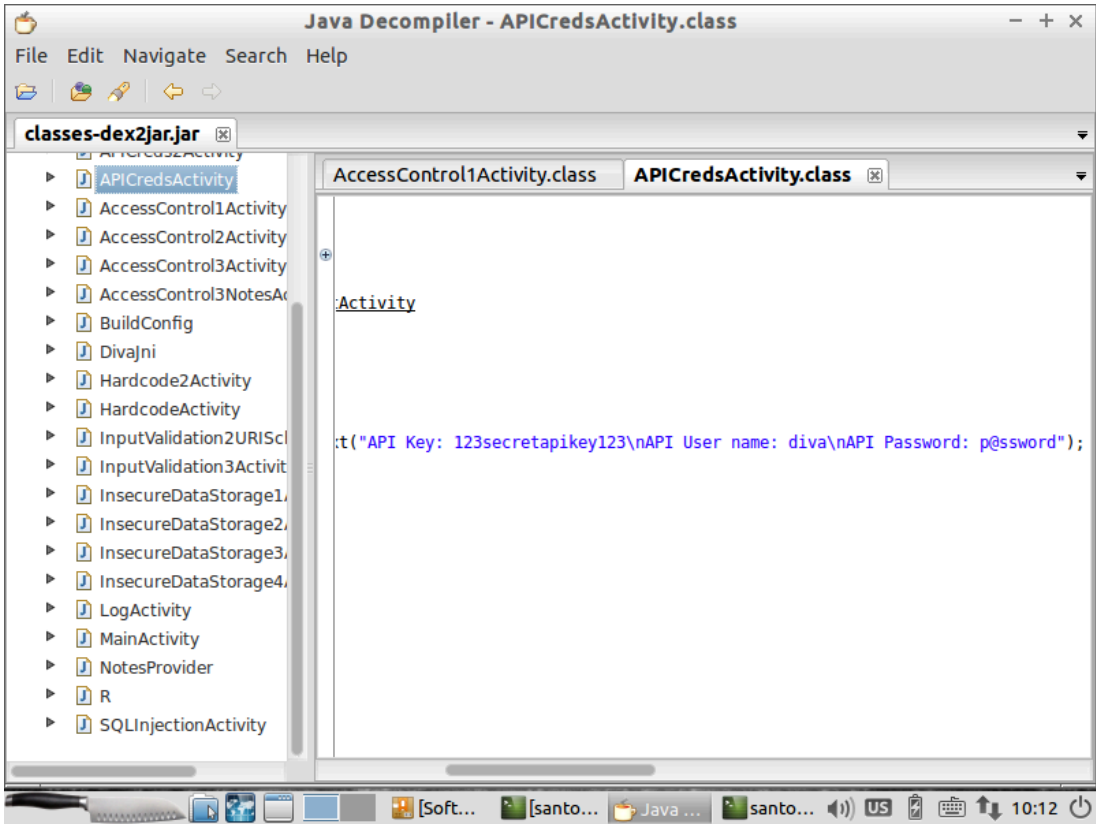


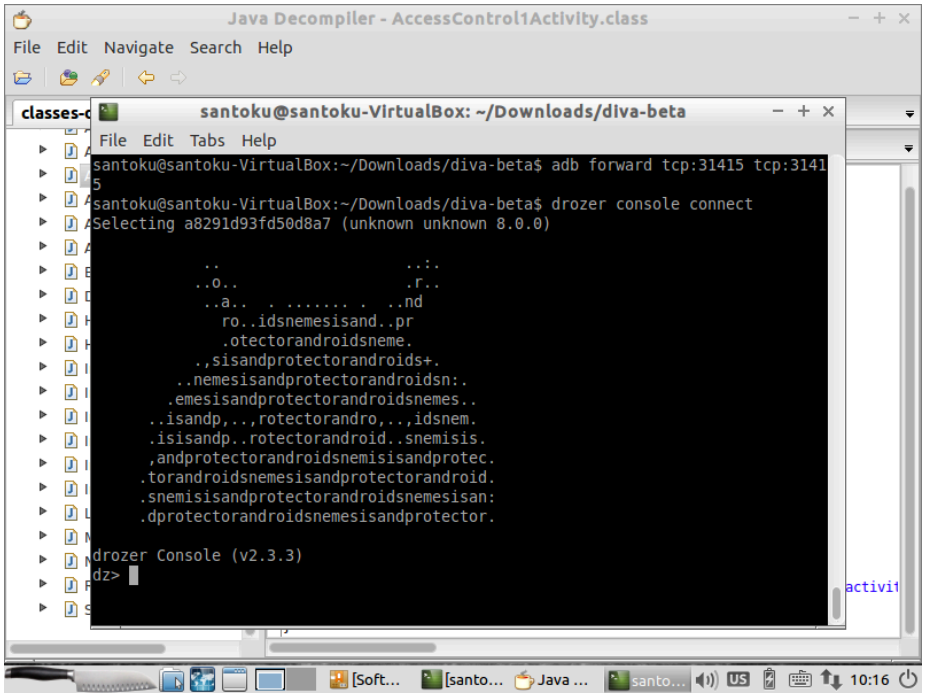

Java Decompiler - AccessControl1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~/Downloads/diva-beta/smali
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads$ ls
diva diva-beta diva-beta.apk
santoku@santoku-VirtualBox:~/Downloads$ cd diva-beta/
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ ls
smali
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ cd smali
santoku@santoku-VirtualBox:~/Downloads/diva-beta/smali$ ls
android jakhar
santoku@santoku-VirtualBox:~/Downloads/diva-beta/smali$
10:08

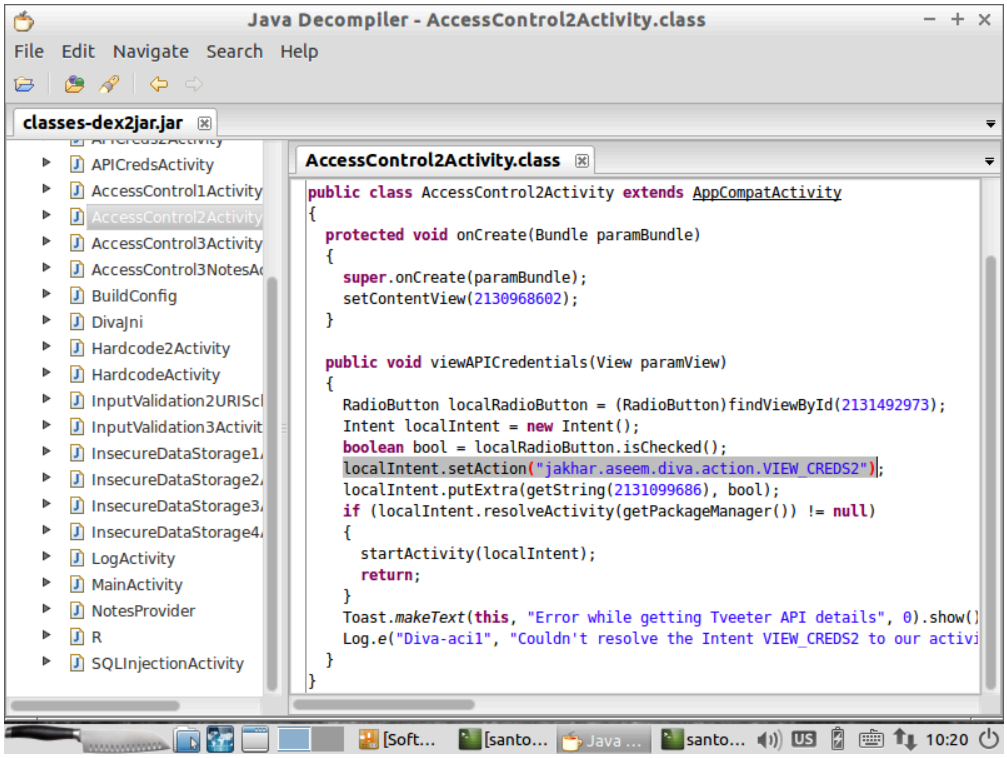

Java Decompiler - AccessControl1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
List of devices attached
192.168.56.105:5555 device
santoku@santoku-VirtualBox:~$ adb forward tcp:31415 tcp:31415
santoku@santoku-VirtualBox:~$ drozer console connect
Selecting a8291d93fd50d8a7 (unknown unknown 8.0.0)
drozer Console (v2.3.3)
dz>
10:09

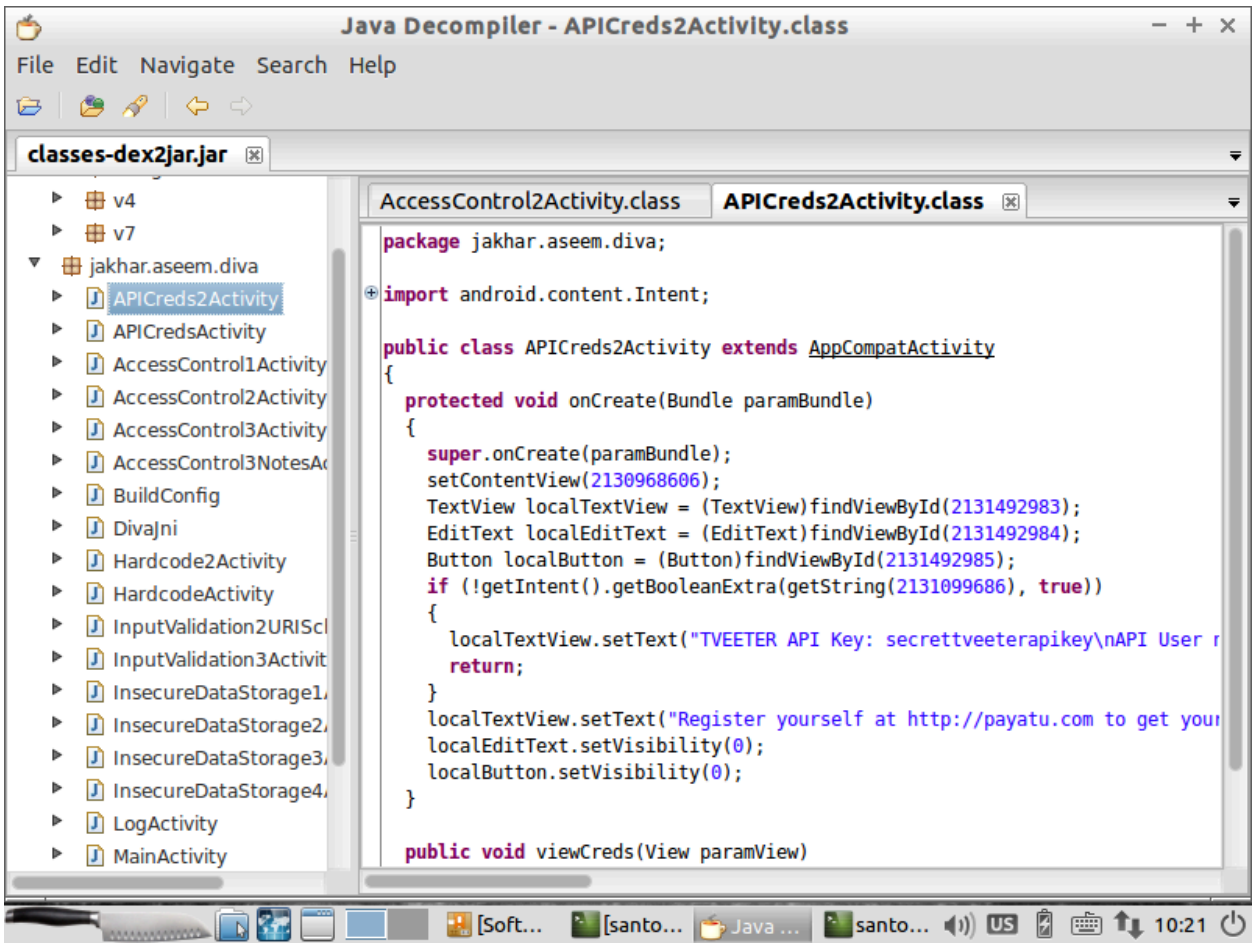

Java Decompiler - AccessControl1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
dialer
scanner.misc.sflagbinaries Find suid/sgid binaries in the given folder (default is /system).
scanner.misc.writablefiles Find world-writable files in the given folder
scanner.provider.finduris Search for content providers that can be queried from our context.
scanner.provider.injection Test content providers for SQL injection vulnerabilities.
scanner.provider.sqltables Find tables accessible through SQL injection vulnerabilities.
scanner.provider.traversal Test content providers for basic directory traversal vulnerabilities.
shell.exec Execute a single Linux command.
shell.send Send an ASH shell to a remote listener.
shell.start Enter into an interactive Linux shell.
tools.file.download Download a File
tools.file.md5sum Get md5 Checksum of file
tools.file.size Get size of file
tools.file.upload Upload a File
tools.setup.busybox Install Busybox.
tools.setup.minimalsu Prepare 'minimal-su' binary installation on the device.
dz> run app.package.manifest jakhar.aseem.diva
10:10


Java Decompiler - AccessControl1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~
File Edit Tabs Help
<activity label="@2131099688"
name="jakhar.aseem.diva.AccessControl2Activity">
</activity>
<activity label="@2131099681"
name="jakhar.aseem.diva.APICreds2Activity">
<intent-filter>
<action name="jakhar.aseem.diva.action.VIEW_CREDS2">
</action>
<category name="android.intent.category.DEFAULT">
</category>
</intent-filter>
</activity>
<provider name="jakhar.aseem.diva.NotesProvider"
enabled="true"
exported="true"
authorities="jakhar.aseem.diva.provider.notesprovider">
</provider>
<activity label="@2131099689"
name="jakhar.aseem.diva.AccessControl3Activity">
</activity>
<activity label="@2131099690"
name="jakhar.aseem.diva.Hardcode2Activity">
</activity>
<activity label="@2131099723"
10:10

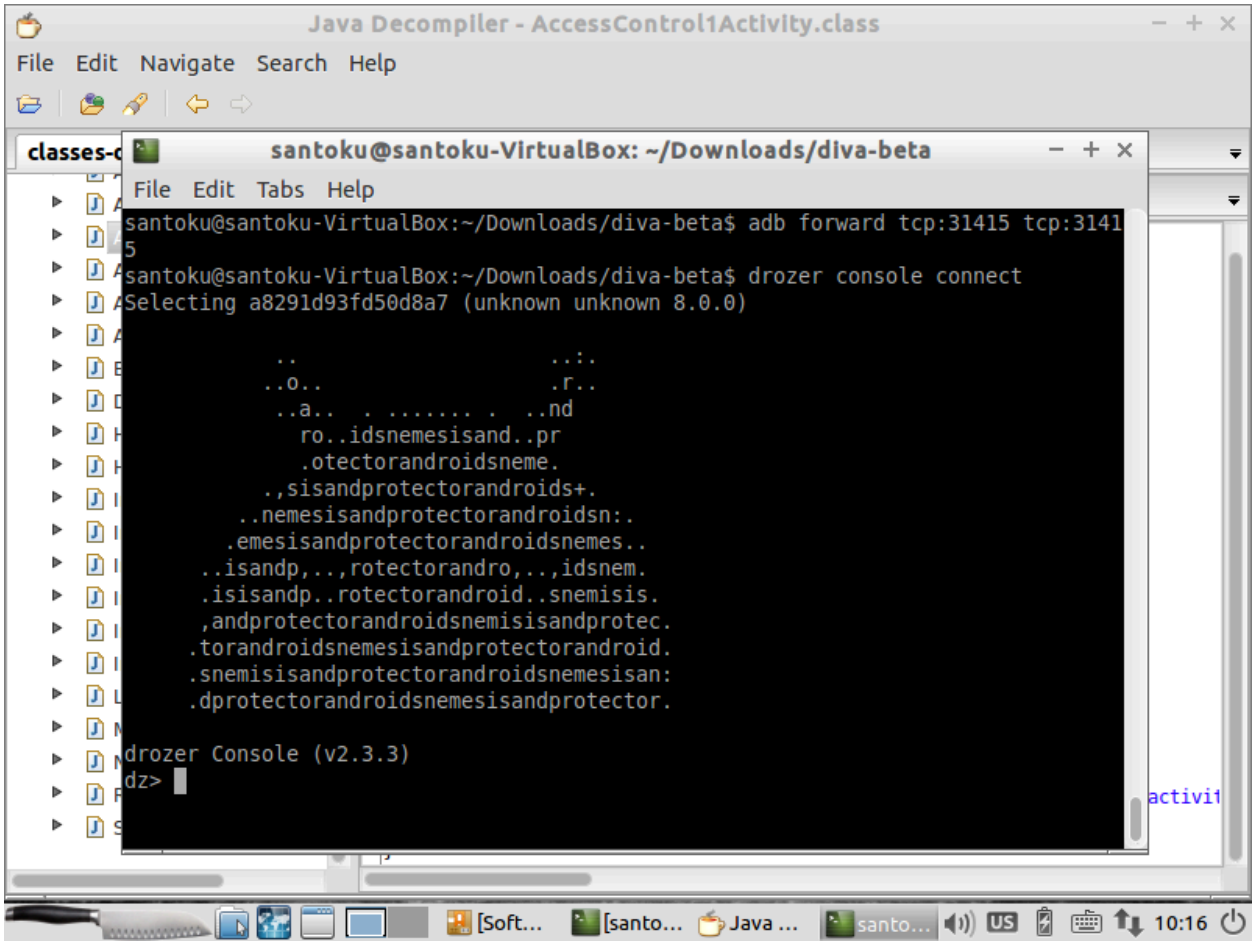

Java Decompiler - APICredsActivity.class
File Edit Navigate Search Help
classes-dex2jar.jar
APICredsActivity
AccessControl1Activity
AccessControl2Activity
AccessControl3Activity
BuildConfig
DivaJni
Hardcode2Activity
HardcodeActivity
LogActivity
MainActivity
NotesProvider
R
SQLInjectionActivity
AccessControl1Activity.class
APICredsActivity.class
:Activity
:t("API Key: 123secretapikey123\nAPI User name: diva\nAPI Password: p@ssword");


Java Decompiler - AccessControl1Activity.class
File Edit Navigate Search Help
santoku@santoku-VirtualBox: ~/Downloads/diva-beta
File Edit Tabs Help
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ adb forward tcp:31415 tcp:31415
santoku@santoku-VirtualBox:~/Downloads/diva-beta$ drozer console connect
Selecting a8291d93fd50d8a7 (unknown unknown 8.0.0)
drozer Console (v2.3.3)
dz>


Java Decompiler - AccessControl2Activity.class
File Edit Navigate Search Help
classes-dex2jar.jar
APICredsActivity
AccessControl1Activity
AccessControl2Activity
AccessControl3Activity
BuildConfig
DivaJni
Hardcode2Activity
HardcodeActivity
InputValidation2URISc
InputValidation3Activit
InsecureDataStorage1
InsecureDataStorage2
InsecureDataStorage3
InsecureDataStorage4
LogActivity
MainActivity
NotesProvider
R
SQLInjectionActivity
AccessControl2Activity.class
public class AccessControl2Activity extends AppCompatActivity
{
protected void onCreate(Bundle paramBundle)
{
super.onCreate(paramBundle);
setContentView(2130968602);
}
public void viewAPICredentials(View paramView)
{
RadioButton localRadioButton = (RadioButton)findViewById(2131492973);
Intent localIntent = new Intent();
boolean bool = localRadioButton.isChecked();
localIntent.setAction("jakhar.aseem.diva.action.VIEW_CREDS2");
localIntent.putExtra(getString(2131099686), bool);
if (localIntent.resolveActivity(getPackageManager()) != null)
{
startActivity(localIntent);
return;
}
Toast.makeText(this, "Error while getting Tveeter API details", 0).show()
Log.e("Diva-aci1", "Couldn't resolve the Intent VIEW_CREDS2 to our activi
}
}
[Soft...
[santo...
Java ...
santo...
US
10:20


Java Decompiler - APICreds2Activity.class
File Edit Navigate Search Help
classes-dex2jar.jar
v4
v7
jakhar.aseem.diva
APICreds2Activity
APICredsActivity
AccessControl1Activity
AccessControl2Activity
AccessControl3Activity
BuildConfig
DivaJni
Hardcode2Activity
HardcodeActivity
InputValidation2URISc
InputValidation3Activit
InsecureDataStorage1
InsecureDataStorage2
InsecureDataStorage3
InsecureDataStorage4
LogActivity
MainActivity
AccessControl2Activity.class
APICreds2Activity.class
package jakhar.aseem.diva;
import android.content.Intent;
public class APICreds2Activity extends AppCompatActivity
{
protected void onCreate(Bundle paramBundle)
{
super.onCreate(paramBundle);
setContentView(2130968606);
TextView localTextView = (TextView)findViewById(2131492983);
EditText localEditText = (EditText)findViewById(2131492984);
Button localButton = (Button)findViewById(2131492985);
if (!getIntent().getBooleanExtra(getString(2131099686), true))
{
localTextView.setText("TVEETER API Key: secrettveeterapikey\nAPI User r
return;
}
localTextView.setText("Register yourself at http://payatu.com to get your
localEditText.setVisibility(0);
localButton.setVisibility(0);
}
public void viewCreds(View paramView)
[Soft...
[santo...
Java ...
santo...
US
10:21

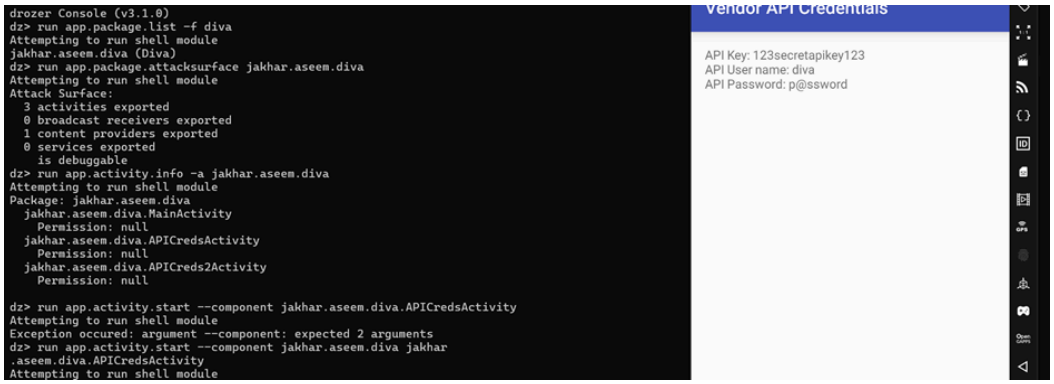
Configuration of Drozer



Security Auditing of DIVA using Drozer

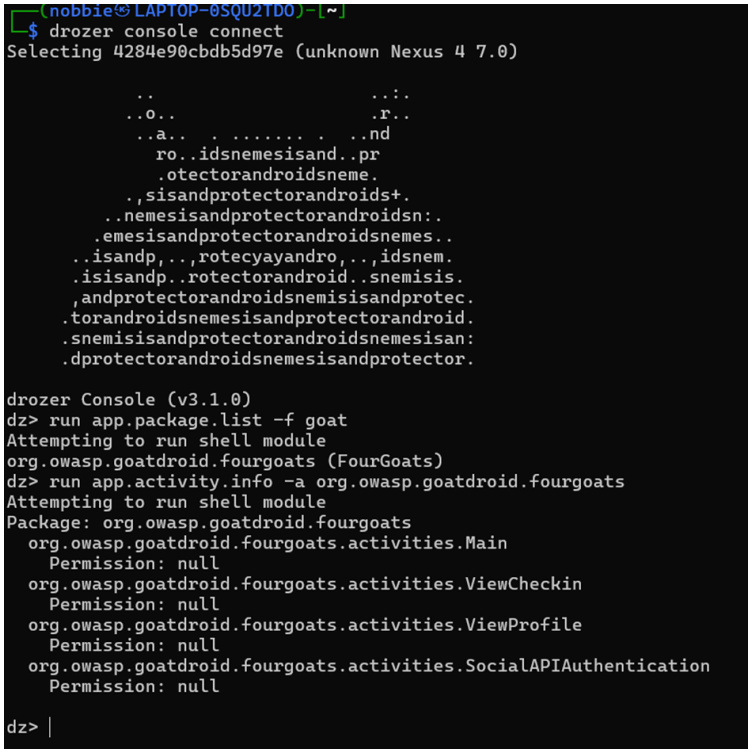
```
drozer Console (v3.1.0)
dz> run app.package.list -f diva
Attempting to run shell module
jakhar.aseem.diva (Diva)
dz> run app.package.attacksurface jakhar.aseem.diva
Attempting to run shell module
Attack Surface:
  3 activities exported
  0 broadcast receivers exported
  1 content providers exported
  0 services exported
    is debuggable
dz>
```

```
z> run app.activity.info -a jakhar.aseem.diva
ttempting to run shell module
ackage: jakhar.aseem.diva
 jakhar.aseem.diva.MainActivity
   Permission: null
 jakhar.aseem.diva.APICredsActivity
   Permission: null
 jakhar.aseem.diva.APICreds2Activity
   Permission: null

z> run app.activity.start --component jakhar.aseem.diva.APICre
sActivity
ttempting to run shell module
xception occured: argument --component: expected 2 arguments
z> run app.activity.start --component jakhar.aseem.diva jakhar
aseem.diva.APICredsActivity
```

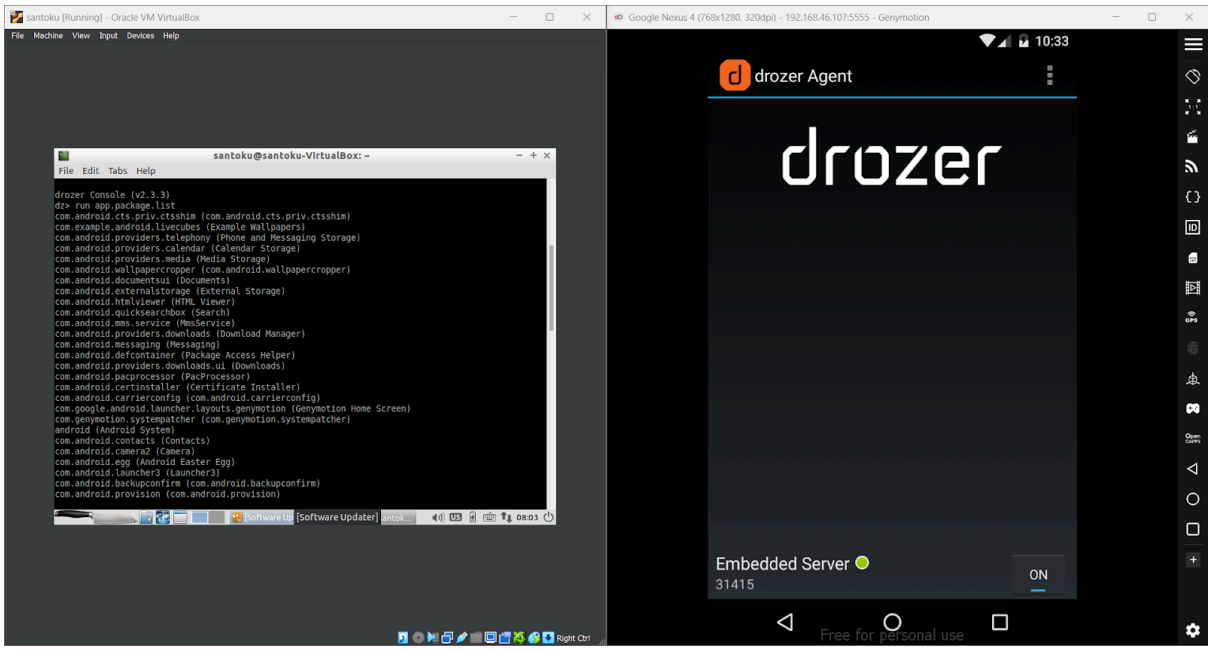


Security Auditing of Insecure Bank using Drozer

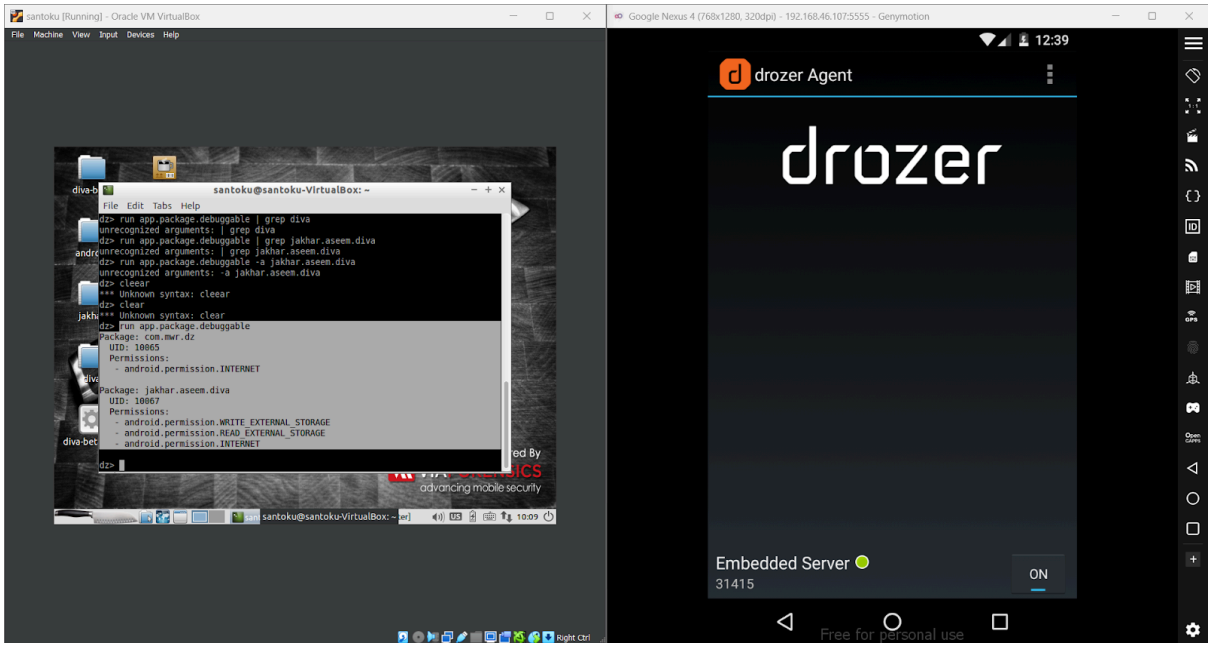
Security Auditing of OWASP GoatDroid using Drozer



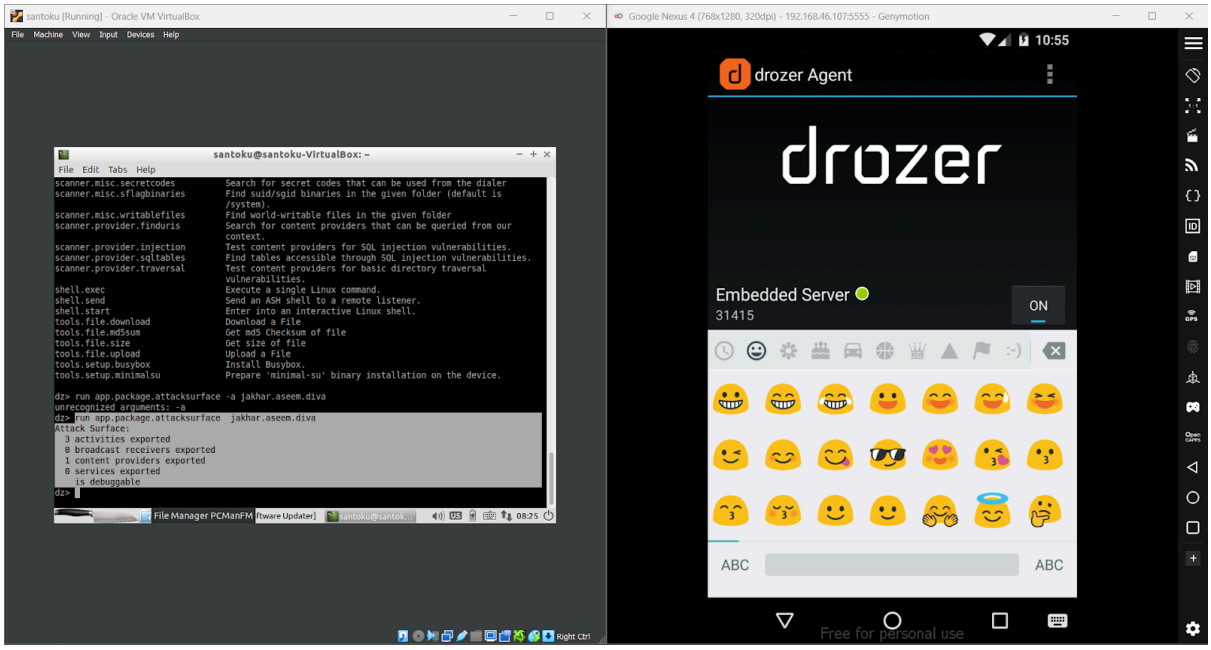
Package listing of android app using app.package.list



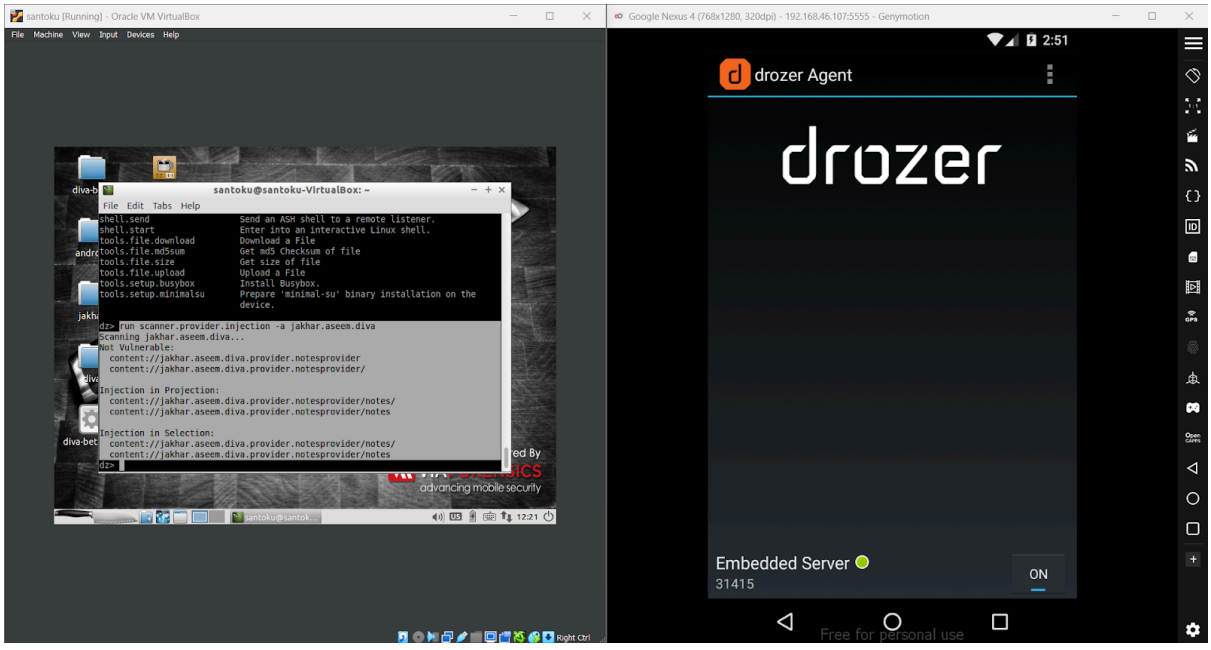
Find Debuggable android application

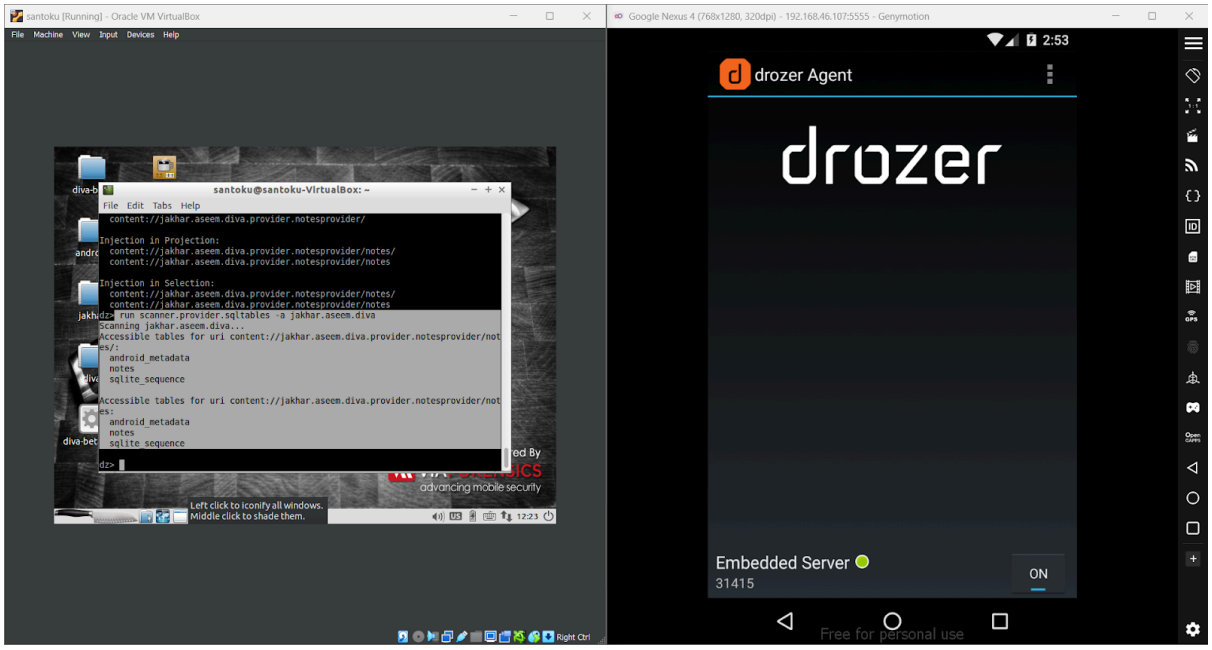


Find attack surface of DIVA

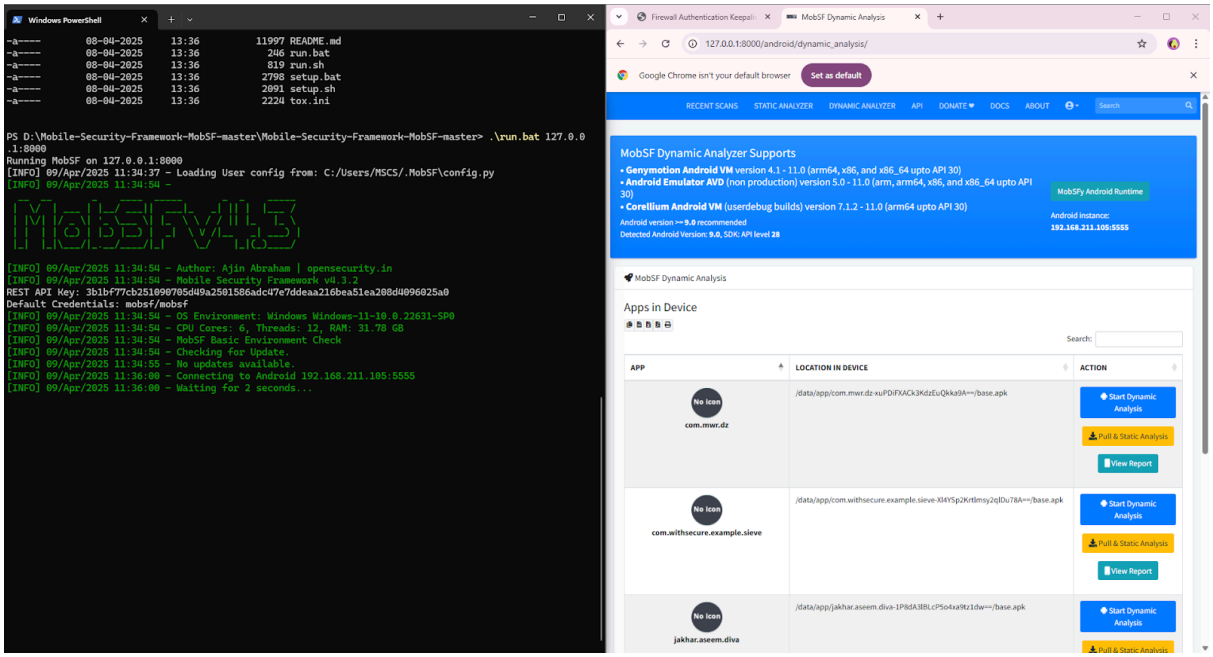


SQL Injection Vulnerability of DIVA using Drozer Modules

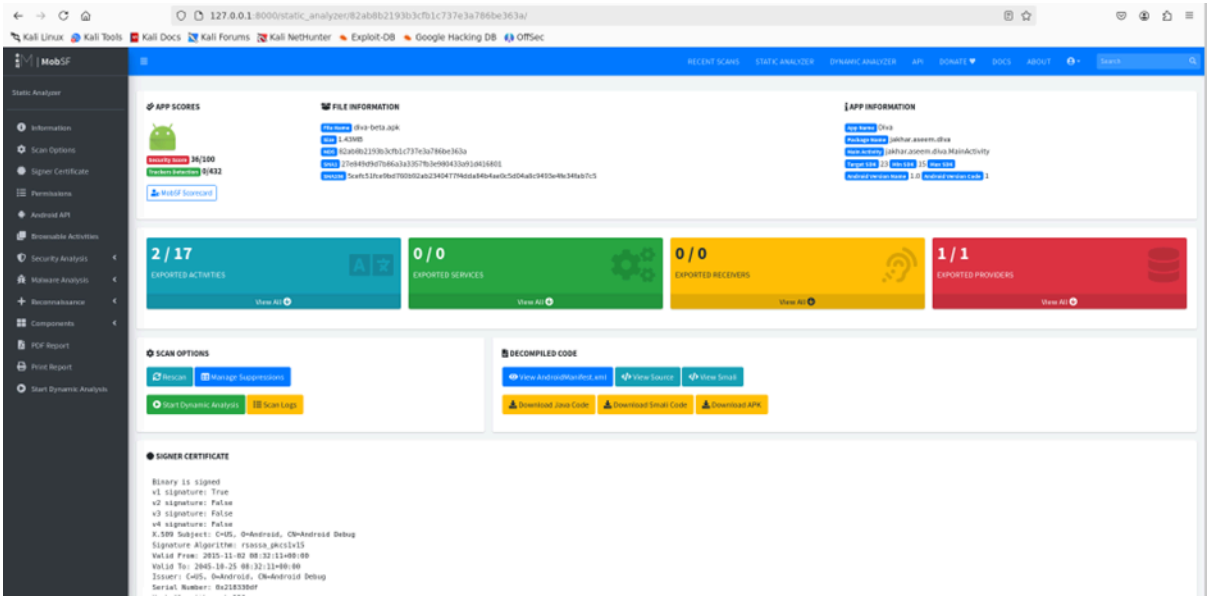




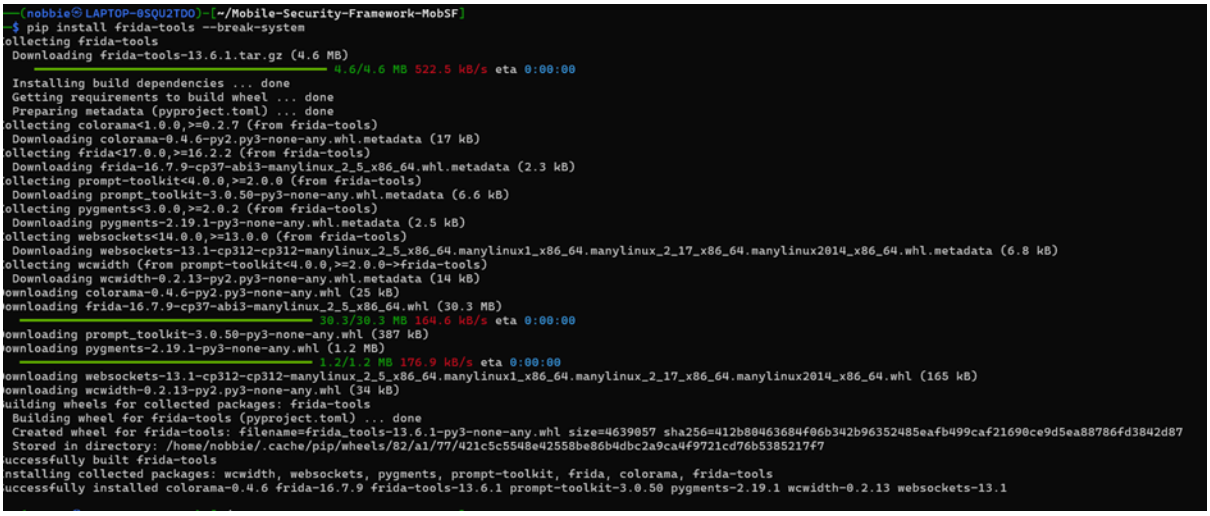
Configuration of MobSF (Mobile Security Framework)



Security Auditing using MobSF (Mobile Security Framework)



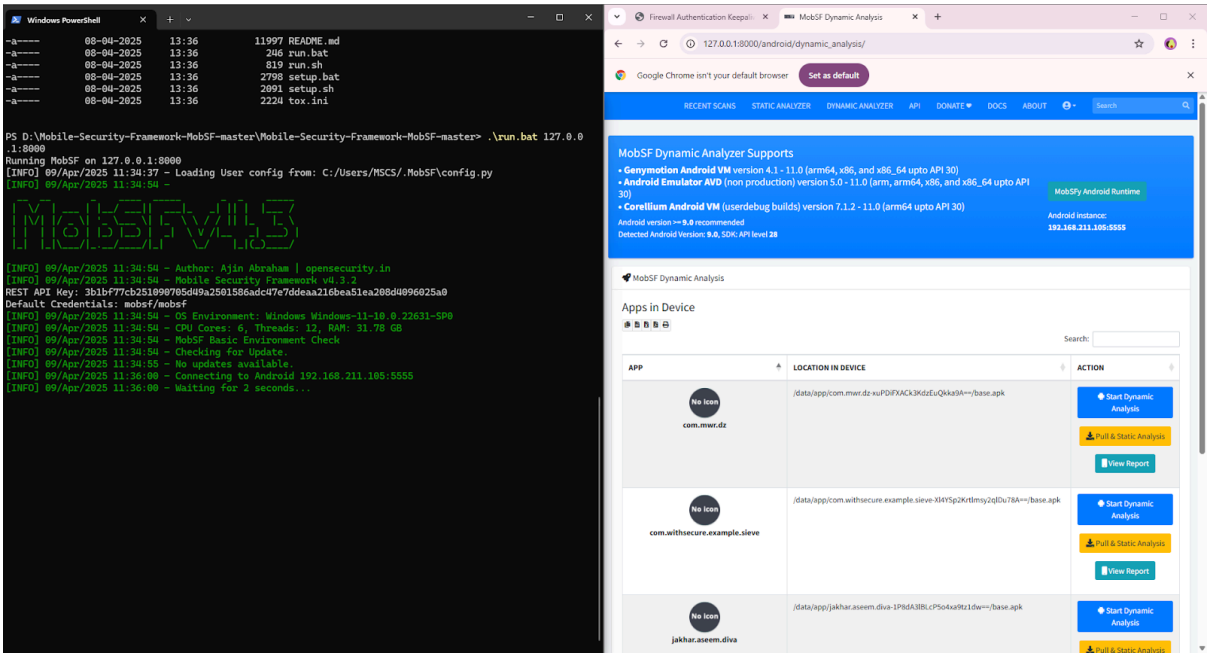
Configuration of Frida

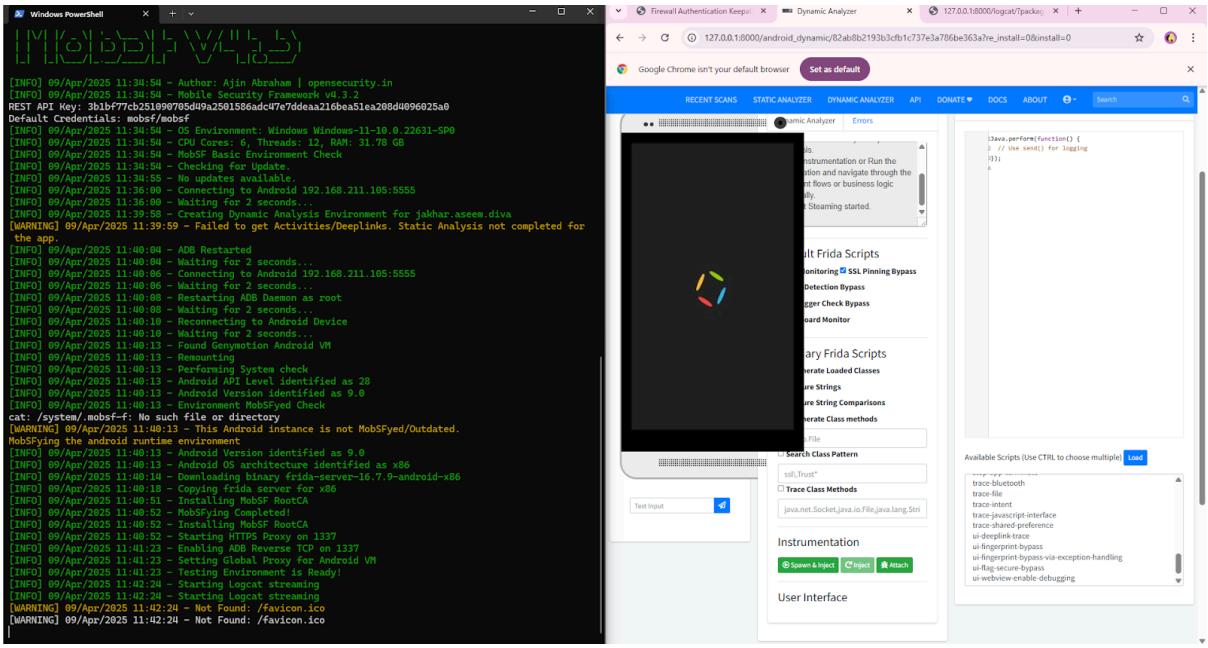


Testing and Evaluation of Android App using Frida

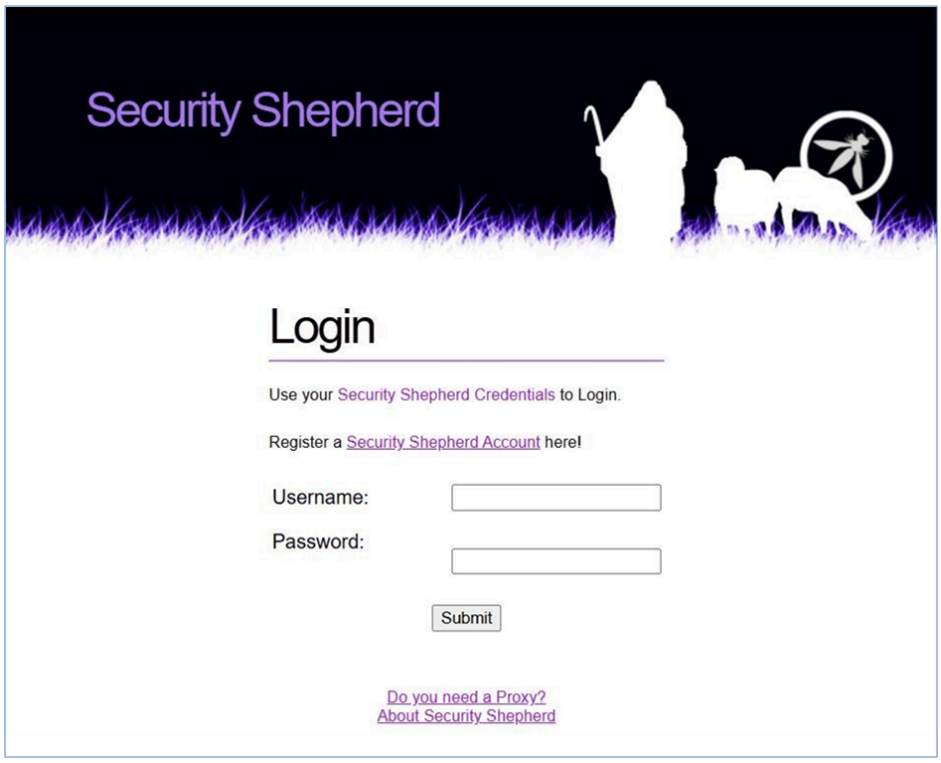
```
┌──(nobbie㉿LAPTOP-0SQU2TDO)-[~/Mobile-Security-Framework-MobSF]
└─$ frida -U -n Diva
     ____
    / _  |   Frida 16.7.9 - A world-class dynamic instrumentation toolkit
   | (_| |
    > _  |   Commands:
   /_/ |_|       help      -> Displays the help system
   . . . .       object?   -> Display information about 'object'
   . . . .       exit/quit -> Exit
   . . . .
   . . . .   More info at https://frida.re/docs/home/
   . . . .
   . . . .   Connected to Nexus 4 (id=192.168.242.102:5555)

[Nexus 4::Diva ]-> Java.perform(function () {
    var Log = Java.use("android.util.Log");
    Log.d.implementation = function(tag, msg) {
        console.log("🔥 Log.d called: " + tag + " → " + msg);
        return this.d(tag, msg);
    };
});
```

Dynamic Analysis using MobSF and Frida



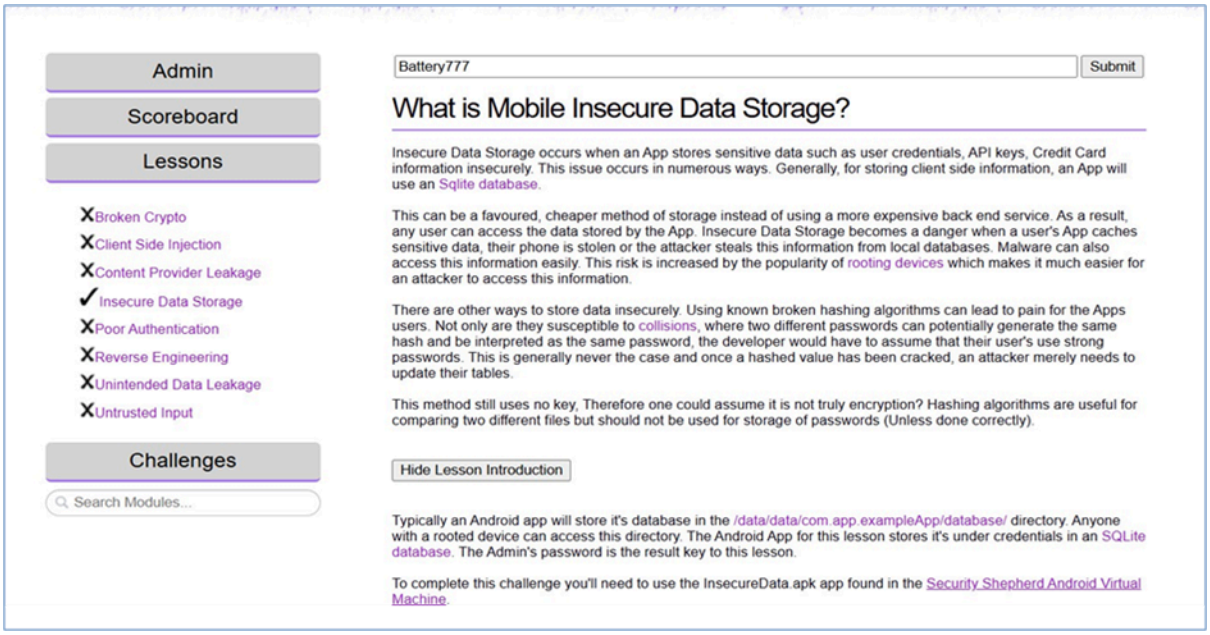


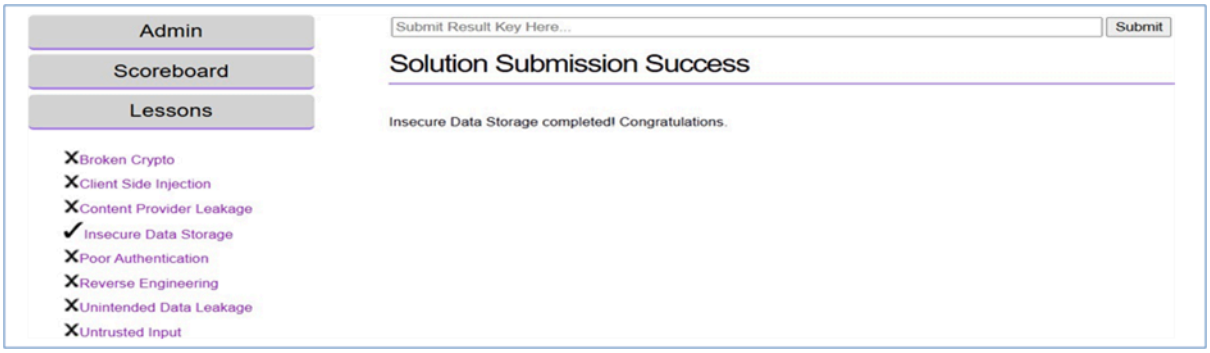
Configuration of OWASP Security Shepherd – Mobile Security platform



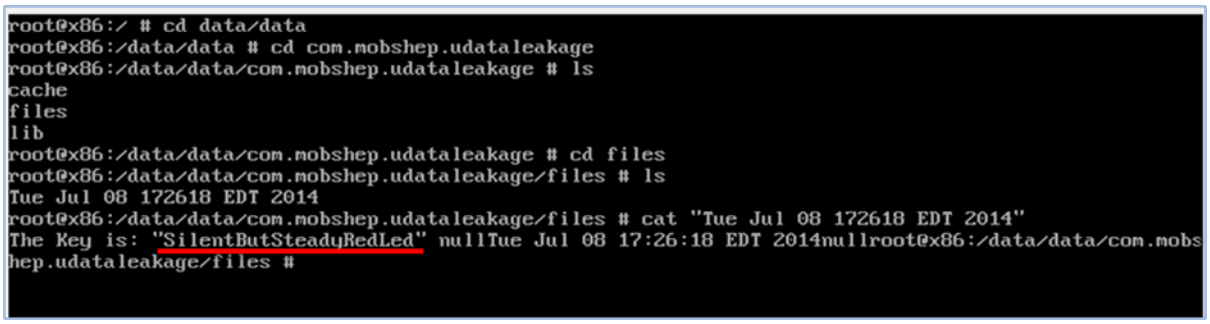
Practical: 01 OWASP Security Shepherd – Mobile Security platform

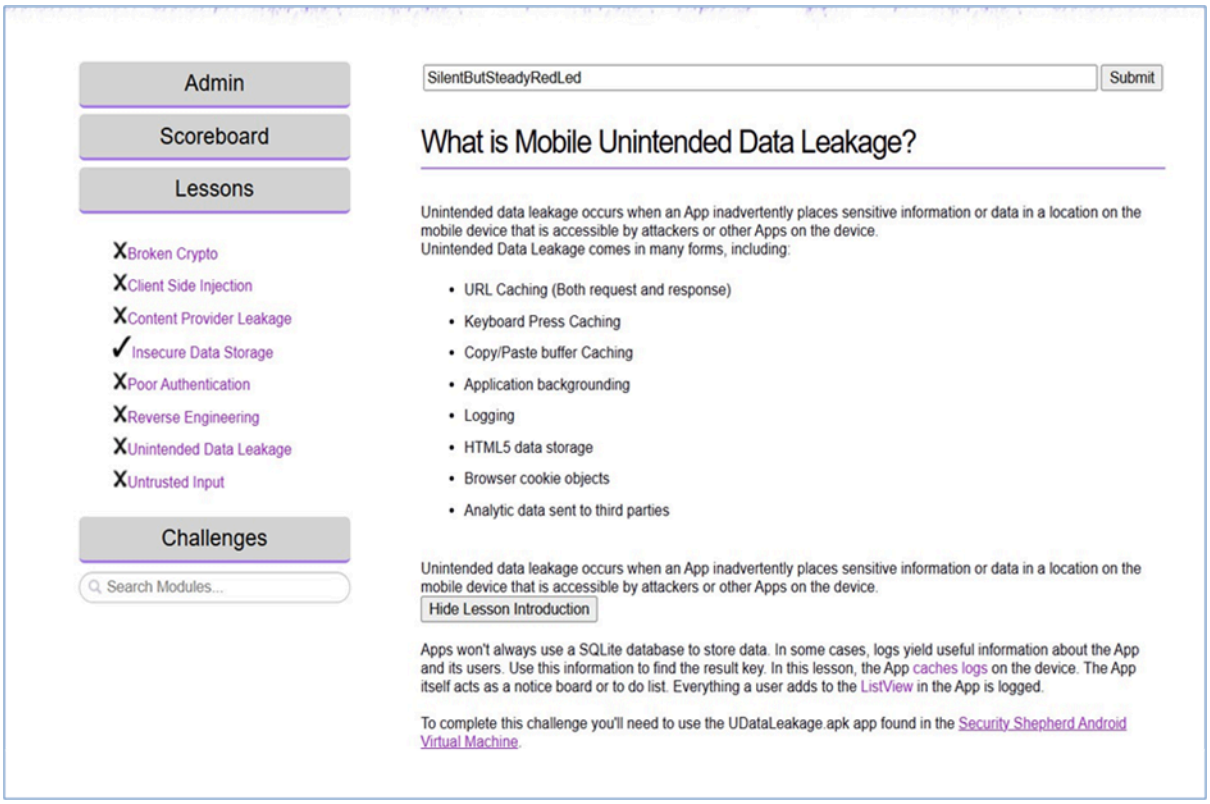
```
root@x86:/ # cd data/data
root@x86:/data/data # cd com.mobshep.insecuredata
root@x86:/data/data/com.mobshep.insecuredata # cd databases
root@x86:/data/data/com.mobshep.insecuredata/databases # ls
Members
Members-journal
root@x86:/data/data/com.mobshep.insecuredata/databases # cat Me
Members         Members-journal
root@x86:/data/data/com.mobshep.insecuredata/databases # cat Members
=■=h■'tableMembersMembersCREATE TABLE Members (id integer primary key, name VARCHAR, password VARCHA
■■!AdminBattery777root@x86:/data/data/com.mobshep.insecuredata/databases # ocale TEXT)
```

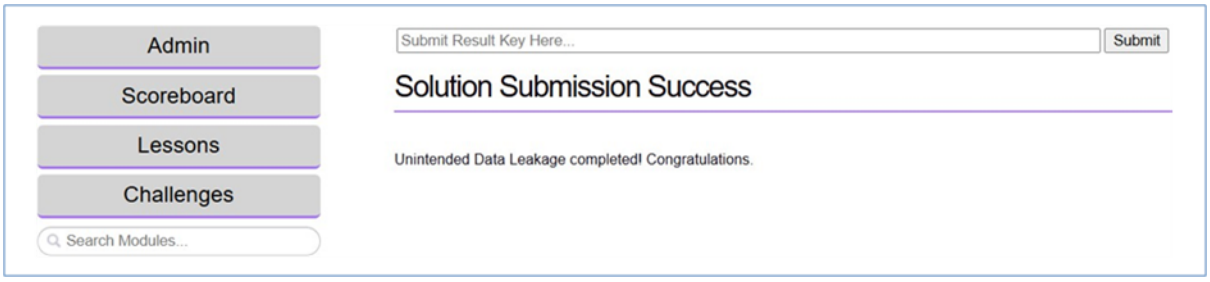




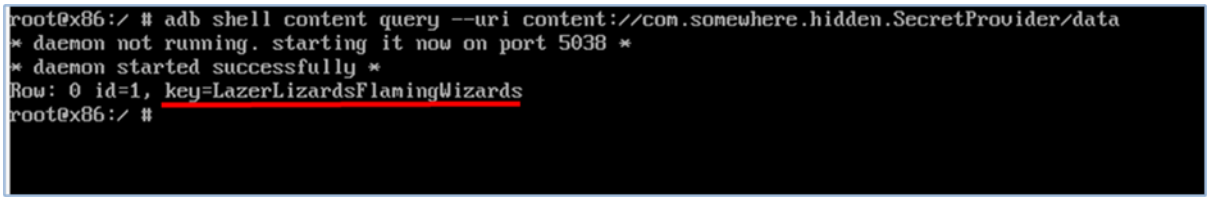
Practical: 02 OWASP Security Shepherd – Mobile Security platform

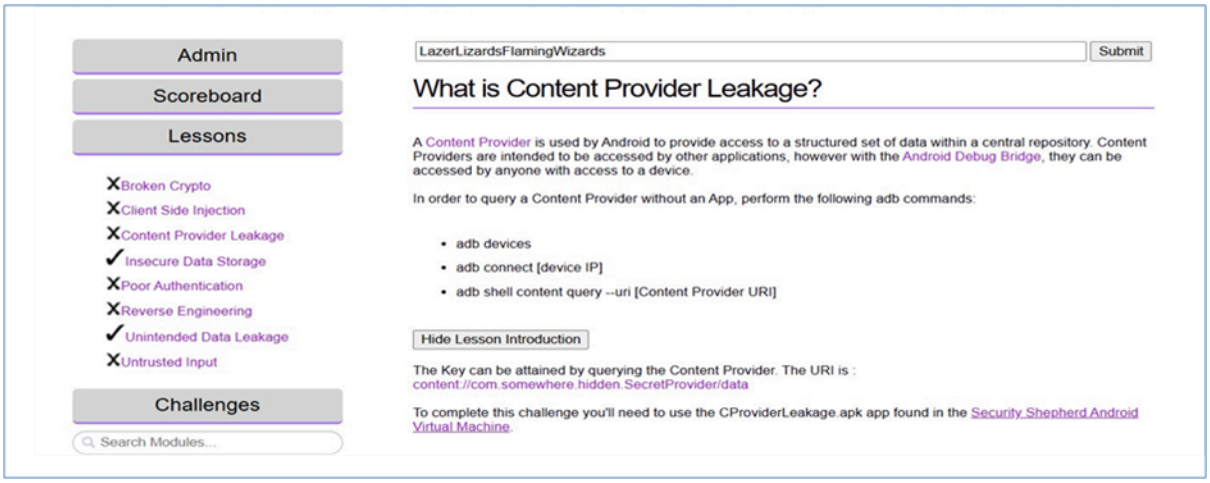


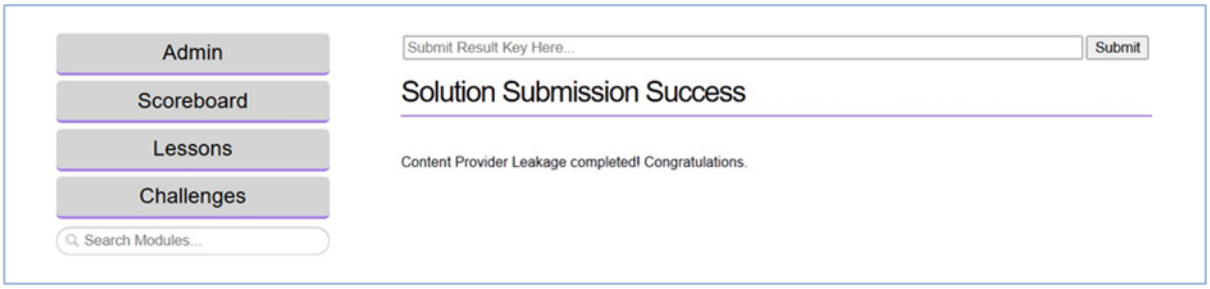




Practical: 03 OWASP Security Shepherd – Mobile Security platform



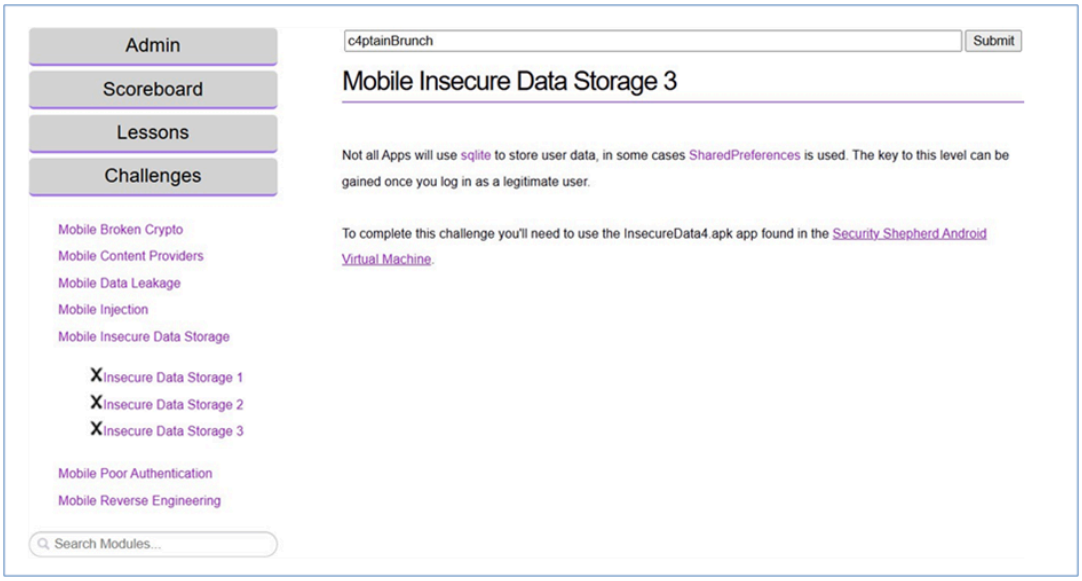




Practical: 04 OWASP Security Shepherd – Mobile Security platform

```
root@x86:/ # cd data/data
root@x86:/data/data # cd com.mobshep.insecuredata3
root@x86:/data/data/com.mobshep.insecuredata3 # ls
cache
lib
shared_prefs
root@x86:/data/data/com.mobshep.insecuredata3 # cd shared_prefs
root@x86:/data/data/com.mobshep.insecuredata3/shared_prefs # ls
AppData.xml
Saved Data.xml
root@x86:/data/data/com.mobshep.insecuredata3/shared_prefs # cat Saved Data.xml
/system/bin/sh: cat: Saved: No such file or directory
/system/bin/sh: cat: Data.xml: No such file or directory
t Saved\ Data.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="Username">Tony</string>
    <string name="Password">qazwsx4562</string>
</map>
root@x86:/data/data/com.mobshep.insecuredata3/shared_prefs #
```


5:38
The Key is: c4ptainBrunch


Admin
Scoreboard
Lessons
Challenges
Mobile Broken Crypto
Mobile Content Providers
Mobile Data Leakage
Mobile Injection
Mobile Insecure Data Storage
XInsecure Data Storage 1
XInsecure Data Storage 2
XInsecure Data Storage 3
Mobile Poor Authentication
Mobile Reverse Engineering
Search Modules...
c4ptainBrunch
Submit
Mobile Insecure Data Storage 3
Not all Apps will use sqlite to store user data, in some cases SharedPreferences is used. The key to this level can be gained once you log in as a legitimate user.
To complete this challenge you'll need to use the InsecureData4.apk app found in the Security Shepherd Android Virtual Machine.