

**RAO ALI NAWAZ**  
**FA22A-222666**  
**DIGITAL FORENSICS LAB TASK 8**

## Androgoat Apk

```
→ MyTest git:(master) ls
AndroGoat.apk  AndroGoatInvoice.txt  AndroGoat_without_network_secutity_config.apk
→ MyTest git:(master) ls -l AndroGoat.apk
-rw-r--r-- 1 ran ran 2765026 May 15 05:03 AndroGoat.apk
→ MyTest git:(master)
```

## Using apktool to extract files

```
→ MyTest git:(master) apktool d AndroGoat.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.7.0-dirty on AndroGoat.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/ran/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
→ MyTest git:(master) X ls -la
total 5304
drwxr-xr-x 4 ran ran    4096 May 15 05:04 .
drwxr-xr-x 3 ran ran    4096 May 15 05:02 ..
drwxr-xr-x 7 ran ran    4096 May 15 05:05 AndroGoat
-rw-r--r-- 1 ran ran 2765026 May 15 05:03 AndroGoat.apk
-rw-r--r-- 1 ran ran     72 May 15 05:03 AndroGoatInvoice.txt
-rw-r--r-- 1 ran ran 2636197 May 15 05:03 AndroGoat_without_network_secutity_config.apk
drwxr-xr-x 8 ran ran    4096 May 15 05:03 .git
→ MyTest git:(master) X cd AndroGoat
→ AndroGoat git:(master) X ls
AndroidManifest.xml  apktool.yml  kotlin  original  res  smali  unknown
→ AndroGoat git:(master) X
```

## AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" package="owasp.sat.agoat">
    <uses-sdk android:minSdkVersion="18" android:targetSdkVersion="20"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <application android:theme="@style/AppTheme" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:debuggable="true" android:allowBackup="true" android:supportRtl="true">
        <activity android:name="owasp.sat.agoat.SplashActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/app_name" android:name="owasp.sat.agoat.MainActivity"/>
        <activity android:label="@string/root" android:name="owasp.sat.agoat.RootDetectionActivity"/>
        <activity android:label="@string/logging" android:name="owasp.sat.agoat.InsecureLoggingActivity"/>
        <activity android:label="@string/xss" android:name="owasp.sat.agoat.XSSActivity"/>
        <activity android:label="@string/sql" android:name="owasp.sat.agoat.SqliInjectionActivity"/>
        <activity android:label="@string/api" android:name="owasp.sat.agoat.InsecureStorageSharedPrefs"/>
        <activity android:label="@string/tempFile" android:name="owasp.sat.agoat.InsecureStorageTempActivity"/>
        <activity android:label="@string/activity" android:name="owasp.sat.agoat.AccessControlIssueActivity"/>
        <activity android:label="@string/activity" android:name="owasp.sat.agoat.AccessControlViewActivity">
            <intent-filter>
                <action android:name="android.intent.action.VIEW"/>
                <category android:name="android.intent.category.DEFAULT"/>
                <data android:scheme="androgoat" android:host="vulnapp"/>
            </intent-filter>
        </activity>
        <receiver android:name="owasp.sat.agoat.ShowDataReceiver" android:enabled="true" android:exported="true">
            <activity android:label="@string/hardcode" android:name="owasp.sat.agoat.HardCodeActivity"/>
        </receiver>
        <activity android:label="@string/sql" android:name="owasp.sat.agoat.InsecureStorageSQLiteActivity"/>
        <activity android:label="@string/app2" android:name="owasp.sat.agoat.InsecureStorageSharedPrefs2Activity"/>
        <activity android:label="@string/network" android:name="owasp.sat.agoat.TrafficActivity"/>
        <activity android:name="owasp.sat.agoat.ContentProviderActivity"/>
        <activity android:label="@string/emulator" android:name="owasp.sat.agoat.EmulatorDetectionActivity"/>
        <activity android:label="@string/edcard" android:name="owasp.sat.agoat.InsecureStorageEdCardActivity"/>
        <activity android:label="@string/wbviewAccess" android:name="owasp.sat.agoat.InputValidationsWebViewURLActivity"/>
        <activity android:label="@string/oscmd" android:name="owasp.sat.agoat.InputValidationsOSCommandInjectionMain2Activity"/>
        <service android:name="owasp.sat.agoat.DownloadInvoiceService" android:enabled="true" android:exported="true"/>
        <activity android:label="@string/BinaryPatching" android:name="owasp.sat.agoat.BinaryPatchingActivity"/>
        <activity android:label="@string/clipboard" android:name="owasp.sat.agoat.ClipboardActivity"/>
        <activity android:label="@string/InsecureStorage" android:name="owasp.sat.agoat.InsecureStorageActivity"/>
        <activity android:label="@string/SideChannelLeakage" android:name="owasp.sat.agoat.SideChannelDataLeakageActivity"/>
        <activity android:label="@string/InputValidations" android:name="owasp.sat.agoat.InputValidationsActivity"/>
        <activity android:label="@string/dict" android:name="owasp.sat.agoat.KeyboardCacheActivity"/>
        <meta-data android:name="android.support.VERSION" android:value="26.1.0"/>
        <meta-data android:name="android.arch.lifecycle.VERSION" android:value="27.0.0-SNAPSHOT"/>
    </application>
</manifest>
```

## Debuggable

on="@mipmap/ic\_launcher" android:debuggable="true" android:allowBackup="true" android:supportRtl="true" android

## Network security

```
<?xml version="1.0" encoding="utf-8"?>
<network-security-config>
    <base-config cleartextTrafficPermitted="true">
        <trust-anchors>
            <certificates src="system"/>
            <certificates src="user"/>
        </trust-anchors>
    </base-config>
</network-security-config>
```

## Main Activity



RECENT SCANS

STATIC ANALYZER

DYNAMIC ANALYZER

API


DONATE

DOCS

ABOUT

Search

APP SCORES



Security Score43/100

Trackers Detection0/432

MobSF Scorecard

FILE INFORMATION

File Name

AndroGoat.apk

Size

2.64MB

MDS

8d351e8fc20c340cf03ff52b0ef125ae

SHA1

ea96f4adc27083696a449b1c6e5cd612a2cf0f5c

SHA256

347a8b0d0b8466a25ccc67d3d2cbb5d69ef2b0de4d4f278b6bee357c7ba5f63b

APP INFORMATION

App Name

AndroGoat - Insecure App (Kotlin)

Package Name

owasp.sat.agoat

Main Activity

owasp.sat.agoat.SplashActivity

Target SDK

26

Min SDK

18

Max SDK

Android Version Name

1.0

Android Version Code

1

1 / 25

EXPORTED ACTIVITIES

View All

1 / 1

EXPORTED SERVICES

View All

1 / 1

EXPORTED RECEIVERS

View All

0 / 0

EXPORTED PROVIDERS

View All

SCAN OPTIONS

Rescan

Manage Suppressions

Start Dynamic Analysis

Scan Logs

DECOMPILED CODE

View AndroidManifest.xml

View Source

View Smali

Download Java Code

Download Smali Code

Download APK

SIGNER CERTIFICATE

Binary is signed  
v1 signature: True  
v2 signature: True  
v3 signature: False  
v4 signature: False  
X.509 Subject: CN=Android Debug, O=Android, C=US

RECENT SCANS

STATIC ANALYZER

DYNAMIC ANALYZER

API

DONATE

DOCS

ABOUT

Search

ANDROID API

API

Crypto

Execute OS Command

Get System Service

Inter Process Communication

Java Reflection

Local File I/O Operations

Message Digest

Set or Read Clipboard data

Starting Activity

Starting Service

FILES

Show Files

Show Files

Show Files

Show Files

Show Files

Show Files

Show Files

Show Files

Show Files

Show Files

Showing 1 to 10 of 12 entries

Previous

BROWSABLE ACTIVITIES

ACTIVITY

INTENT

RECENT SCANS   STATIC ANALYZER   DYNAMIC ANALYZER   API   DONATE ▼   DOCS   ABOUT   Search

### FIREBASE DATABASE ANALYSIS

Search:

TITLE	SEVERITY	DESCRIPTION
Open Firebase database	high	The Firebase database at <a href="https://androgoat-42597.firebaseio.com/.json">https://androgoat-42597.firebaseio.com/.json</a> is exposed to internet without any authentication

Showing 1 to 1 of 1 entries

Previous

### MALWARE LOOKUP

[VirusTotal Report](#) | [Triage Report](#) | [MetaDefender Report](#) | [Hybrid Analysis Report](#)

### APKID ANALYSIS

Search:

DEX	DETECTIONS
classes.dex	<div><div><div><div><div></div><div></div><div></div><div></div><div></div></div><div></div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div><div><div></div><div></div><div></div><div></div><div></div></div></div> <div>Search: <input type="text"/></div>

FINDINGS

DETAILS

← → ↻ 🏠 <https://androgoat-42597.firebaseio.com/.json>

JSON   Raw Data   Headers

Save   Copy   Collapse All   Expand All   Filter JSON

```
password: "androgoat"
user: "androgoat"
```

Res folder

```

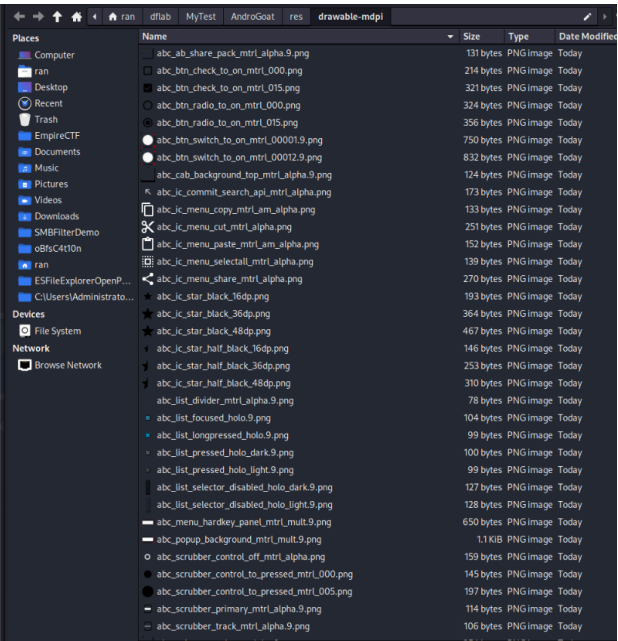
→ AndroGoat git:(master) X cd res
→ res git:(master) X ls
anim                drawable-v21        mipmap-xhdpi        values-ca            values-fi            values-it            values-lt
color               drawable-v23        mipmap-xxhdpi       values-cs            values-fr            values-iw            values-lv
color-v23           drawable-v24        mipmap-xxxhdpi      values-da            values-fr-rCA        values-ja            values-mk
drawable            drawable-xhdpi      values              values-de            values-gl            values-ka            values-ml
drawable-anydpi-v21 drawable-xxhdpi      values-af            values-el            values-gu            values-kk            values-mn
drawable-hdpi       drawable-xxxhdpi    values-am            values-en-rAU        values-h720dp        values-km            values-mr
drawable-ldpi       layout              values-ar            values-en-rGB        values-hdpi          values-kn            values-ms
drawable-ldrtl-hdpi layout-v21           values-az            values-en-rIN        values-hi            values-ko            values-my
drawable-ldrtl-mdpi layout-v22           values-be            values-es-rIN        values-hr            values-ky            values-nb
drawable-ldrtl-xhdpi layout-v26           values-bg            values-es-rUS        values-hu            values-land          values-ne
drawable-ldrtl-xxhdpi mipmap-anydpi-v26   values-bn            values-et            values-hy            values-large          values-nigh
drawable-ldrtl-xxxhdpi mipmap-hdpi         values-bs            values-eu            values-in            values-ldltr-v21     values-nl
drawable-mdpi       mipmap-mdpi        values-b+sr+Latn    values-fa            values-is            values-lo            values-pa
→ res git:(master) X

```

```

→ AndroGoat git:(master) X ls
AndroidManifest.xml apktool.yml kotlin original res smali unknown
→ AndroGoat git:(master) X cd res
→ res git:(master) X ls
anim                drawable-v21        mipmap-xhdpi        values-ca            values-fi            values-it            values-lt
color               drawable-v23        mipmap-xxhdpi       values-cs            values-fr            values-iw            values-lv
color-v23           drawable-v24        mipmap-xxxhdpi      values-da            values-fr-rCA        values-ja            values-mk
drawable            drawable-xhdpi      values              values-de            values-gl            values-ka            values-ml
drawable-anydpi-v21 drawable-xxhdpi      values-af            values-el            values-gu            values-kk            values-mn
drawable-hdpi       drawable-xxxhdpi    values-am            values-en-rAU        values-h720dp        values-km            values-mr
drawable-ldpi       layout              values-ar            values-en-rGB        values-hdpi          values-kn            values-ms
drawable-ldrtl-hdpi layout-v21           values-az            values-en-rIN        values-hi            values-ko            values-my
drawable-ldrtl-mdpi layout-v22           values-be            values-es-rIN        values-hr            values-ky            values-nb
drawable-ldrtl-xhdpi layout-v26           values-bg            values-es-rUS        values-hu            values-land          values-ne
drawable-ldrtl-xxhdpi mipmap-anydpi-v26   values-bn            values-et            values-hy            values-large          values-nigh
drawable-ldrtl-xxxhdpi mipmap-hdpi         values-bs            values-eu            values-in            values-ldltr-v21     values-nl
drawable-mdpi       mipmap-mdpi        values-b+sr+Latn    values-fa            values-is            values-lo            values-pa
→ res git:(master) X cd drawable-mdpi
→ drawable-mdpi git:(master) X ls
abc_ab_share_pack_mtrl_alpha.9.png      abc_ic_star_half_black_36dp.png
abc_btn_check_to_on_mtrl_000.png         abc_ic_star_half_black_48dp.png
abc_btn_check_to_on_mtrl_015.png         abc_list_divider_mtrl_alpha.9.png
abc_btn_radio_to_on_mtrl_000.png         abc_list_focused_holo.9.png
abc_btn_radio_to_on_mtrl_015.png         abc_list_longpressed_holo.9.png
abc_btn_switch_to_on_mtrl_00001.9.png    abc_list_pressed_holo_dark.9.png
abc_btn_switch_to_on_mtrl_00012.9.png    abc_list_pressed_holo_light.9.png
abc_cab_background_top_mtrl_alpha.9.png   abc_list_selector_disabled_holo_dark.9.png
abc_ic_commit_search_api_mtrl_alpha.png   abc_list_selector_disabled_holo_light.9.png
abc_ic_menu_copy_mtrl_am_alpha.png        abc_menu_hardkey_panel_mtrl_mult.9.png
abc_ic_menu_cut_mtrl_alpha.png            abc_popup_background_mtrl_mult.9.png
abc_ic_menu_paste_mtrl_am_alpha.png       abc_scrubber_control_off_mtrl_alpha.png
abc_ic_menu_selectall_mtrl_alpha.png       abc_scrubber_control_to_pressed_mtrl_000.png
abc_ic_menu_share_mtrl_alpha.png          abc_scrubber_control_to_pressed_mtrl_005.png
abc_ic_star_black_16dp.png               abc_scrubber_primary_mtrl_alpha.9.png
abc_ic_star_black_36dp.png               abc_scrubber_track_mtrl_alpha.9.png
abc_ic_star_black_48dp.png               abc_spinner_mtrl_am_alpha.9.png
abc_ic_star_half_black_16dp.png           abc_switch_track_mtrl_alpha.9.png
→ drawable-mdpi git:(master) X thunar ./
→ drawable-mdpi git:(master) X

```



## Security Stuff

There is bypass for root detection functionality using frida and also we can patch the apk by changing the smali

