

Mobile Pentest – Project

DYNAMIC ANALYSIS

Created by: Cindy

1. Sesuai dengan guide yang diberikan, berikut merupakan code yang telah dianalisis dari app-release.apk.

a. MASTG-TEST-0003 - Testing Logs for Sensitive Data

Merupakan test case yang mengidentifikasi data aplikasi yang sensitive dengan menganalisis source code, cek log file, mengumpulkan log untuk mencari data sensitive.

Dapat di cek pada EmailRepository terdapat log receive and send email.

```
30 public static /* synthetic */ boolean lambda$getUserEmails$0(EmailGetUserEmailsDto emailGetUserEmailsDto, Email email) {
31     Iterator<User> it = email.getTo().iterator();
32     while (it.hasNext()) {
33         User next = it.next();
34         Log.v("testing", email.getId() + " - " + next.getEmail() + " - " + emailGetUserEmailsDto.getUserEmail());
35         if (next.getEmail().equals(emailGetUserEmailsDto.getUserEmail())) {
36             return false;
37         }
38     }
39     if (email.getCc() == null) {
40         return true;
41     }
42     Iterator<User> it2 = email.getCc().iterator();
43     while (it2.hasNext()) {
44         if (it2.next().getEmail().equals(emailGetUserEmailsDto.getUserEmail())) {
45             return false;
46         }
47     }
48     return true;
49 }
```

Kita dapat menggunakan command **adb shell ps** untuk mengetahui pid dari aplikasi.

```
u0_a160      16665    386 13906536 117280 0      0 S com.climawan.comp6844001_uts.competitormail
```

Berdasarkan foto di atas, pid aplikasi competitorMail merupakan 16665.

Setelah kita mendapatkan pid dari aplikasi tersebut, kita dapat menggunakan **logcat** agar dapat melihat aktivitas log dari aplikasi competitorMail.

```
04-30 12:22:06.885 16665 16665 V testing : 84a39e70-b104-44f9-8ce3-32eaf8fde279 - user2@climawan.com --- user1@climawan.com
04-30 12:22:06.885 16665 16665 V testing : 3d3b4b29-5c34-497a-8abb-d4ecc267ebfd - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 7a5abaf9-a683-42bf-95be-0d75bf8dbccb - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 85931c47-16a4-42b6-868a-7b2a2b325949 - user1@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : a3ec4b3d-a225-4f3a-bf06-e1213704ccae - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 86911ded-4d9d-46c2-b445-60dd7f3ccc36 - user2@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : c17f60b5-a110-4824-a13a-42405c576c58 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 7bd1665f-0acd-43a2-874f-17129-f549d8 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 576f15bd-026d-4e4d-9901-ac3069dad641 - user1@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 2876caca-de66-4291-abb4-200916843bf2 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 4b3254fc-b917-45ba-bfe5-08dfdad8982 - user2@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 078bda89-5511-4649-856a-c16a3bf6a00 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : a9cc5c01-977f-4048-b76d-54ee175460b2 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 33920af4-aede-4f96-ba79-5fb3d29fd288 - user1@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 105e483a-3a58-4b07-b49a-75665ed16b2d - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : f234f129-a117-4d1c-8c65-11830fd40a32 - user2@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 2ba7456f-7226-41d7-9d3d-af6c4fe5d492 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : d2ec937c-c11c-4e9f-9391-794dd7896645 - user3@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 9cfbf44b-f616-44ee-8bb6-088cd2ebf6ad - user1@climawan.com --- user1@climawan.com
04-30 12:22:06.886 16665 16665 V testing : 9702ff56-ef4c-4dc9-a4a9-38512d8d5a19 - user3@climawan.com --- user1@climawan.com
```

Command : **adb logcat -pid 16665**

Terlihat bahwa dari log tersebut tidak ada data sensitive yang tercatat.

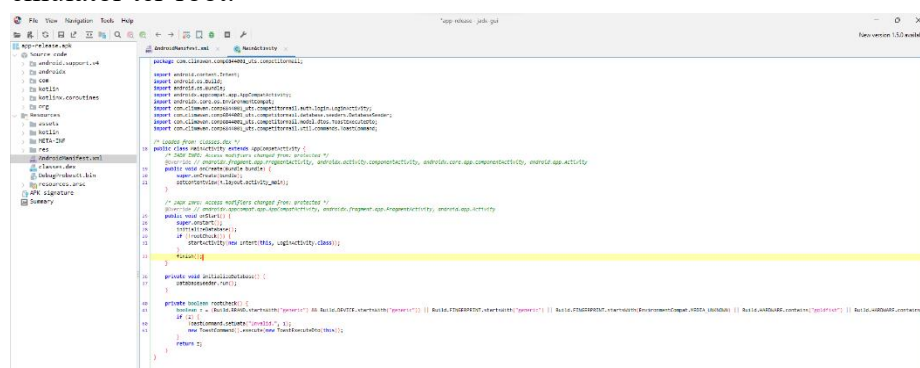
b. MASTG-TEST-0006 – Determining Whether the Keyboard Cache Is Disabled for Text Input Fields

Merupakan test case yang menganalisis berdasarkan aktivitas melalui keyboard. Terdapat pada XML atribut “android:inputType” yang bernilai textNoSuggestions yang dimana cache tidak akan ditampilkan jika input field terpilih. File ini terdapat pada “res/layout/mtrl_search_view.xml” di line 99.

c. MASTG-TEST-0024 - Testing for App Permissions

```
C:\Users\PicoPark\Downloads>aapt d permissions app-release.apk
package: com.climawan.comp6844001_uts.competitormail
uses-permission: name='android.permission.INTERNET'
permission: com.climawan.comp6844001_uts.competitormail.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION
uses-permission: name='com.climawan.comp6844001_uts.competitormail.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION'
```

Merupakan test case yang mengecek adanya root detection pada sebuah aplikasi, sehingga aplikasi tidak dapat berjalan pada code. Contohnya terdapat di bawah ini. Terdapat pada file MainActivity line ke 29 – 41 mendeteksi adanya root sehingga aplikasi tidak dapat dibuka.



e. **MASTG-TEST-0051 - Testing Obfuscation**

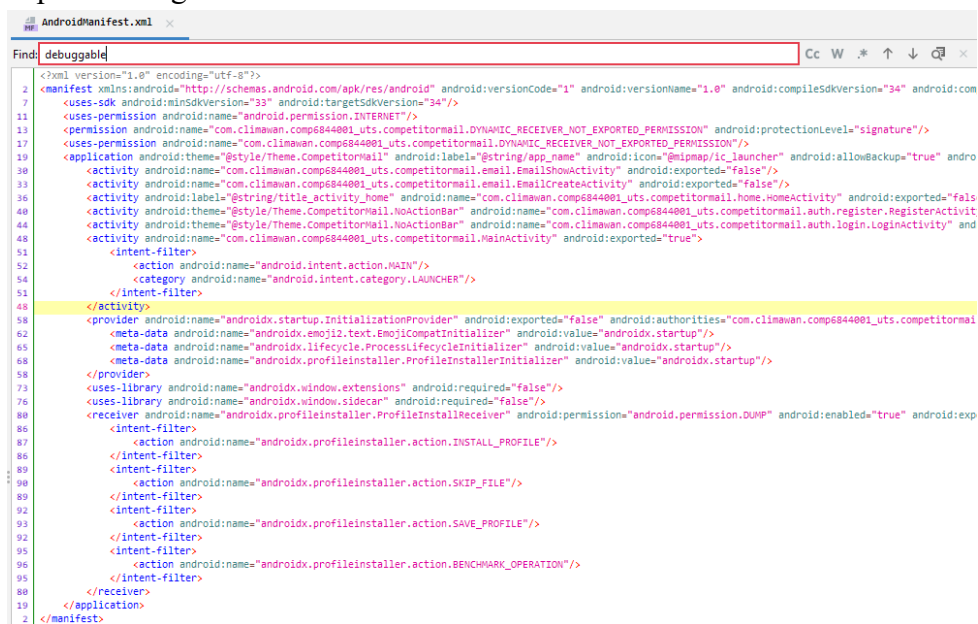
```

10 public class UserSeeder extends BaseSeeder {
11     public static void run() {
12         UserRepository userRepository = UserRepository.getInstance();
13         Vector vector = new Vector();
14         vector.add(new UserCreateDto("user 1", "user1@climawan.com", "user1user1"));
15         vector.add(new UserCreateDto("user 2", "user2@climawan.com", "helloworlds123"));
16         vector.add(new UserCreateDto("user 3", "user3@climawan.com", "blabla512"));
17         vector.add(new UserCreateDto("user 4", "user4@climawan.com", "welcometomobilelegend"));
18         userRepository.massCreate(new UserMassCreateDto(vector));
19     }
20 }

```

f. MASTG-TEST-0082 - Testing whether the App is Debuggable

Merupakan test case yang menganalisa dengan mengecek value dari “get-task-allow”, jika bernilai true maka aplikasi merupakan debuggable. Debuggable dapat ditemukan di AndroidManifest.xml. Jika tidak ditemukan maka aplikasi tidak dapat didebug.



```

<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName="1.0" android:compileSdkVersion="34" android:com
7
<uses-sdk android:minSdkVersion="33" android:targetSdkVersion="34"/>
11
<uses-permission android:name="android.permission.INTERNET"/>
13
<uses-permission android:name="com.climawan.comp6844001_uts.competitormail.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION" android:protectionLevel="signature"/>
17
<uses-permission android:name="com.climawan.comp6844001_uts.competitormail.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"/>
19
<application android:theme="@style/Theme.CompetitorMail" android:label="@string/app_name" android:icon="@mipmap/ic_launcher" android:allowBackup="true" andro
30
<activity android:name="com.climawan.comp6844001_uts.competitormail.email.EmailShowActivity" android:exported="false"/>
33
<activity android:name="com.climawan.comp6844001_uts.competitormail.email.EmailCreateActivity" android:exported="false"/>
36
<activity android:label="@string/title_activity_home" android:name="com.climawan.comp6844001_uts.competitormail.home.HomeActivity" android:exported="false"
40
<activity android:theme="@style/Theme.CompetitorMail.NoActionBar" android:name="com.climawan.comp6844001_uts.competitormail.auth.register.RegisterActivit
44
<activity android:theme="@style/Theme.CompetitorMail.NoActionBar" android:name="com.climawan.comp6844001_uts.competitormail.auth.login.LoginActivity" and
48
<activity android:name="com.climawan.comp6844001_uts.competitormail.MainActivity" android:exported="true">
51
    <intent-filter>
52        <action android:name="android.intent.action.MAIN"/>
53        <category android:name="android.intent.category.LAUNCHER"/>
54    </intent-filter>
55
48 </activity>
58
<provider android:name="androidx.startup.InitializationProvider" android:exported="false" android:authorities="com.climawan.comp6844001_uts.competitormail
62
    <meta-data android:name="androidx.emoji2.text.EmojiCompatInitializer" android:value="androidx.startup"/>
65
    <meta-data android:name="androidx.lifecycle.ProcessLifecycleInitializer" android:value="androidx.startup"/>
68
    <meta-data android:name="androidx.profileinstaller.ProfileInstallerInitializer" android:value="androidx.startup"/>
58
</provider>
73
<uses-library android:name="androidx.window.extensions" android:required="false"/>
76
<uses-library android:name="androidx.window.sidecar" android:required="false"/>
80
<receiver android:name="androidx.profileinstaller.ProfileInstallReceiver" android:permission="android.permission.DUMP" android:enabled="true" android:exp
86
    <intent-filter>
87        <action android:name="androidx.profileinstaller.action.INSTALL_PROFILE"/>
88    </intent-filter>
89
    <intent-filter>
90        <action android:name="androidx.profileinstaller.action.SKIP_FILE"/>
91    </intent-filter>
92
    <intent-filter>
93        <action android:name="androidx.profileinstaller.action.SAVE_PROFILE"/>
94    </intent-filter>
95
    <intent-filter>
96        <action android:name="androidx.profileinstaller.action.BENCHMARK_OPERATION"/>
97    </intent-filter>
98
    </receiver>
19 </application>
2 </manifest>

```

g. MASTG-TEST-0092 – Testing Emulator Detection

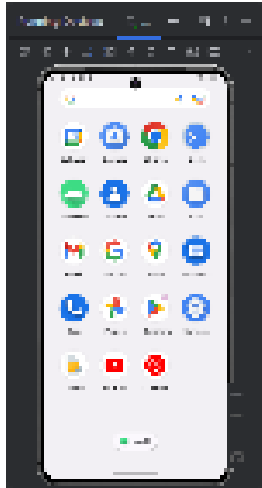
Sesuai dengan nama “Testing Emulator Detection, merupakan test case untuk mendeteksi apakah aplikasi yang dipakai dapat dijalankan pada emulator dan lihat apa respon aplikasi yang digunakan.

```

private boolean rootCheck() {
    boolean z = (Build.BRAND.startsWith("generic") && Build.DEVICE.startsWith("generic")) || Build.FINGERPRINT.startsWith("generic") || Build.FINGERPRINT.
    if (z) {
        ToastCommand.setData("Invalid.", 1);
        new ToastCommand().execute(new ToastExecuteDto(this));
    }
    return z;
}



```

Seperti pada code sebelumnya, pada line 41 terdapat perintah jika aplikasi dijalankan pada emulator maka aplikasi akan force close dan menampilkan tulisan “Invalid”.

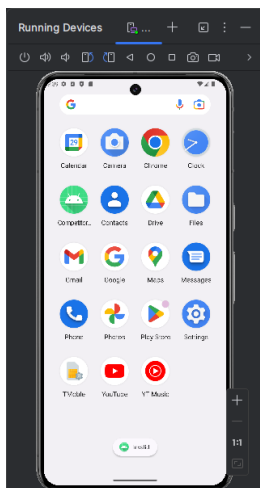


2. Write Up

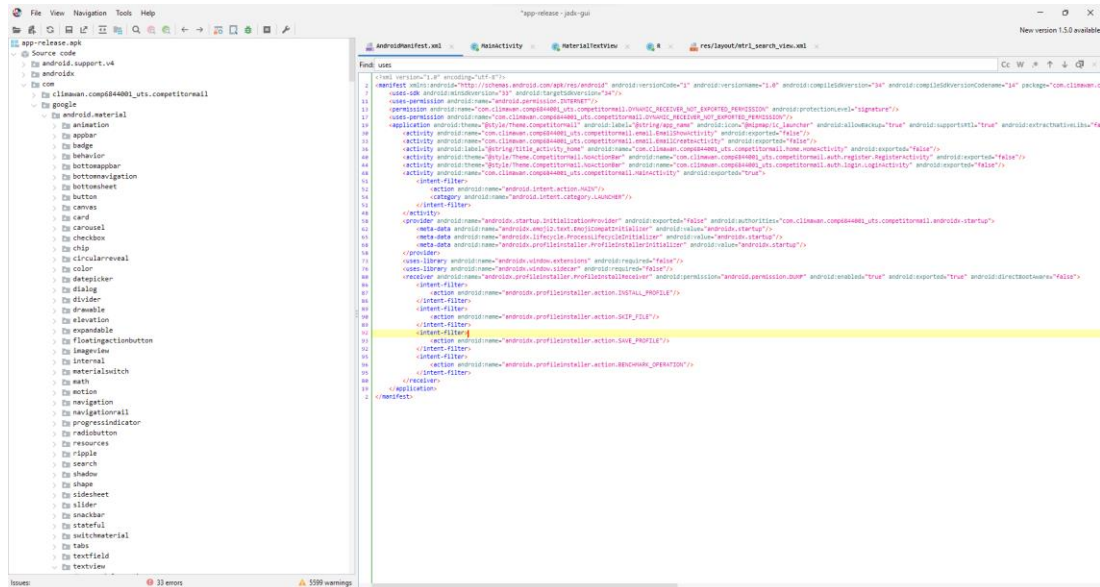
Diberikan sebuah aplikasi bernama app-release.apk.

i...	Name	Date Modified	File Size
	app-release.apk	2024-03-13	10.4 MB
	_MACOSX	2024-03-13	

Setelah didownload, saya mencoba untuk mendownload ke emulator. Namun hasilnya aplikasi tidak dapat dibuka, dan menampilkan tulisan invalid.



Setelah itu, dicoba cek dengan menganalisis source code dari aplikasi tersebut dengan menggunakan JADX-GUI dan menampilkan seperti di bawah ini.



Setelah ditelaah, terdapat code yang mendeteksi root dan emulator pada file /Source Code/com/climawan.comp6844001_uts.competitormail/MainActivity seperti gambar di bawah ini.

```

25 public void onStart() {
26     super.onStart();
27     initializeDatabase();
28     if (!rootCheck()) {
29         startActivity(new Intent(this, LoginActivity.class));
30     }
31 }
32
33 private void initializeDatabase() {
34     databaseHelper.run();
35 }
36
37 private boolean rootCheck() {
38     boolean z = (Build.BRAND.startsWith("generic") && Build.DEVICE.startsWith("generic")) || Build.FINGERPRINT.startsWith("generic") || Build.FINGERPRINT.startsWith(EnvironmentCompat.MEDIA_UNKNOWN) || Build.HARDWARE.contains("goldfish") || Build.W
39     if (z) {
40         ToastCommand.setData("Invalid.", 1);
41         new ToastCommand().execute(new ToastExecuteoto(this));
42     }
43     return z;
44 }
45 }

```

Untuk menghapus kondisi detect root, maka harus meng-decompile aplikasi tersebut dengan menggunakan apktool dan menghapus detect root lewat file smali.










```

I: Using Apktool 2.9.3 on app-release.apk
I: Loading resource table...
I: Decoding file-resources...
I: Loading resource table from file: C:\Users\PicoPark\AppData\Local\apktool\framework\1.apk
I: Decoding values */* XMLs...
I: Decoding AndroidManifest.xml with resources...
I: Regular manifest package...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
I: Copying META-INF/services directory

```

apktool d app-release.apk

Aplikasi yang telah ter-decompile akan menghasilkan tampilan di bawah ini

 apktool	30/04/2024 10:52	Yaml Source File	4 KB
 AndroidManifest.xml	30/04/2024 10:52	xmlfile	4 KB
 assets	30/04/2024 10:52	File folder	
 kotlin	30/04/2024 10:52	File folder	
 META-INF	30/04/2024 10:52	File folder	
 original	30/04/2024 10:52	File folder	
 smali	30/04/2024 10:52	File folder	
 unknown	30/04/2024 10:52	File folder	
 res	30/04/2024 10:52	File folder	

Pada gambar sebelumnya, terdapat code yang mendetect root dan emulator pada line 29-61 di MainActivity maka kita hapus dan mengubah return true menjadi false pada file smali

```

25  .method private rootCheck()Z
26      .register 1
27
28      const/4 v0, 0x0
29
30      return v0
31
32  .end method

```

Setelah di save dan membuka kembali di JADX-Gui, maka tampilan pada MainActivity bagian rootCheck() akan berubah menjadi return false. Maka dapat disimpulkan bahwa kita dapat membuka aplikasi ini kembali, namun harus meng-build kembali aplikasi yang telah diedit smalnya dengan cara:

1. Membuat key yang dibutuhkan untuk build kembali aplikasi menggunakan keytool.

```

Enter keystore password:
Re-enter new password:
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
Enter the distinguished name. Provide a single dot (.) to leave a sub-component empty or press ENTER to use the default value in braces.
What is your first and last name?
What is the name of your organizational unit?
What is the name of your organization?
What is the name of your City or Locality?
What is the name of your State or Province?
What is the two-letter country code for this unit?
Is CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct?
[no]: y
Generating 2,048 bit RSA key pair and self-signed certificate (SHA384withRSA) with a validity of 1,000 days
for: CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown

```

keytool -genkeypair -keyalg RSA -keysize 2048 -validity 1000 -keystore key.keystore

2. Melakukan build kembali pada aplikasi yang sudah diedit smali nya menggunakan apktool.

```
I: Using Apktool 2.9.3
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Copying libs... (/kotlin)
I: Copying libs... (/META-INF/services)
I: Building apk file...
I: Copying unknown files/dir...
I: Built apk into: patch.apk
```

apktool b app-release -o patch.apk

3. Setelah itu menggunakan zipalign agar aplikasi yang dibuild terkompres dengan rapi.
Command: **zipalign -p 4 patch.apk patched.apk**
4. Langkah terakhir, harus menandatangani aplikasi yang telah di zipalign agar aplikasi dapat dilaunch dan dibuka pada emulator.
Command: **apksigner sign -ks key.keystore -out final.apk patched.apk**
5. Kemudian aplikasi yang lama dapat didelete dari emulator dan aplikasi yang baru dapat di adb install lagi untuk menginstall ke dalam emulator.
6. Aplikasi dapat dibuka tertera pada gambar di bawah.

