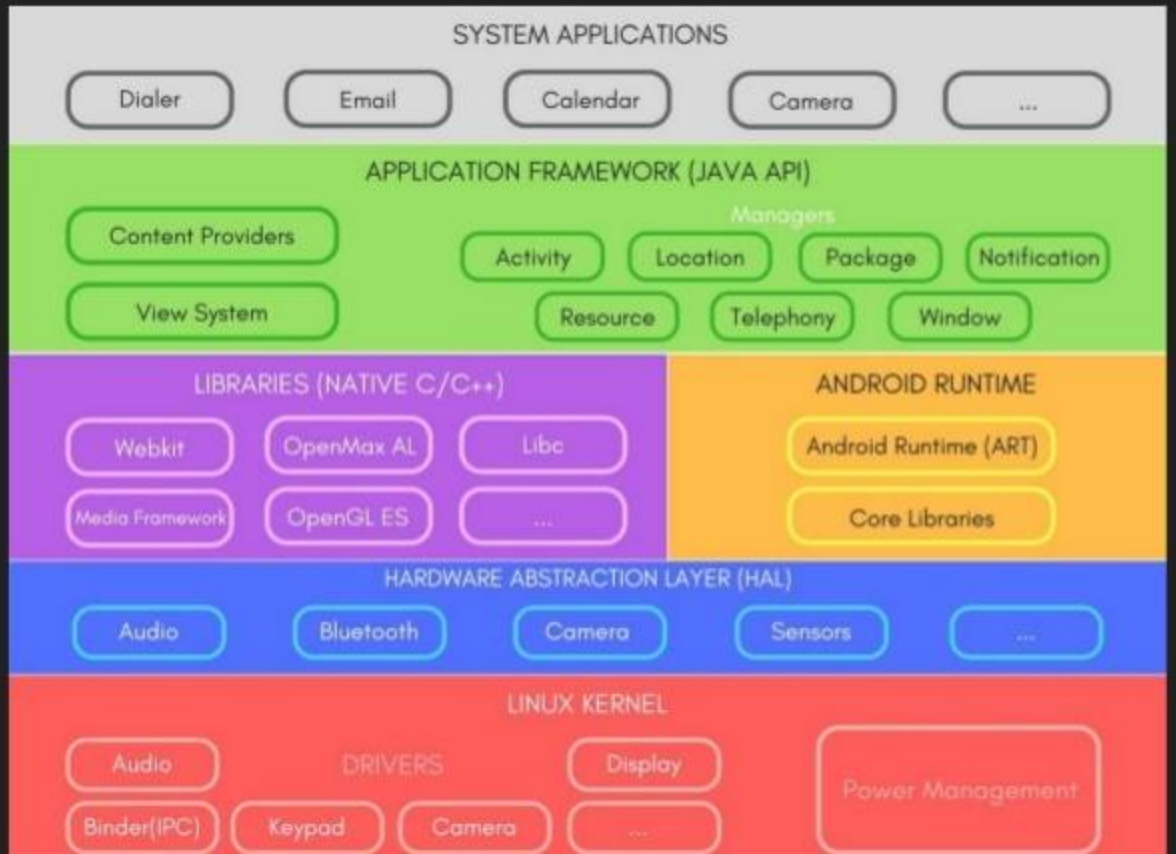
Android Security & Penetration Testing

Beginners guide to Penetration Testing Mobile Application (Android) Using DIVA

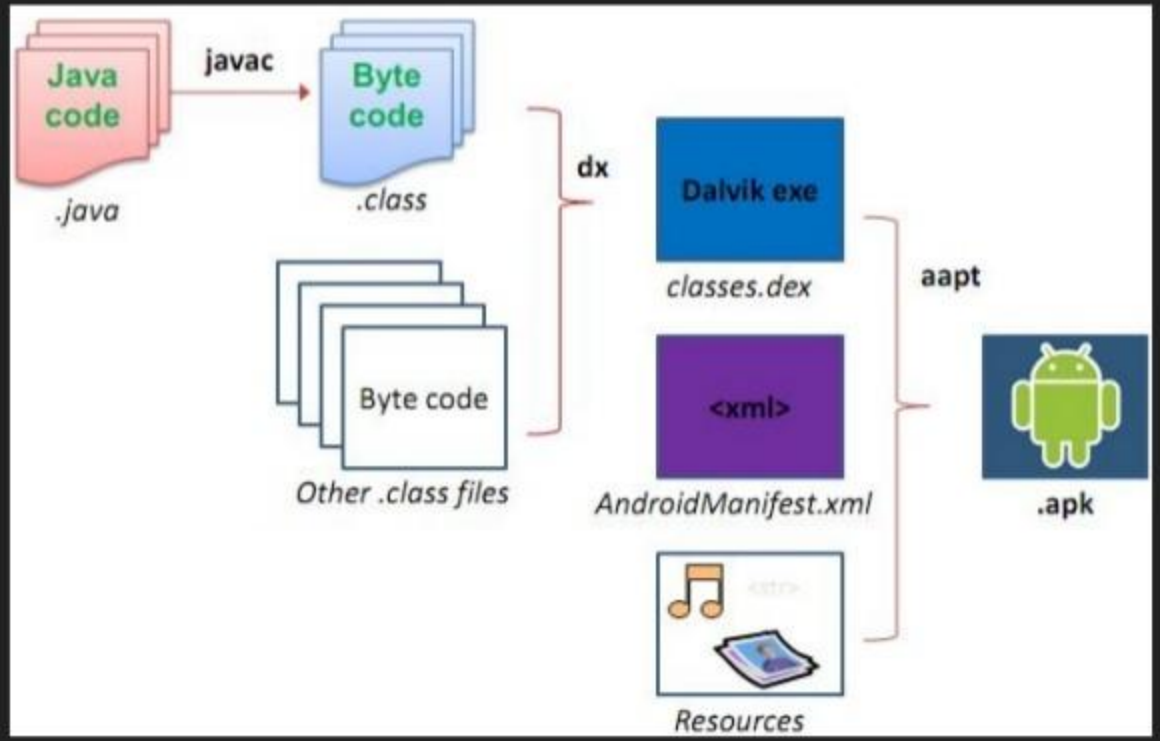
Android Architecture



Android Runtime (ART):

1. Alternative to Dalvik Virtual Mach
2. Released with 4.4 as an experim 5.0 it completely replaced Dalvi Virtual Machine.
3. Major change in ART is because Ahead-of-time(AOT) Compilation Garbage Collection.
4. In Ahead-of-time(AOT) Compilat ,android apps will be compiled w user installs them on their devic whereas in the Dalvik used Just-in-time(JIT) compilation in wl bytecode are compiled when us runs the app.

Android Application Fundamentals



1. Written in JAVA or Kotlin (Native)
2. Hybrid could be written using frameworks like ionic (HTML) or Xamarin

When you get an apk, it's more than a resource!

What’s inside the apk?

AndroidManifest.xml : Contains all the top level components like Activities, Services, Broadcast Receivers etc. Contains permissions as well. All the dangerous permissions has to be in Manifest file!

Keep your eye on:

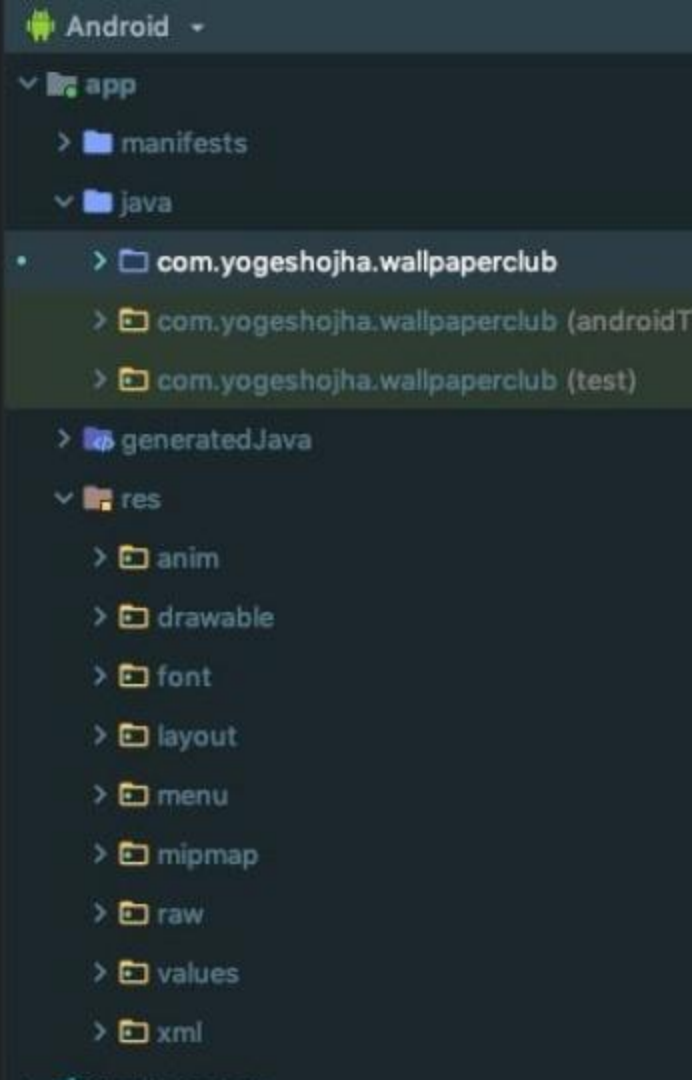
1. Debug Mode : Defines whether the application can be debugged or not! If the application can be debugged then it can provide plenty of information to an attacker. Android applications not in the production state can have it set to true otherwise it must be false.
2. BackUp Flag: Defines whether application data can be backed up and restored by a user who has enable usb debugging. Applications that handle and store sensitive information such as card details, passwords etc. should have this setting set to false to prevent such risks.
3. External Storage
   Applications that have the permission to copy data to external storage should be reviewed to ensure tha no sensitive information is stored.
4. Permissions!!! Keep an eye on permissions to check if application is asking for dangerous permissions tha do NOT require!

AndroidManifest.xml

```xml
<?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://schemas.android.com/apk/res/android" package="jakhar.aseem.diva"
platformBuildVersionCode="23" platformBuildVersionName="6.0-2166767">
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
    <uses-permission android:name="android.permission.INTERNET"/>
    <application android:allowBackup="true" android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:supportsRtl="true"
    android:theme="@style/AppTheme">
        <activity android:label="@string/app_name" android:name="jakhar.aseem.diva.MainActivity" android:theme="@style/AppTheme.NoActionBar">
            <intent-filter>
                <action android:name="android.intent.action.MAIN"/>
                <category android:name="android.intent.category.LAUNCHER"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d1" android:name="jakhar.aseem.diva.LogActivity"/>
        <activity android:label="@string/d2" android:name="jakhar.aseem.diva.HardcodeActivity"/>
        <activity android:label="@string/d3" android:name="jakhar.aseem.diva.InsecureDataStorage1Activity"/>
        <activity android:label="@string/d4" android:name="jakhar.aseem.diva.InsecureDataStorage2Activity"/>
        <activity android:label="@string/d5" android:name="jakhar.aseem.diva.InsecureDataStorage3Activity"/>
        <activity android:label="@string/d6" android:name="jakhar.aseem.diva.InsecureDataStorage4Activity"/>
        <activity android:label="@string/d7" android:name="jakhar.aseem.diva.SQLInjectionActivity"/>
        <activity android:label="@string/d8" android:name="jakhar.aseem.diva.InputValidation2URISchemeActivity"/>
        <activity android:label="@string/d9" android:name="jakhar.aseem.diva.AccessControl1Activity"/>
        <activity android:label="@string/apic_label" android:name="jakhar.aseem.diva.APICredsActivity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <activity android:label="@string/d10" android:name="jakhar.aseem.diva.AccessControl2Activity"/>
        <activity android:label="@string/apic2_label" android:name="jakhar.aseem.diva.APICreds2Activity">
            <intent-filter>
                <action android:name="jakhar.aseem.diva.action.VIEW_CREDS2"/>
                <category android:name="android.intent.category.DEFAULT"/>
            </intent-filter>
        </activity>
        <provider android:authorities="jakhar.aseem.diva.provider.notesprovider" android:enabled="true" android:exported="true" android:name="
        jakhar.aseem.diva.NotesProvider"/>
        <activity android:label="@string/d11" android:name="jakhar.aseem.diva.AccessControl3Activity"/>
        <activity android:label="@string/d12" android:name="jakhar.aseem.diva.Hardcode2Activity"/>
        <activity android:label="@string/pnotes" android:name="jakhar.aseem.diva.AccessControl3NotesActivity"/>
        <activity android:label="@string/d13" android:name="jakhar.aseem.diva.InputValidation3Activity"/>
    </application>
```

What's more inside the apk?

- Java Files
  Activity
  Activity represents a single screen with a user interface.
  Services
  Component that runs on background.
  Broadcast Receiver
  Component that responds to system-wide broadcast announcements.
  "Hey, is the device booted?"
- Resource Directory
  Values has Strings.xml file



Android Sandbox

Each Android app lives in its own security sandbox!
The Android operating system is a multi-user Linux system in which each app is a different user.

The Android system assigns each app a unique Linux UID known only to system and not the app!
The system sets permissions for all the files in an app so that only the UID assigned to that app can access ther

Each process has its own virtual machine (VM), so an app's code runs in isolation from other apps.
By default, every app runs in its own Linux process. Android starts the process when any of the app's components need to be executed, then shuts down the process when it's no longer needed or when the syster must recover memory for other apps.

The Android system implements the principle of least privilege, that is each app by default has access only to th components that it requires to do its work and no more.
This creates a very secure environment in which an app cannot access parts of the system for which it is not having permission. As every Android app runs in its own sandbox environment and cannot affect other apps by default but two apps can have same Linux User ID and can also share the same Dalvik VM if they are signed wit the same Certificates.

What's in the Arsenal?

Know your tools!

Android Debug Bridge:

```
yogeshojha@Yogeshs-MacBook-Air  ~  adb devices
List of devices attached
a3ab9809        device

yogeshojha@Yogeshs-MacBook-Air  ~  adb install Downloads/Diva_jakhar.aseem.diva.apk
Success
yogeshojha@Yogeshs-MacBook-Air  ~  adb push Downloads/Diva_jakhar.aseem.diva.apk /sdcard
Downloads/Diva_jakhar.aseem.diva.apk: 1 file pushed. 20.4 MB/s (1502294 bytes in 0.070s)
yogeshojha@Yogeshs-MacBook-Air  ~  adb shell
```

$adb logcat

```
ool size = 0, active threads = 0, queued tasks = 0, completed tasks = 9]
01-28 09:56:38.632 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: InstallBackgroundThread com.google.android.finsky.bo.
ng, pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 0]
01-28 09:56:39.171   891   891 W thermal-engine: type=1400 audit(0.0:1038231): avc: denied { read } for name="u:object_r:system_prop:s0" dev="tmpfs" ino=20705 scon
l-engine:s0 tcontext=u:object_r:system_prop:s0 tclass=file permissive=0
01-28 09:56:39.185   891  1051 E libc    : Access denied finding property "sys.thermal.para"
01-28 09:56:40.211  3668 25459 V FA      : Inactivity, disconnecting from the service
01-28 09:56:41.634 25300 25300 E diva-log: Error while processing transaction with credit card: 7646956659499466646464646646
01-28 09:56:43.697  1372  3797 W NotificationService: Toast already killed. pkg=jakhar.aseem.diva callback=android.app.ITransientNotification$Stub$Proxy@b33367e
01-28 09:56:43.993 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: Db-frosting.db com.google.android.finsky.bo.ao@f071882
size = 0, active threads = 0, queued tasks = 0, completed tasks = 419]
01-28 09:56:43.993 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: Db-notification_cache com.google.android.finsky.bo.ao
, pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 795]
01-28 09:56:44.181   891   891 W thermal-engine: type=1400 audit(0.0:1038232): avc: denied { read } for name="u:object_r:system_prop:s0" dev="tmpfs" ino=20705 scon
l-engine:s0 tcontext=u:object_r:system_prop:s0 tclass=file permissive=0
01-28 09:56:44.189   891  1051 E libc    : Access denied finding property "sys.thermal.para"
01-28 09:56:44.227   813  1365 W SurfaceFlinger: Attempting to destroy on removed layer: 5ad0be8 Toast#0
```

What's in the Arsenal?

Apktool

```
┌─[user@parrot]─[~]
└──╼ $apktool
Apktool v2.3.4-dirty - a tool for reengineering Android apk files
with smali v2.2.3-dev and baksmali v2.2.3-dev
Copyright 2014 Ryszard Wiśniewski <brut.alll@gmail.com>
Updated by Connor Tumbleson <connor.tumbleson@gmail.com>

usage: apktool
 -advance,--advanced   prints advance information.
 -version,--version    prints the version then exits
usage: apktool if|install-framework [options] <framework.apk>
 -p,--frame-path <dir>   Stores framework files into <dir>.
 -t,--tag <tag>          Tag frameworks using <tag>.
usage: apktool d[ecode] [options] <file_apk>
 -f,--force              Force delete destination directory.
 -o,--output <dir>       The name of folder that gets written. Default is apk.out
 -p,--frame-path <dir>   Uses framework files located in <dir>.
 -r,--no-res             Do not decode resources.
 -s,--no-src             Do not decode sources.
 -t,--frame-tag <tag>    Uses framework files tagged by <tag>.
usage: apktool b[uild] [options] <app_path>
 -f,--force-all          Skip changes detection and build all files.
 -o,--output <dir>       The name of apk that gets written. Default is dist/name.apk
 -p,--frame-path <dir>   Uses framework files located in <dir>.

For additional info, see: http://ibotpeaches.github.io/Apktool/
For smali/baksmali info, see: https://github.com/JesusFreke/smali
```

What's in the Arsenal?

How do I decompile the apk?

```
┌─[user@parrot]─[~/Downloads]
└──╼ $apktool d Diva_jakhar.aseem.diva.apk
I: Using Apktool 2.3.4-dirty on Diva_jakhar.aseem.diva.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: /home/user/.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...
```

What's in the Arsenal?

Dex2Jar : convert an APK file in to a jar file containing reconstructed source code

```
┌─[user@parrot]─[~/Downloads]
└──╼ $d2j-dex2jar Diva_jakhar.aseem.diva.apk
dex2jar Diva_jakhar.aseem.diva.apk -> ./Diva_jakhar.aseem.diva-dex2jar.jar
```

Jd-gui: To open that jar file in JD-GUI and view that reconstructed source code.

GeanyMotion as well!

DIVA

Damn insecure and vulnerable App

1. Insecure Logging

adb logcat

```
ool size = 0, active threads = 0, queued tasks = 0, completed tasks = 9]
01-28 09:56:38.632 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: InstallBackgroundThread com.google.android.finsky.bo.ao@8dc176e[Ru
ng, pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 0]
01-28 09:56:39.171   891   891 W thermal-engine: type=1400 audit(0.0:1038231): avc: denied { read } for name="u:object_r:system_prop:s0" dev="tmpfs" ino=20705 scontext=u:r:the
l-engine:s0 tcontext=u:object_r:system_prop:s0 tclass=file permissive=0
01-28 09:56:39.185   891  1051 E libc    : Access denied finding property "sys.thermal.para"
01-28 09:56:40.211  3668 25459 V FA      : Inactivity, disconnecting from the service
01-28 09:56:41.634 25300 25300 E diva-log: Error while processing transaction with credit card: 7646956659499466646464646646
01-28 09:56:43.697  1372  3797 W NotificationService: Toast already killed. pkg=jakhar.aseem.diva callback=android.app.ITransientNotification$Stub$Proxy@b33367e
01-28 09:56:43.993 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: Db-frosting.db com.google.android.finsky.bo.ao@f071882[Running, po
size = 0, active threads = 0, queued tasks = 0, completed tasks = 419]
01-28 09:56:43.993 15168 15201 I Finsky  : [824] com.google.android.finsky.bo.an.run(6): Stats for Executor: Db-notification_cache com.google.android.finsky.bo.ao@6093b93[Runn
, pool size = 0, active threads = 0, queued tasks = 0, completed tasks = 795]
01-28 09:56:44.181   891   891 W thermal-engine: type=1400 audit(0.0:1038232): avc: denied { read } for name="u:object_r:system_prop:s0" dev="tmpfs" ino=20705 scontext=u:r:the
l-engine:s0 tcontext=u:object_r:system_prop:s0 tclass=file permissive=0
01-28 09:56:44.189   891  1051 E libc    : Access denied finding property "sys.thermal.para"
01-28 09:56:44.227   813  1365 W SurfaceFlinger: Attempting to destroy on removed layer: 5adbbe8 Toast#0
```

1. Insecure Logging

Vulnerable Code

```
public class LogActivity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_log);
    }

    public void checkout(View view) {
        EditText cctxt = (EditText) findViewById(C0209R.id.ccText);
        try {
            processCC(cctxt.getText().toString());
        } catch (RuntimeException e) {
            Log.e("diva-log", "Error while processing transaction with credit card: " + cctxt.getText().toString());
            Toast.makeText(this, "An error occured. Please try again later", 0).show();
        }
    }

    private void processCC(String ccstr) {
        throw new RuntimeException();
    }
}
```

2. HardCoding Issues

```
public class HardcodeActivity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_hardcode);
    }

    public void access(View view) {
        if (((EditText) findViewById(C0209R.id.hcKey)).getText().toString().equals("vendorsecretkey")) {
            Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
        } else {
            Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
        }
    }
}
```

2. HardCoding Issues

```
public class HardcodeActivity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_hardcode);
    }

    public void access(View view) {
        if (((EditText) findViewById(C0209R.id.hcKey)).getText().toString().equals("vendorsecretkey")) {
            Toast.makeText(this, "Access granted! See you on the other side :)", 0).show();
        } else {
            Toast.makeText(this, "Access denied! See you in hell :D", 0).show();
        }
    }
}
```

2. Insecure Data Storage

Where is the android data being stored?

```
OnePlus5T:/data/data/jakhar.aseem.diva # ls -al
total 56
drwxr-x--x   6 u0_a173 u0_a173        4096 2018-12-20 21:24 .
drwxrwx--x 277 system  system        12288 2019-01-28 08:42 ..
drwxrws--x   2 u0_a173 u0_a173_cache  4096 2018-12-20 21:24 cache
drwxrws--x   2 u0_a173 u0_a173_cache  4096 2018-12-20 21:24 code_cache
drwxrwx--x   2 u0_a173 u0_a173        4096 2018-12-20 21:24 databases
drwxrwx--x   2 u0_a173 u0_a173        4096 2019-01-28 10:31 shared_prefs
OnePlus5T:/data/data/jakhar.aseem.diva #
```

2. Insecure Data Storage

Vulnerable Code

```
public class InsecureDataStorage1Activity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_insecure_data_storage1);
    }

    public void saveCredentials(View view) {
        Editor spedit = PreferenceManager.getDefaultSharedPreferences(this).edit();
        EditText pwd = (EditText) findViewById(C0209R.id.ids1Pwd);
        spedit.putString("user", ((EditText) findViewById(C0209R.id.ids1Usr)).getText().toString());
        spedit.putString("password", pwd.getText().toString());
        spedit.commit();
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}
```

3. Insecure Data Storage

Shared Preference

```
OnePlus5T:/data/data/jakhar.aseem.diva/shared_prefs # ls
embryo.xml jakhar.aseem.diva_preferences.xml
OnePlus5T:/data/data/jakhar.aseem.diva/shared_prefs # cat jakhar.aseem.diva_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="password">hello</string>
    <string name="user">hi</string>
</map>
OnePlus5T:/data/data/jakhar.aseem.diva/shared_prefs #
```

4. Insecure Data Storage - II

Vulnerable Code

```
public class InsecureDataStorage2Activity extends AppCompatActivity {
    private SQLiteDatabase mDB;

    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        try {
            this.mDB = openOrCreateDatabase("ids2", 0, null);
            this.mDB.execSQL("CREATE TABLE IF NOT EXISTS myuser(user VARCHAR, password VARCHAR);");
        } catch (Exception e) {
            Log.d("Diva", "Error occurred while creating database: " + e.getMessage());
        }
        setContentView((int) C0209R.layout.activity_insecure_data_storage2);
    }

    public void saveCredentials(View view) {
        try {
            this.mDB.execSQL("INSERT INTO myuser VALUES ('" + ((EditText) findViewById(C0209R.id.ids2Usr)).getText().toString()
            this.mDB.close();
        } catch (Exception e) {
            Log.d("Diva", "Error occurred while inserting into database: " + e.getMessage());
        }
        Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
    }
}
```

4. Insecure Data Storage - II

adb (adb) ⌘1 | adb (adb) ⌘2

```
OnePlus5T:/data/data/jakhar.aseem.diva/databases # ls -al
total 180
drwxrwx--x 2 u0_a173 u0_a173  4096 2019-01-28 10:34 .
drwxr-x--x 6 u0_a173 u0_a173  4096 2018-12-20 21:24 ..
-rw-rw---- 1 u0_a173 u0_a173  4096 2018-12-20 21:24 divanotes.db
-rw------- 1 u0_a173 u0_a173 32768 2019-01-28 10:20 divanotes.db-shm
-rw------- 1 u0_a173 u0_a173 32992 2018-12-20 21:24 divanotes.db-wal
-rw-rw---- 1 u0_a173 u0_a173  4096 2019-01-28 10:34 ids2
-rw------- 1 u0_a173 u0_a173 32768 2019-01-28 10:34 ids2-shm
-rw------- 1 u0_a173 u0_a173 28872 2019-01-28 10:34 ids2-wal
OnePlus5T:/data/data/jakhar.aseem.diva/databases #
```

4. Insecure Data Storage - II

How do I pull the database?

4. Insecure Data Storage - II

How do I pull the database?

```
✘ yogeshojha@Yogeshs-MacBook-Air >> adb pull /sdcard/divanotes.db
/sdcard/divanotes.db: 1 file pulled. 0.5 MB/s (4096 bytes in 0.008s)
```

```
$ sqlite3 ids2

SQLite version 3.8.5 2014-08-15 22:37:57

Enter ". help" for usage hints.

sqlite> .tables

android_metadata myuser

sqlite> select * from myuser;

SECRET|SECRET

sqlite>
```

5. Insecure Data Storage - III

Vulnerable Code

```
public class InsecureDataStorage3Activity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_insecure_data_storage3);
    }

    public void saveCredentials(View view) {
        EditText usr = (EditText) findViewById(C0209R.id.ids3Usr);
        EditText pwd = (EditText) findViewById(C0209R.id.ids3Pwd);
        try {
            File uinfo = File.createTempFile("uinfo", "tmp", new File(getApplicationInfo().dataDir));
            uinfo.setReadable(true);
            uinfo.setWritable(true);
            FileWriter fw = new FileWriter(uinfo);
            fw.write(usr.getText().toString() + ":" + pwd.getText().toString() + "\n");
            fw.close();
            Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        } catch (Exception e) {
            Toast.makeText(this, "File error occurred", 0).show();
            Log.d("Diva", "File error: " + e.getMessage());
        }
    }
}
```

5. Insecure Data Storage - III

```
OnePlus5T:/data/data/jakhar.aseem.diva # ls
cache code_cache databases shared_prefs uinfo6395957743866297225tmp
OnePlus5T:/data/data/jakhar.aseem.diva # cat uinfo6395957743866297225tmp
cache/                    code_cache/               databases/                shared_prefs/             uinfo6395957743866297225tmp
OnePlus5T:/data/data/jakhar.aseem.diva # cat uinfo6395957743866297225tmp
hiv:guh
OnePlus5T:/data/data/jakhar.aseem.diva #
```

6. Insecure Data Storage - IV

Vulnerable Code

```
public class InsecureDataStorage4Activity extends AppCompatActivity {
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) C0209R.layout.activity_insecure_data_storage4);
    }

    public void saveCredentials(View view) {
        EditText usr = (EditText) findViewById(C0209R.id.ids4Usr);
        EditText pwd = (EditText) findViewById(C0209R.id.ids4Pwd);
        try {
            File uinfo = new File(Environment.getExternalStorageDirectory().getAbsolutePath() + "/.uinfo.txt");
            uinfo.setReadable(true);
            uinfo.setWritable(true);
            FileWriter fw = new FileWriter(uinfo);
            fw.write(usr.getText().toString() + ":" + pwd.getText().toString() + "\n");
            fw.close();
            Toast.makeText(this, "3rd party credentials saved successfully!", 0).show();
        } catch (Exception e) {
            Toast.makeText(this, "File error occurred", 0).show();
            Log.d("Diva", "File error: " + e.getMessage());
        }
    }
}
```

6. Insecure Data Storage - IV

Any Guess where this file could be stored?

6. Insecure Data Storage - IV

Any Guess where this file could be stored?

```
OnePlus5T:/data/data/jakhar.aseem.diva # cd /sdcard/
OnePlus5T:/sdcard # ls
2ndLine       AutoWallpaper  Diva_jakhar.aseem.diva.apk InsWall              Music                 Pictures     RirioCars  Telegram   Xiaomi       mipush
Alarms        AzRecorderFree Documents                  KineMaster           NetCapture            Podcasts     SSLCapture Tencent    amap         oem_log
AmoledWalls   CamScanner     Download                   MIWiFi               Nordic\ Semiconductor Qrcode       Sketch     VpnCapture bluetooth    recordmaster
Analog\ Clock DCIM           Dumpster                   MiniVectorWallpapers Notifications         Ringtones    Snapseed   Wallify    dataconfigs  viber
Android       Dingtone       ExtractedApks              Movies               Papers                Ririo2Gaming TWRP       WhatsApp   divanotes.db
OnePlus5T:/sdcard # la -al
total 1916
drwxrwx--x 52 root sdcard_rw    4096 2019-01-28 10:50 .
drwx--x--x  6 root sdcard_rw    4096 2019-01-13 08:19 ..
drwxrwx--x  2 root sdcard_rw    4096 2019-01-20 12:02 .Ota
drwxrwx--x  3 root sdcard_rw    4096 2018-12-20 00:21 .images
-rw-rw----  1 root sdcard_rw      36 2018-12-15 07:44 .profig.os
drwxrwx--x  2 root sdcard_rw    4096 2019-01-11 16:41 .temp_tmp
-rw-rw----  1 root sdcard_rw      16 2019-01-28 10:50 .uinfo.txt
```

```
OnePlus5T:/sdcard # cat .uinfo.txt
secret:veryku h
```

7. Input Validation Issues - I

What could be done here?

7. Input Validation Issues - I

What could be done here?

Let’s try ‘ ? 😉

7. Input Validation Issues - I

What could be done here?

Let's try ' ? 😉

You Know it 😉

Possible SQL Injection

7. Input Validation Issues - I

How about 1' or ‘1’ != ‘2 ?

7. Input Validation Issues - I

Vulnerable Code

```
public void search(View view) {
    EditText srchtxt = (EditText) findViewById(C0209R.id.ivi1search);
    try {
        Cursor cr = this.mDB.rawQuery("SELECT * FROM sqliuser WHERE user = '" + srchtxt.getText().toString() + "'", null);
        StringBuilder strb = new StringBuilder("");
        if (cr == null || cr.getCount() <= 0) {
            strb.append("User: (" + srchtxt.getText().toString() + ") not found");
        } else {
            cr.moveToFirst();
            do {
                strb.append("User: (" + cr.getString(0) + ") pass: (" + cr.getString(1) + ") Credit card: (" + cr.getStrin
            } while (cr.moveToNext());
        }
        Toast.makeText(this, strb.toString(), 0).show();
    } catch (Exception e) {
        Log.d("Diva-sqli", "Error occurred while searching in database: " + e.getMessage());
    }
}
```

8. Input Validation Issues - II

More Dangerous!!!

8. Input Validation Issues - II

How about file:///sdcard/.uinfo.txt

Can we take this to next level? To read shared prefs? 😉

8. Input Validation Issues - II

How about file:///sdcard/.uinfo.txt

Can we take this to next level? To read shared prefs? 😉

file:///data/data/jakhar.aseem.diva/shared_prefs/ jakhar.aseem.diva_preferences.xml

Problem? Remember that permission External Storage?

How to capture packets in Burp?

Summary

Insecure Data Storage

- Shared Preferences, Database, Cache
- Pretty much everything inside /data/data

Binary Protections

- Remember you decompile an apk?
- Application Code can be obfuscated with the help of Proguard.
- For security conscious application's application, Dexguard can be used. Dexguard is a commercial version of Proguard. Besides encrypting classes, strings, native libraries, it also adds tamper detection to let your application react accordingly if a hacker has tried to modify it or is accessing it illegitimately.

Will be continued...

Any Questions?