



DOP: / /2023

DOS: / /2023

Experiment No:

Title: Reversing Android applications (APKs) APKTOOL, dex2jar and JD-GUI.

Theory:

What is DIVA?

DIVA (Damn insecure and vulnerable App) is an App intentionally designed to be insecure. We are releasing the Android version of Diva. We thought it would be a nice way to start the year by contributing something to the security community. The aim of the App is to teach developers/QA/security professionals, flaws that are generally present in the Apps due poor or insecure coding practices. If you are reading this, you want to either learn App pentesting or secure coding and I sincerely hope that DIVA solves your purpose. So, sit back and enjoy the ride.

Who can use Diva?

The idea originated, from a developer's perspective. The Android security training for developers becomes slightly boring with lot of theory and not much hands-on. SO, I created DIVA for our Android developer training. Diva gamifies secure development learning. With that said, it is an excellent learning tool for aspiring Android penetration testers and security professionals as it gives an insight into app vulnerabilities including the source code. To sum it up:

- Android App developers
- Android Penetration testers
- Security professionals
- Students

What is included in Diva?

I tried to put as much vulnerabilities as possible in a short period of time. I am sure I have missed out on some vulnerabilities. Please ping me if you know of a good vulnerability that can be included in Diva. It covers common vulnerabilities in Android apps ranging from insecure storage, input validation to access control issues. I have also included few vulnerabilities in native code, which makes it more interesting from the perspective of covering both Java and C vulnerabilities. Current Challenges include:

1. Insecure Logging
2. Hardcoding Issues – Part 1
3. Insecure Data Storage – Part 1
4. Insecure Data Storage – Part 2
5. Insecure Data Storage – Part 3
6. Insecure Data Storage – Part 4
7. Input Validation Issues – Part 1
8. Input Validation Issues – Part 2
9. Access Control Issues – Part 1



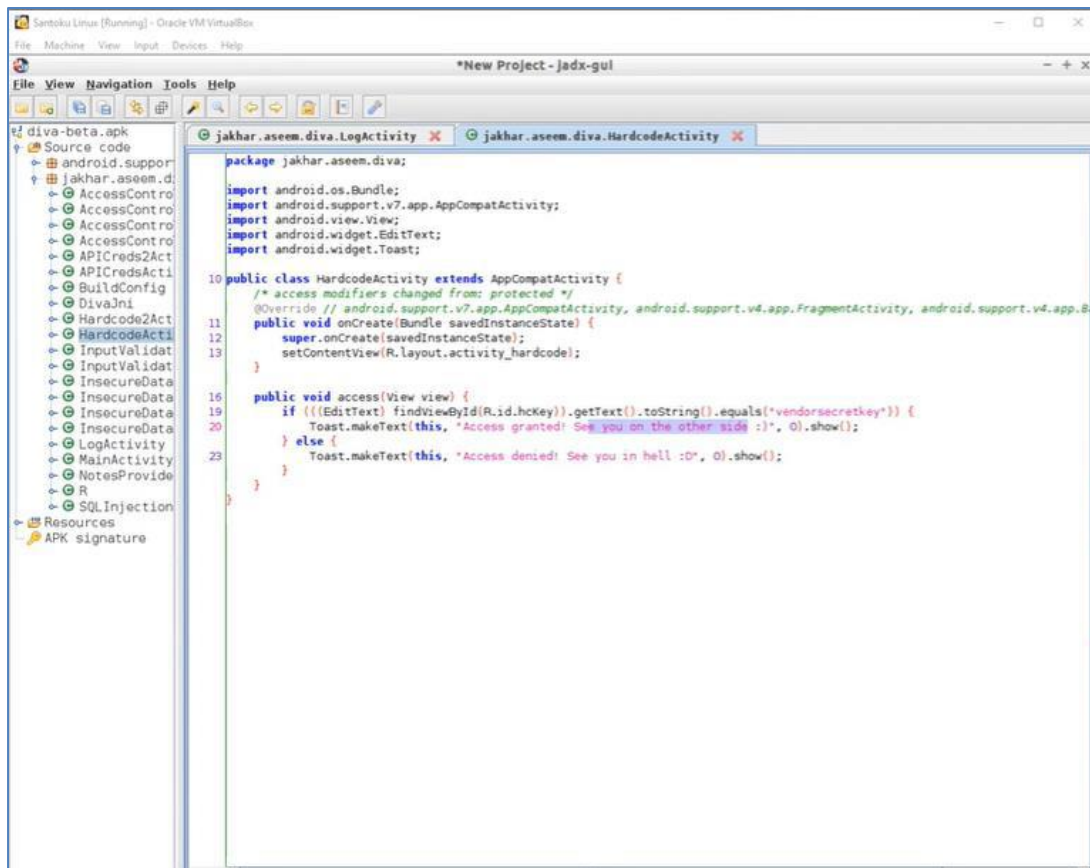
10. Access Control Issues – Part 2
11. Access Control Issues – Part 3
12. Hardcoding Issues – Part 2
13. Input Validation Issues – Part 3

How to compile Diva?

- Download the source
- Open the project in Android Studio
- For Native library – open command line
- `$ cd /app/src/main/jni`
- `$ make` (This needs to be done only once, unless you make changes to the native code – in which case run `make clean && make`)
- This will compile the native library and copy all the compiled versions in directory `jniLibs` which is required when building the app
- From the menu bar: Build->Make Project or Run->Run App

How to run Diva?

- Download the app
- On your phone settings. Go to security and check Unknown Sources checkbox. This allows you to install apps outside of play store. You don't need to do this if you are installing the app on an emulator.
- Connect your phone to the computer (make sure USB debugging is enabled on your phone) or run the emulator.
- `cd`
- `adb install`
- Start playing.



```

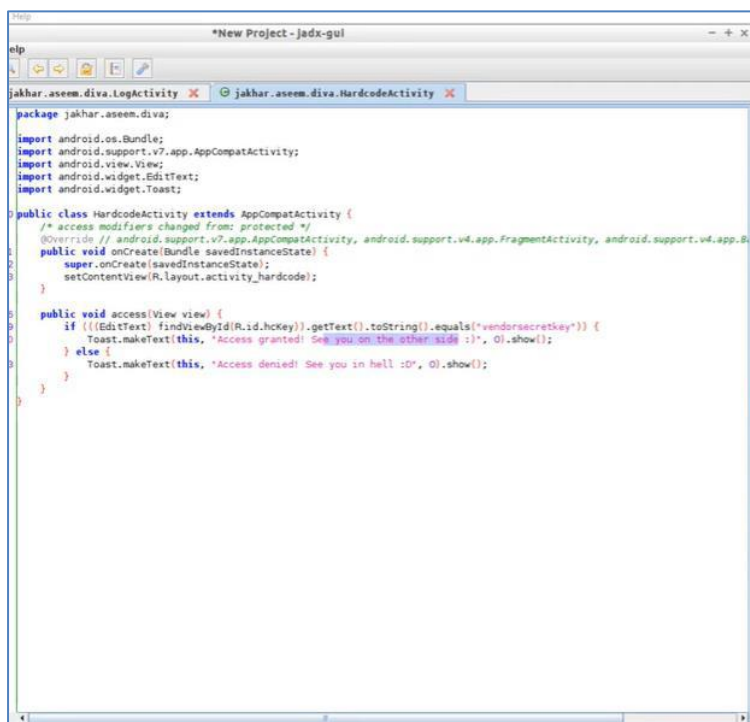
package jakhar.aseem.diva;

import android.os.Bundle;
import android.support.v7.app.AppCompatActivity;
import android.view.View;
import android.widget.EditText;
import android.widget.Toast;

10 public class HardcodeActivity extends AppCompatActivity {
    /* access modifiers changed from: protected */
    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.support.v4.app.B
    11 public void onCreate(Bundle savedInstanceState) {
    12     super.onCreate(savedInstanceState);
    13     setContentView(R.layout.activity_hardcode);
    }

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

```



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.

asfwd

.....

SAVE

3rd party credentials saved successfully!

```

andropentes... X andropentes... X
sdcard
seapp_contexts
sepolicy
storage
sys
system
tmp
ueventd.rc
ueventd.vbox86.rc
vendor
root@vbox86p:/ # cd data/data/
dalvik-cache/ data/
root@vbox86p:/ # cd data/data/
com.android.backupconfirm/
com.android.bluetooth/
com.android.browser/
com.android.calculator2/
com.android.calendar/
com.android.camera/
com.android.certinstaller/
com.android.contacts/
com.android.customloca2/
com.android.defcontainer/
com.android.deskclock/
com.android.development/
com.android.development_settings/
com.android.dialer/
com.android.documentsui/
com.android.dreams.basic/
com.android.dreams.phototable/
com.android.email/
com.android.exchange/
com.android.externalstorage/
com.android.galaxy4/
com.android.gallery3d/
com.android.gesture.builder/
com.android.htmlviewer/
com.android.inputdevices/
com.android.inputmethod.latin/
com.android.keychain/
com.android.keyguard/
com.android.launcher/
com.android.location.fused/
com.android.magicsmoke/
com.android.mms/
com.android.music/
com.android.musicfx/
com.android.musicvis/
com.android.noisefield/
com.android.onetimeinitializer/
com.android.packageinstaller/
root@vbox86p:/ # cd data/data/
com.android.pacprocessor/
com.android.phasebeam/
com.android.phone/
com.android.printspooler/
com.android.providers.calendar/
com.android.providers.contacts/
com.android.providers.downloads.ui/
com.android.providers.downloads/
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.settings/
com.android.sharedstoragebackup/
com.android.shell/
com.android.smspush/
com.android.soundrecorder/
com.android.systemui/
com.android.videorecorder/
com.android.voicedialer/
com.android.vpndialogs/
com.android.wallpaper.holospiral/
com.android.wallpaper.livepicker/
com.android.wallpaper/
com.android.wallpapercropper/
com.cyanogenmod.filemanager/
com.dp.logcatapp/
com.example.android.apis/
com.example.android.livecubes/
com.genymotion.genyid/
com.genymotion.superuser/
com.genymotion.systempatcher/
com.svox.pico/
jakhar.aseem.diva/
jp.co.omronsoft.openmn/

```

Conclusion: - Thus we have studied Android security analysis for hand coding issues and insecure data storage using DIVA.