

# Mobile Application Pentesting- Part 2



Piyush Patil

May 17 · 5 min read ★



## Hardcoding issues



Get one more story in your member preview when you sign up. It's free.

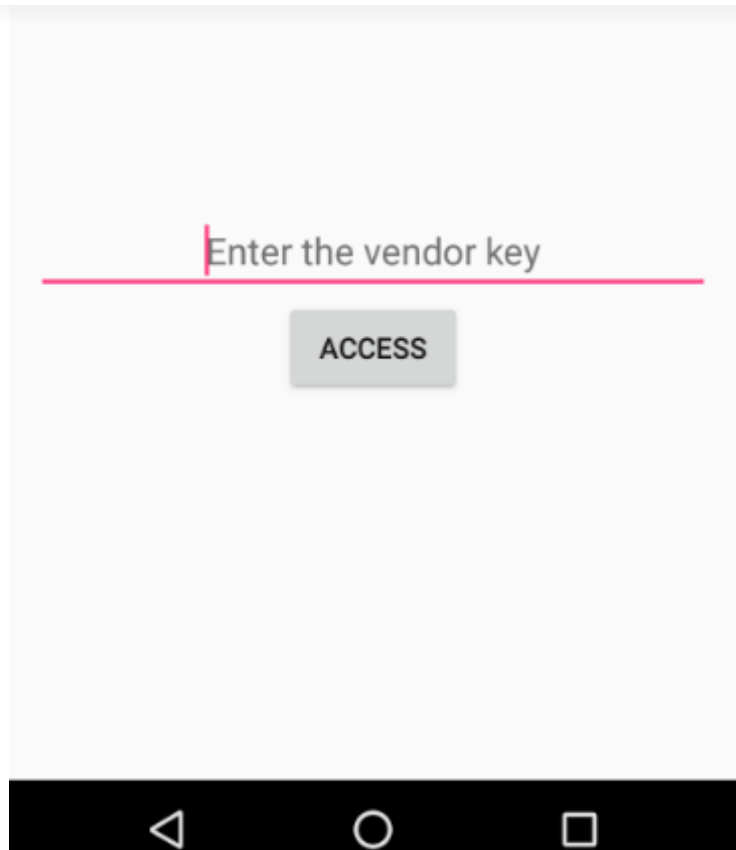


Sign up with Google



Sign up with Facebook


Already have an account? [Sign in](#)




This is an important vulnerability because using reverse engineering it would be possible to see that sensitive information. Examples could be access keys, passwords, etc ...


Let's try entering any random string just to see if it allows access or not.





**Get one more story in your member preview when you sign up. It's free.**

 Sign up with Google

 Sign up with Facebook

Already have an account? [Sign in](#)



How to download apk from installed application in mobile phone?

```
adb shell ps | grep -i appname => get package name
```

```
adb shell pm path package_name
```

```
adb pull mobile_app_path .
```

. means downloading mobile app to current directory



```
mv base.apk diva.apk
```

## Apktool

```
apktool d diva.apk -o diva
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

## Now where to look for java code files?

Let's ask *AndroidManifest.xml*

*AndroidManifest.xml* contains

- Specifies properties of the application
- Package Name
- Activities, Services, Broadcast, Receivers etc
- Permissions definitions and usage
- Info on external Libraries
  - Shared UID

The *AndroidManifest.xml* file tells that the package of the application is ***jakhar.assem.diva***

Going inside the package:-

Once reached to the inner folder */smali/jakhar/aseem/diva*, there is the Java source code of all the activities used by the application

Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

Here you can see **HardcodeActivity.smali**

But smali is hard to understand as compared to java.

Lets try to decompile app and get all code in .java format instead of .smali

## JADX

/jadx application.apk -d outputfolder



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

There will be so many warnings and errors but don't worry, it doesn't matter.

```
cd diva
```

```
cd sources/jakhar/aseem/diva
```

```
cat HardcodeActivity.java
```



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



• • •

## Hardcoding Issues

*Part 2 (Shared Object Files / Libraries)*



Get one more story in your member preview when you sign up. It's free.

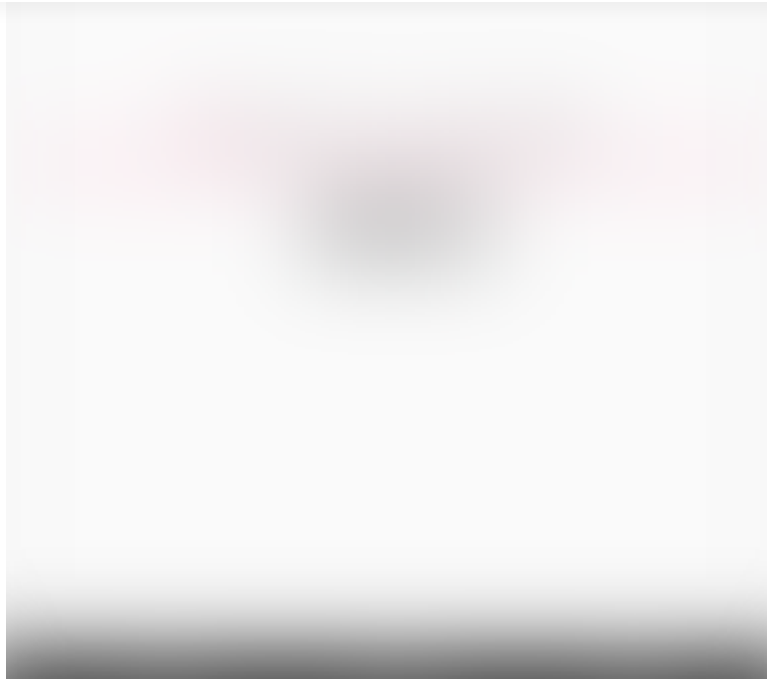


Sign up with Google

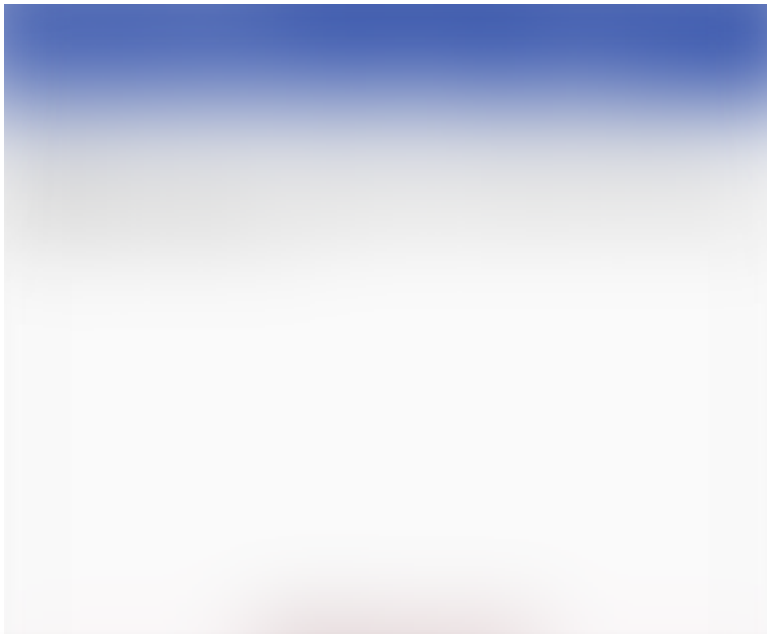


Sign up with Facebook

Already have an account? [Sign in](#)



Let's try any random vendor key



**Get one more story in your member preview when you sign up. It's free.**



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



```
cd sources/jakhar/aseem/diva
```



```
cat Hardcode2Activity.java
```



**Get one more story in your member preview when you sign up. It's free.**



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

## Android Native Library

Google develops the Android Native Development Kit (NDK) beside Android SDK. The purpose of NDK is helping developers to build libraries in C or C++ . Some of the benefits of using native libraries are:

- Using Native Activities
- Access physical device components like sensors
- Reusing old C or C++ code in Android application
- Building extra fast application when you need high computational features

When the native library built, The Java Native Interface (JNI) handles the communication between the native library and java based code.

Now let's check the code of class **DivaJni.java**



cat DivaJni.java



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

Open the apk extracted folder which we did using apktool.



**ls \*** => list out all the files within each directory.

There are different library files based on architectures. Try to open any one of them .

`cat x86/libdivajni.so`



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

We can run strings command on lib file, but then it will be difficult to find access code.

**Lets try another way**

```
objdump -s -j .rodata libdivajni.so
```

.rodata segment => stores read only data and constant data of the program



**Get one more story in your member preview when you sign up. It's free.**



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

. . .

## Insecure Data Storage

*Part -1*



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)

Let's enter the username as **piyush** and password as **patil**.



Get one more story in your member preview when you sign up. It's free.




Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



As the code shows, DIVA uses PreferenceManager to save plain sensitive data. Preferences is an Android lightweight mechanism to store and retrieve pairs of primitive data types (also called Maps, and Associative Arrays).

**PreferenceManager** saves data in a XML file located in application path. Any application that has a root access can read those sensitive data.

```
/data/data/<APPLICATION NAME>/shared_prefs/*.xml
```


```
adb shell su
```

```
cd /data/data/jakhar.aseem.diva/shared_prefs
```



Get one more story in your member preview when you sign up. It's free. ×

 Sign up with Google

 Sign up with Facebook

Already have an account? [Sign in](#)



**Piyush Patil**

Reverse Engineering, Penetration Testing( Web, Mobile, IoT, Network, Infra)

Follow

## More From Medium

Top on Medium



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

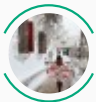
Already have an account? [Sign in](#)



Top on Medium



## Apparently I Was Nothing But A Woo-Girl



Michelle Ann in Fearless She Wrote

Nov 13 · 4 min read ★



4.98K



Top on Medium



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)



# How to Predict the End of a Relationship



Colleen Murphy in Mindful Muse

Nov 22 · 5 min read ★



2.4K



**Medium**

[About](#) [Help](#) [Legal](#)



Get one more story in your member preview when you sign up. It's free.



Sign up with Google



Sign up with Facebook

Already have an account? [Sign in](#)