# Android Pentesting

## Setup:

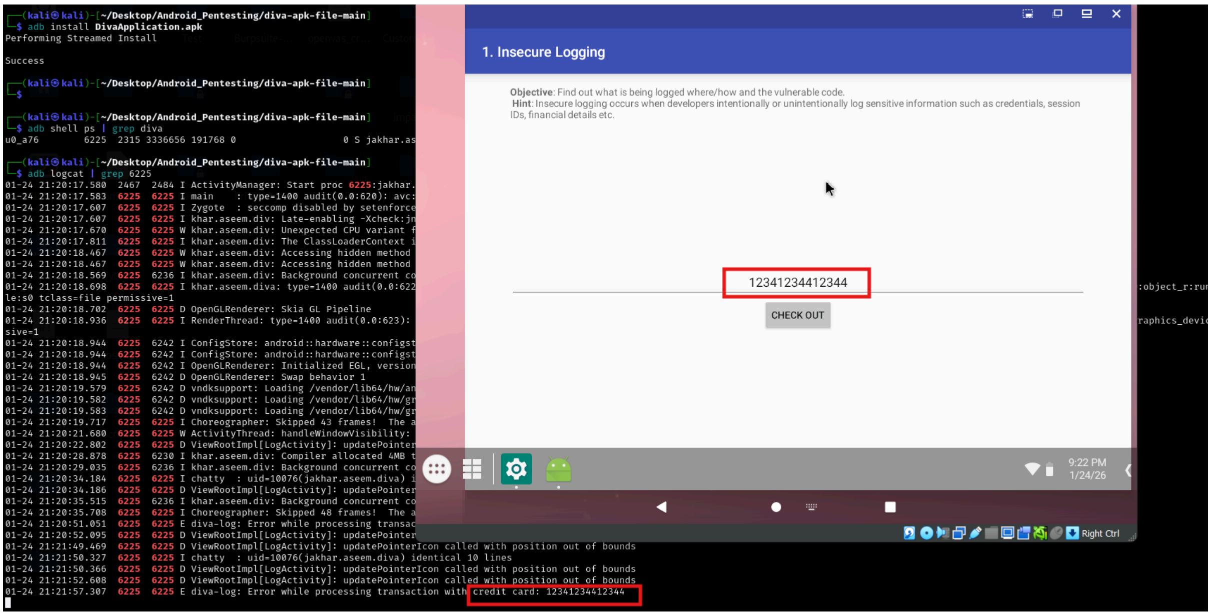
Attacker - Kali (Virtual Box)
Target Env  - Android (Virtualbox)

## Overview:

Performed a pentesting on an android application using various tool like apktool, jadx, and adb , while performing the analysis i have discovered several vulnerabilities like “Insecure logging” and Unwanted permissions required by the application.

## Steps Followed:

1. Converted the apk file into a java code using jadx
2. Using ADB tool and insecure logging has identified with the help of logcat



```
┌──(kali㉿kali)-[~/Desktop/Android_Pentesting/diva-apk-file-main]
└─$ adb install DivaApplication.apk
Performing Streamed Install

Success

┌──(kali㉿kali)-[~/Desktop/Android_Pentesting/diva-apk-file-main]
└─$

┌──(kali㉿kali)-[~/Desktop/Android_Pentesting/diva-apk-file-main]
└─$ adb shell ps | grep diva
u0_a76        6225  2315 3336656 191768 0                   0 S jakhar.as

┌──(kali㉿kali)-[~/Desktop/Android_Pentesting/diva-apk-file-main]
└─$ adb logcat | grep 6225
01-24 21:20:17.580  2467  2484 I ActivityManager: Start proc 6225:jakhar.
01-24 21:20:17.583  6225  6225 I main    : type=1400 audit(0.0:620): avc:
01-24 21:20:17.607  6225  6225 I Zygote  : seccomp disabled by setenforce
01-24 21:20:17.607  6225  6225 I khar.aseem.div: Late-enabling -Xcheck:jn
01-24 21:20:17.670  6225  6225 W khar.aseem.div: Unexpected CPU variant f
01-24 21:20:17.811  6225  6225 I khar.aseem.div: The ClassLoaderContext i
01-24 21:20:18.467  6225  6225 W khar.aseem.div: Accessing hidden method
01-24 21:20:18.467  6225  6225 W khar.aseem.div: Accessing hidden method
01-24 21:20:18.569  6225  6236 I khar.aseem.div: Background concurrent co
01-24 21:20:18.698  6225  6225 I khar.aseem.diva: type=1400 audit(0.0:622
le:s0 tclass=file permissive=1
01-24 21:20:18.702  6225  6225 D OpenGLRenderer: Skia GL Pipeline
01-24 21:20:18.936  6225  6225 I RenderThread: type=1400 audit(0.0:623):
sive=1
01-24 21:20:18.944  6225  6242 I ConfigStore: android::hardware::configst
01-24 21:20:18.944  6225  6242 I ConfigStore: android::hardware::configst
01-24 21:20:18.944  6225  6242 I OpenGLRenderer: Initialized EGL, version
01-24 21:20:18.945  6225  6242 D OpenGLRenderer: Swap behavior 1
01-24 21:20:19.579  6225  6242 D vndksupport: Loading /vendor/lib64/hw/an
01-24 21:20:19.582  6225  6242 D vndksupport: Loading /vendor/lib64/hw/gr
01-24 21:20:19.583  6225  6242 D vndksupport: Loading /vendor/lib64/hw/gr
01-24 21:20:19.717  6225  6225 I Choreographer: Skipped 43 frames!  The a
01-24 21:20:21.680  6225  6225 W ActivityThread: handleWindowVisibility:
01-24 21:20:22.802  6225  6225 D ViewRootImpl[LogActivity]: updatePointer
01-24 21:20:28.878  6225  6230 I khar.aseem.div: Compiler allocated 4MB t
01-24 21:20:29.035  6225  6236 I khar.aseem.div: Background concurrent co
01-24 21:20:34.184  6225  6225 I chatty  : uid=10076(jakhar.aseem.diva) i
01-24 21:20:34.186  6225  6225 D ViewRootImpl[LogActivity]: updatePointer
01-24 21:20:35.515  6225  6236 I khar.aseem.div: Background concurrent co
01-24 21:20:35.708  6225  6225 I Choreographer: Skipped 48 frames!  The a
01-24 21:20:51.051  6225  6225 E diva-log: Error while processing transac
01-24 21:20:52.095  6225  6225 D ViewRootImpl[LogActivity]: updatePointer
01-24 21:21:49.469  6225  6225 D ViewRootImpl[LogActivity]: updatePointerIcon called with position out of bounds
01-24 21:21:50.327  6225  6225 I chatty  : uid=10076(jakhar.aseem.diva) identical 10 lines
01-24 21:21:50.366  6225  6225 D ViewRootImpl[LogActivity]: updatePointerIcon called with position out of bounds
01-24 21:21:52.608  6225  6225 D ViewRootImpl[LogActivity]: updatePointerIcon called with position out of bounds
01-24 21:21:57.307  6225  6225 E diva-log: Error while processing transaction with credit card: 12341234412344
```

```
:object_r:ru
raphics_devi
```

1. Insecure Logging

**Objective**: Find out what is being logged where/how and the vulnerable code.
**Hint**: Insecure logging occurs when developers intentionally or unintentionally log sensitive information such as credentials, session IDs, financial details etc.

12341234412344