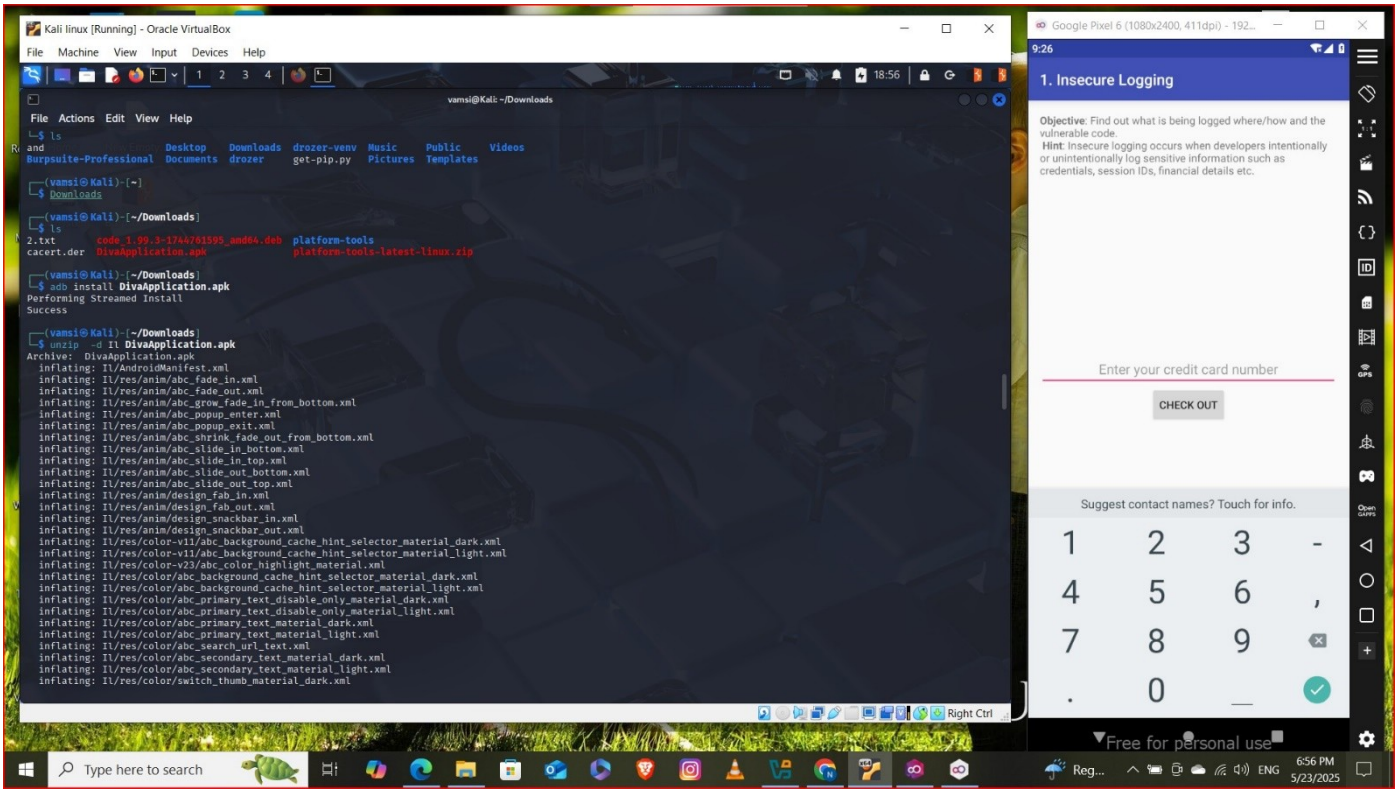
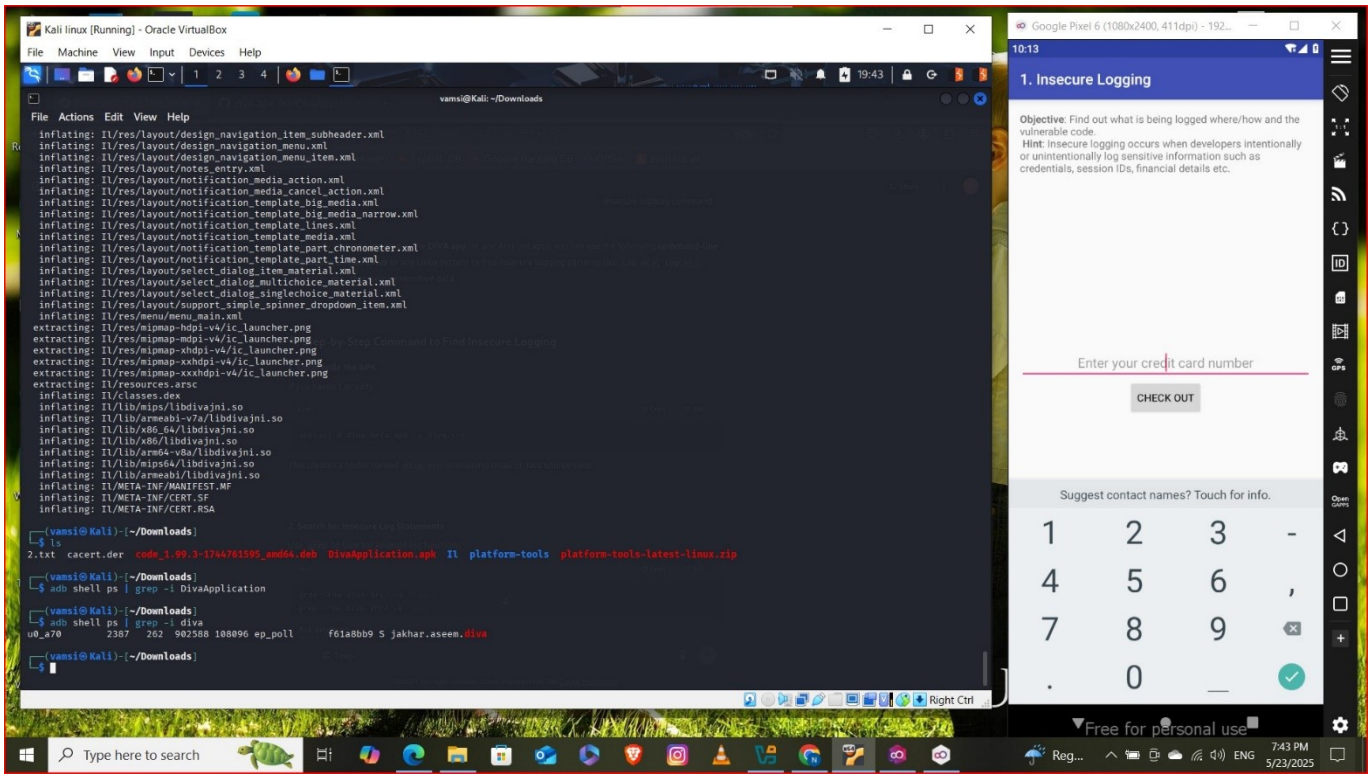
CYBER SECURED INDIA

ASSIGNMENT – 12

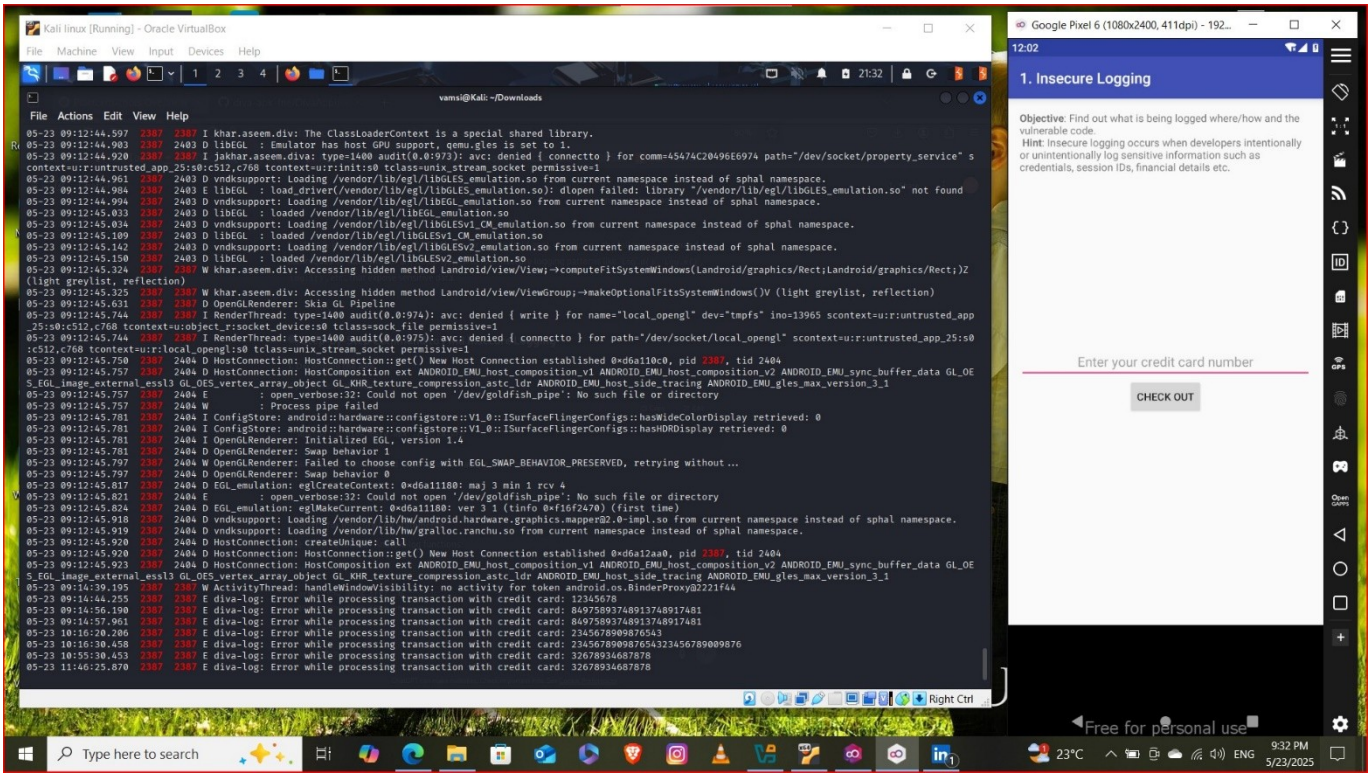
DIVA (Damn Insecure and Vulnerable App)

➢ 1.INSECURE LOGGING

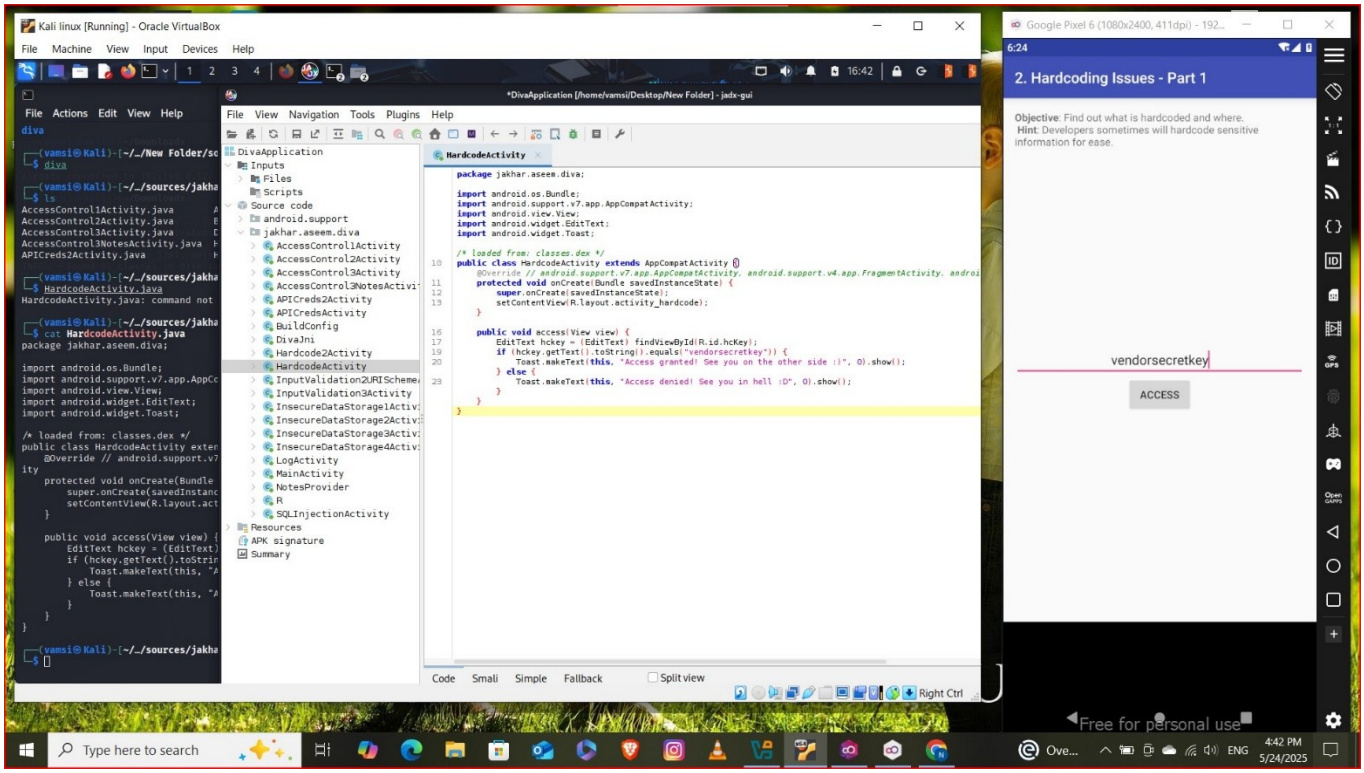


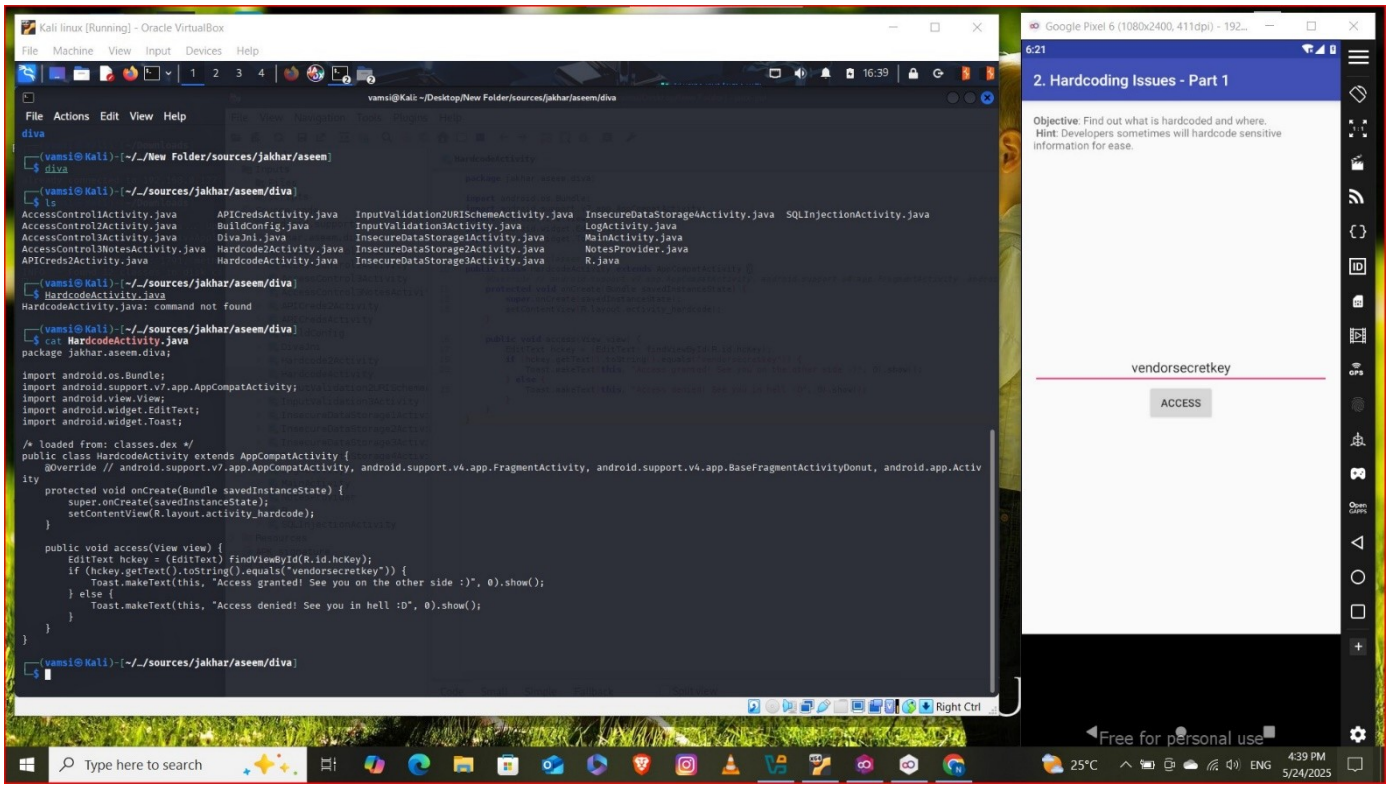

Kali linux [Running] - Oracle VirtualBox
vamsi@Kali: ~/Downloads
inflating: I1/res/layout/notification_template_lines.xml
inflating: I1/res/layout/notification_template_media.xml
inflating: I1/res/layout/notification_template_part_chronometer.xml
inflating: I1/res/layout/notification_template_part_time.xml
inflating: I1/res/layout/select_dialog_item_material.xml
inflating: I1/res/layout/select_dialog_multichoice_material.xml
inflating: I1/res/layout/select_dialog_singlechoice_material.xml
inflating: I1/res/layout/support_simple_spinner_dropdown_item.xml
inflating: I1/res/menu/menu_main.xml
extracting: I1/res/mipmap-hdpi-v4/ic_launcher.png
extracting: I1/res/mipmap-mdpi-v4/ic_launcher.png
extracting: I1/res/mipmap-xhdpi-v4/ic_launcher.png
extracting: I1/res/mipmap-xxhdpi-v4/ic_launcher.png
extracting: I1/res/mipmap-xxxhdpi-v4/ic_launcher.png
extracting: I1/resources.arsc
inflating: I1/classes.dex
inflating: I1/lib/mips/libdivajni.so
inflating: I1/lib/armeabi-v7a/libdivajni.so
inflating: I1/lib/x86_64/libdivajni.so
inflating: I1/lib/x86/libdivajni.so
inflating: I1/lib/arm64-v8a/libdivajni.so
inflating: I1/lib/mips64/libdivajni.so
inflating: I1/lib/armeabi/libdivajni.so
inflating: I1/META-INF/MANIFEST.MF
inflating: I1/META-INF/CERT.SF
inflating: I1/META-INF/CERT.RSA
(vamsi㉿Kali)-[~/Downloads]
$ ls
2.txt cacert.der code_1.99.3-1744761595_amd64.deb DivaApplication.apk I1 platform-tools platform-tools-latest-linux.zip
(vamsi㉿Kali)-[~/Downloads]
$ adb shell ps | grep -i DivaApplication
(vamsi㉿Kali)-[~/Downloads]
$ adb shell ps | grep -i diva
u0_a70 2387 262 902588 108096 ep_poll f61a8bb9 S jakhar.aseem.diva
(vamsi㉿Kali)-[~/Downloads]
$
Google Pixel 6 (1080x2400, 411dpi) - 192...
10:13
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.
Enter your credit card number
CHECK OUT
Suggest contact names? Touch for info.
Free for personal use
Type here to search
7:43 PM
5/23/2025

➢

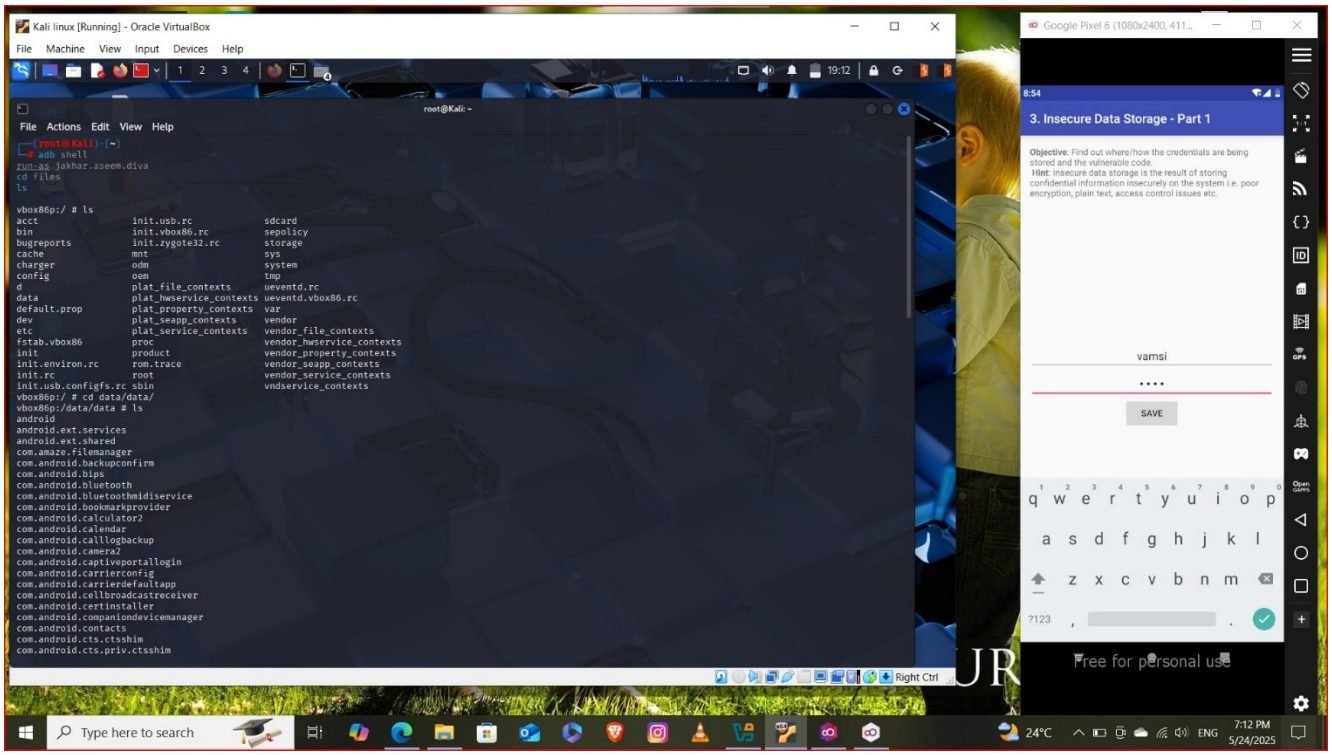

Kali linux [Running] - Oracle VirtualBox
vamsi@Kali: ~/Downloads
05-23 09:12:44.597 2387 2387 I khar.aseem.div: The ClassLoaderContext is a special shared library.
05-23 09:12:44.903 2387 2403 D libEGL : Emulator has host GPU support, qemu.gles is set to 1.
05-23 09:12:44.920 2387 2387 I jakhar.aseem.diva: type=1400 audit(0.0:973): avc: denied { connectto } for comm=45474C20496E6974 path="/dev/socket/property_service" scontext=u:r:untrusted_app_25:s0:c512,c768 tcontext=u:r:init:s0 tclass=unix_stream_socket permissive=1
05-23 09:12:44.961 2387 2403 D vndksupport: Loading /vendor/lib/egl/libGLES_emulation.so from current namespace instead of sphal namespace.
05-23 09:12:44.984 2387 2403 E libEGL : load_driver(/vendor/lib/egl/libGLES_emulation.so): dlopen failed: library "/vendor/lib/egl/libGLES_emulation.so" not found
05-23 09:12:44.994 2387 2403 D vndksupport: Loading /vendor/lib/egl/libEGL_emulation.so from current namespace instead of sphal namespace.
05-23 09:12:45.033 2387 2403 D libEGL : loaded /vendor/lib/egl/libEGL_emulation.so
05-23 09:12:45.034 2387 2403 D vndksupport: Loading /vendor/lib/egl/libGLESv1_CM_emulation.so from current namespace instead of sphal namespace.
05-23 09:12:45.109 2387 2403 D libEGL : loaded /vendor/lib/egl/libGLESv1_CM_emulation.so
05-23 09:12:45.142 2387 2403 D vndksupport: Loading /vendor/lib/egl/libGLESv2_emulation.so from current namespace instead of sphal namespace.
05-23 09:12:45.150 2387 2403 D libEGL : loaded /vendor/lib/egl/libGLESv2_emulation.so
05-23 09:12:45.324 2387 2387 W khar.aseem.div: Accessing hidden method Landroid/view/View;→computeFitSystemWindows(Landroid/graphics/Rect;Landroid/graphics/Rect;)Z (light greylist, reflection)
05-23 09:12:45.325 2387 2387 W khar.aseem.div: Accessing hidden method Landroid/view/ViewGroup;→makeOptionalFitsSystemWindows()V (light greylist, reflection)
05-23 09:12:45.631 2387 2387 D OpenGLRenderer: Skia GL Pipeline
05-23 09:12:45.744 2387 2387 I RenderThread: type=1400 audit(0.0:974): avc: denied { write } for name="local_opengl" dev="tmpfs" ino=13965 scontext=u:r:untrusted_app_25:s0:c512,c768 tcontext=u:object_r:socket_device:s0 tclass=sock_file permissive=1
05-23 09:12:45.744 2387 2387 I RenderThread: type=1400 audit(0.0:975): avc: denied { connectto } for path="/dev/socket/local_opengl" scontext=u:r:untrusted_app_25:s0:c512,c768 tcontext=u:r:local_opengl:s0 tclass=unix_stream_socket permissive=1
05-23 09:12:45.750 2387 2404 D HostConnection::get() New Host Connection established 0×d6a110c0, pid 2387, tid 2404
05-23 09:12:45.757 2387 2404 D HostConnection: HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_gles_max_version_3_1
05-23 09:12:45.757 2387 2404 E : open_verbose:32: Could not open '/dev/goldfish_pipe': No such file or directory
05-23 09:12:45.757 2387 2404 W : Process pipe failed
05-23 09:12:45.781 2387 2404 I ConfigStore: android::hardware::configstore::V1_0::ISurfaceFlingerConfigs::hasWideColorDisplay retrieved: 0
05-23 09:12:45.781 2387 2404 I ConfigStore: android::hardware::configstore::V1_0::ISurfaceFlingerConfigs::hasHDRDisplay retrieved: 0
05-23 09:12:45.781 2387 2404 I OpenGLRenderer: Initialized EGL, version 1.4
05-23 09:12:45.781 2387 2404 D OpenGLRenderer: Swap behavior 1
05-23 09:12:45.797 2387 2404 W OpenGLRenderer: Failed to choose config with EGL_SWAP_BEHAVIOR_PRESERVED, retrying without...
05-23 09:12:45.797 2387 2404 D OpenGLRenderer: Swap behavior 0
05-23 09:12:45.817 2387 2404 D EGL_emulation: eglCreateContext: 0×d6a11180: maj 3 min 1 rcv 4
05-23 09:12:45.821 2387 2404 E : open_verbose:32: Could not open '/dev/goldfish_pipe': No such file or directory
05-23 09:12:45.824 2387 2404 D EGL_emulation: eglMakeCurrent: 0×d6a11180: ver 3 1 (tinfo 0×f16f2470) (first time)
05-23 09:12:45.918 2387 2404 D vndksupport: Loading /vendor/lib/hw/android.hardware.graphics.mapper@2.0-impl.so from current namespace instead of sphal namespace.
05-23 09:12:45.919 2387 2404 D vndksupport: Loading /vendor/lib/hw/gralloc.ranchu.so from current namespace instead of sphal namespace.
05-23 09:12:45.920 2387 2404 D HostConnection: createUnique: call
05-23 09:12:45.920 2387 2404 D HostConnection: HostConnection::get() New Host Connection established 0×d6a12aa0, pid 2387, tid 2404
05-23 09:12:45.923 2387 2404 D HostConnection: HostComposition ext ANDROID_EMU_host_composition_v1 ANDROID_EMU_host_composition_v2 ANDROID_EMU_sync_buffer_data GL_OES_EGL_image_external_essl3 GL_OES_vertex_array_object GL_KHR_texture_compression_astc_ldr ANDROID_EMU_host_side_tracing ANDROID_EMU_gles_max_version_3_1
05-23 09:14:39.195 2387 2387 W ActivityThread: handleWindowVisibility: no activity for token android.os.BinderProxy@2221f44
05-23 09:14:44.255 2387 2387 E diva-log: Error while processing transaction with credit card: 12345678
05-23 09:14:56.190 2387 2387 E diva-log: Error while processing transaction with credit card: 8497589374891374891748917481
05-23 09:14:57.961 2387 2387 E diva-log: Error while processing transaction with credit card: 8497589374891374891748917481
05-23 10:16:20.206 2387 2387 E diva-log: Error while processing transaction with credit card: 23456789098765432345678909876
05-23 10:16:30.450 2387 2387 E diva-log: Error while processing transaction with credit card: 23456789098765432345678909876
05-23 10:55:30.453 2387 2387 E diva-log: Error while processing transaction with credit card: 32678934687878
05-23 11:46:25.870 2387 2387 E diva-log: Error while processing transaction with credit card: 32678934687878
Google Pixel 6 (1080x2400, 411dpi) - 192...
12:02
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.
Enter your credit card number
CHECK OUT
Free for personal use
Type here to search
9:32 PM
5/23/2025

➢ 2. HARDCODING ISSUES PART 1

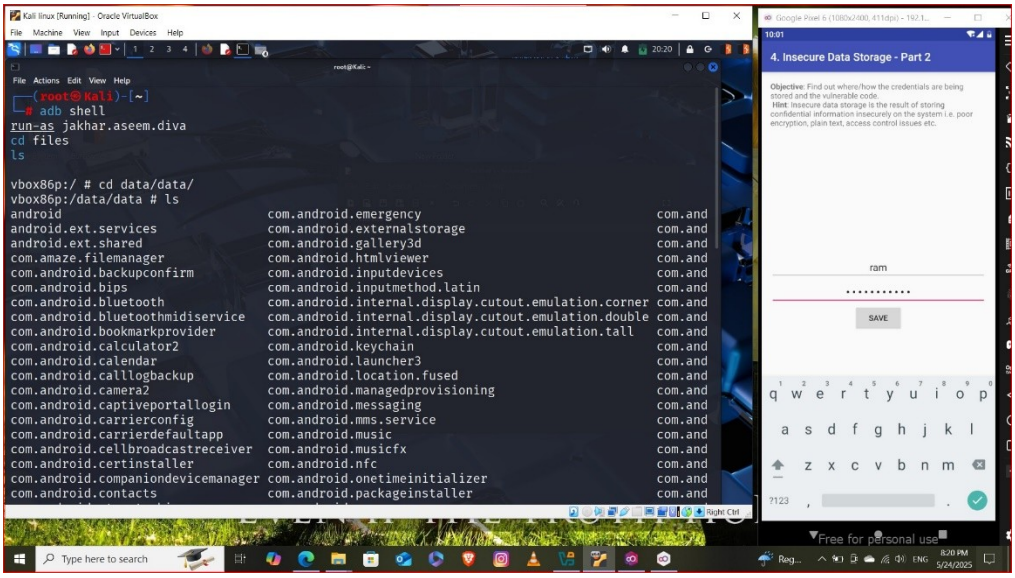




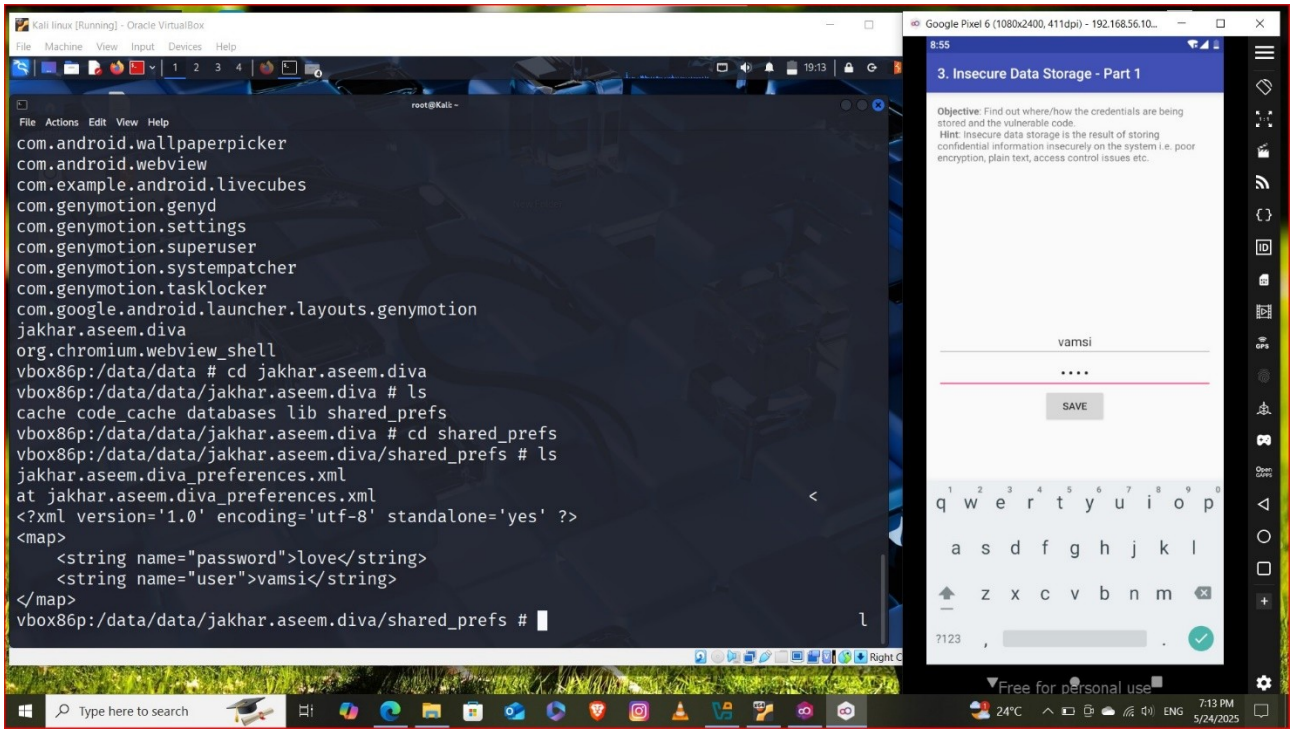
3. INSECURE DATA STORAGE-PART 1

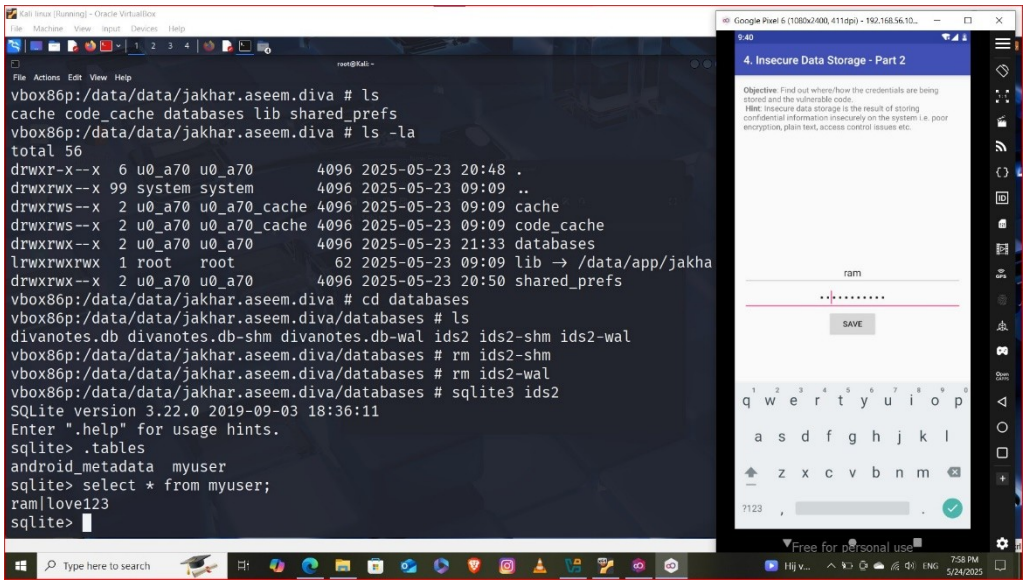


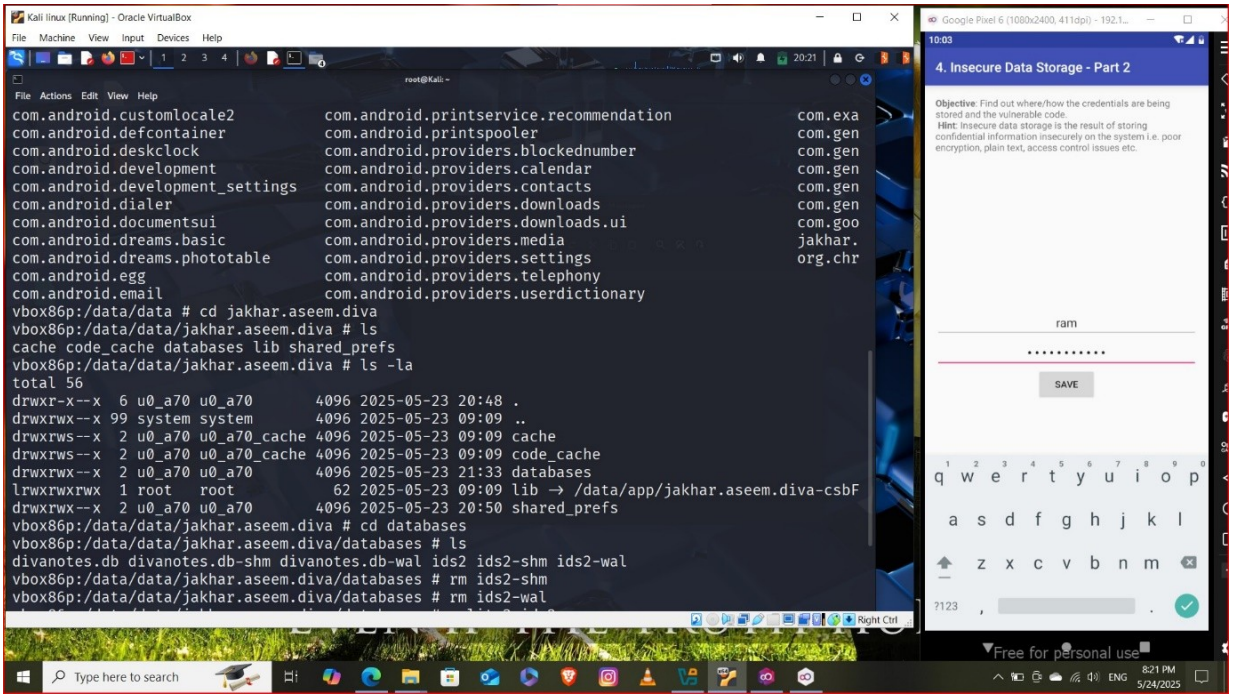
4.



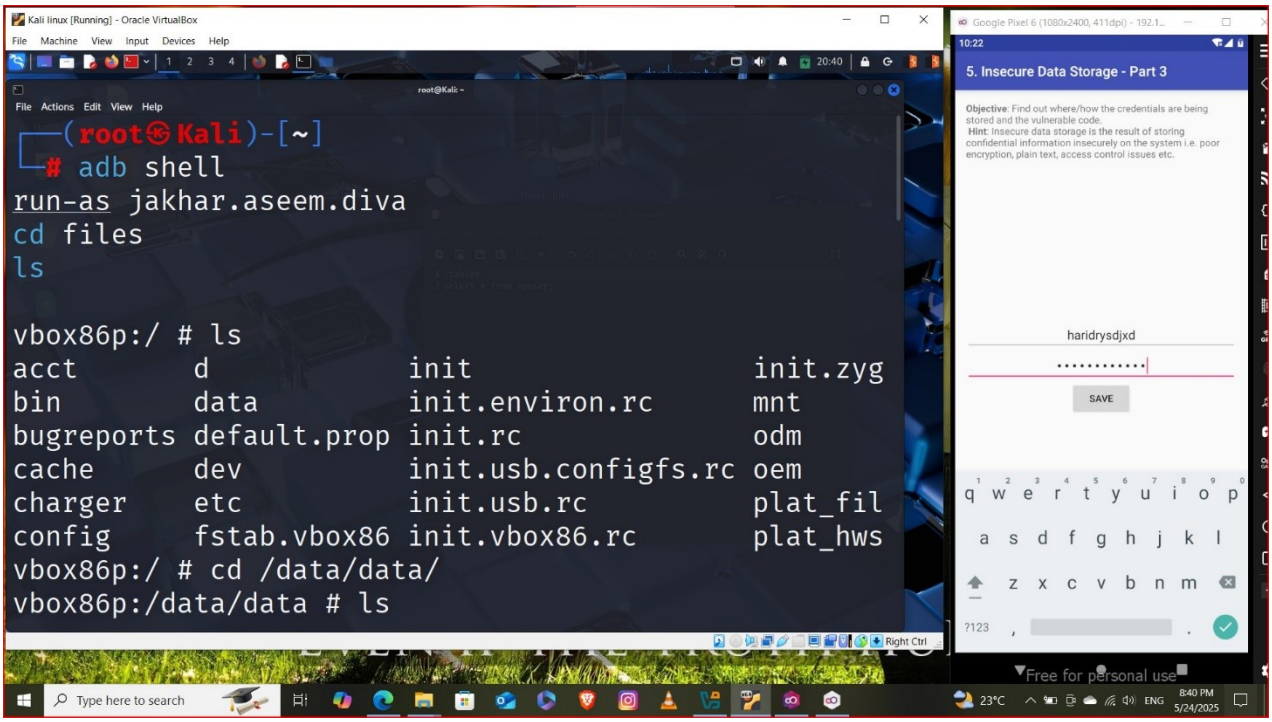
INSECURE DATA STORAGE-PART 2

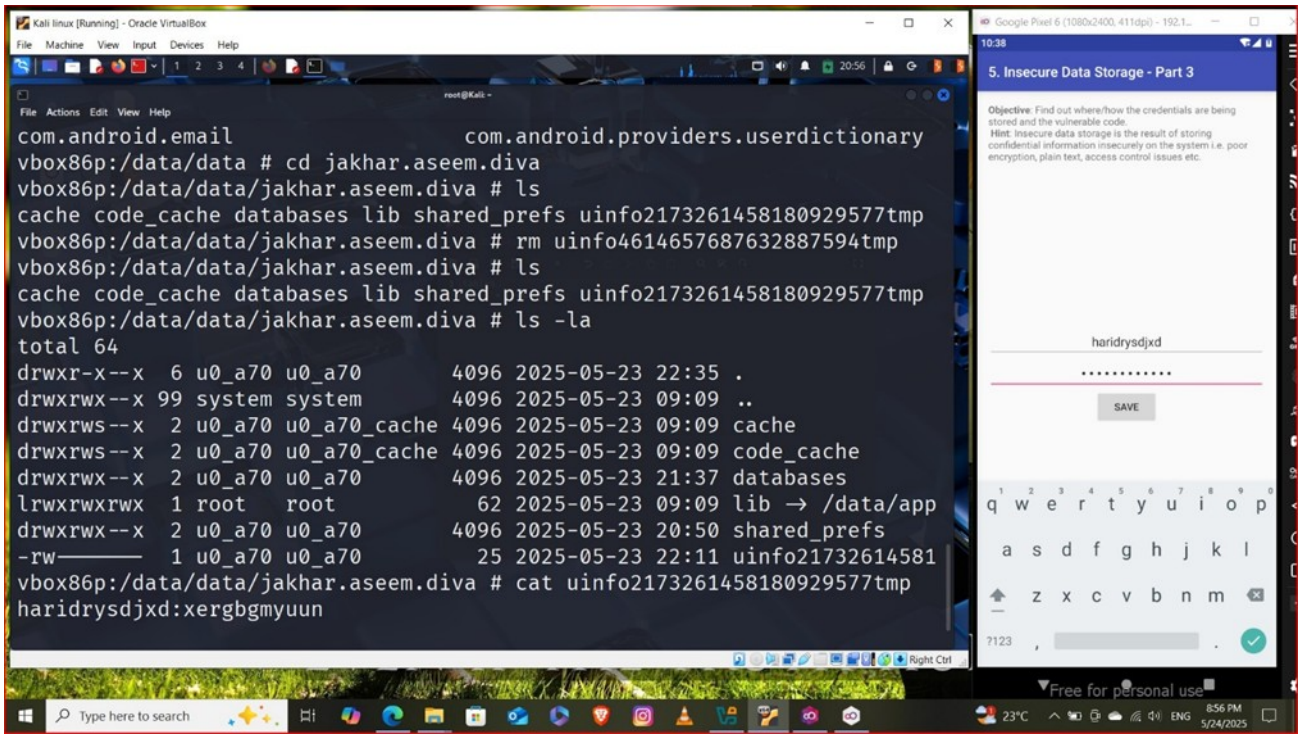



vbox86p:/data/data/jakhar.aseem.diva # ls
cache code_cache databases lib shared_prefs
vbox86p:/data/data/jakhar.aseem.diva # ls -la
total 56
drwxr-x--x 6 u0_a70 u0_a70   4096 2025-05-23 20:48 .
drwxrwx--x 99 system system   4096 2025-05-23 09:09 ..
drwxrws--x 2 u0_a70 u0_a70_cache 4096 2025-05-23 09:09 cache
drwxrws--x 2 u0_a70 u0_a70_cache 4096 2025-05-23 09:09 code_cache
drwxrwx--x 2 u0_a70 u0_a70   4096 2025-05-23 21:33 databases
lrwxrwxrwx 1 root   root   62 2025-05-23 09:09 lib → /data/app/jakha
drwxrwx--x 2 u0_a70 u0_a70   4096 2025-05-23 20:50 shared_prefs
vbox86p:/data/data/jakhar.aseem.diva # cd databases
vbox86p:/data/data/jakhar.aseem.diva/databases # ls
divanotes.db divanotes.db-shm divanotes.db-wal ids2 ids2-shm ids2-wal
vbox86p:/data/data/jakhar.aseem.diva/databases # rm ids2-shm
vbox86p:/data/data/jakhar.aseem.diva/databases # rm ids2-wal
vbox86p:/data/data/jakhar.aseem.diva/databases # sqlite3 ids2
SQLite version 3.22.0 2019-09-03 18:36:11
Enter ".help" for usage hints.
sqlite> .tables
android_metadata myuser
sqlite> select * from myuser;
ram|love123
sqlite>
4. Insecure Data Storage - Part 2
ram
SAVE

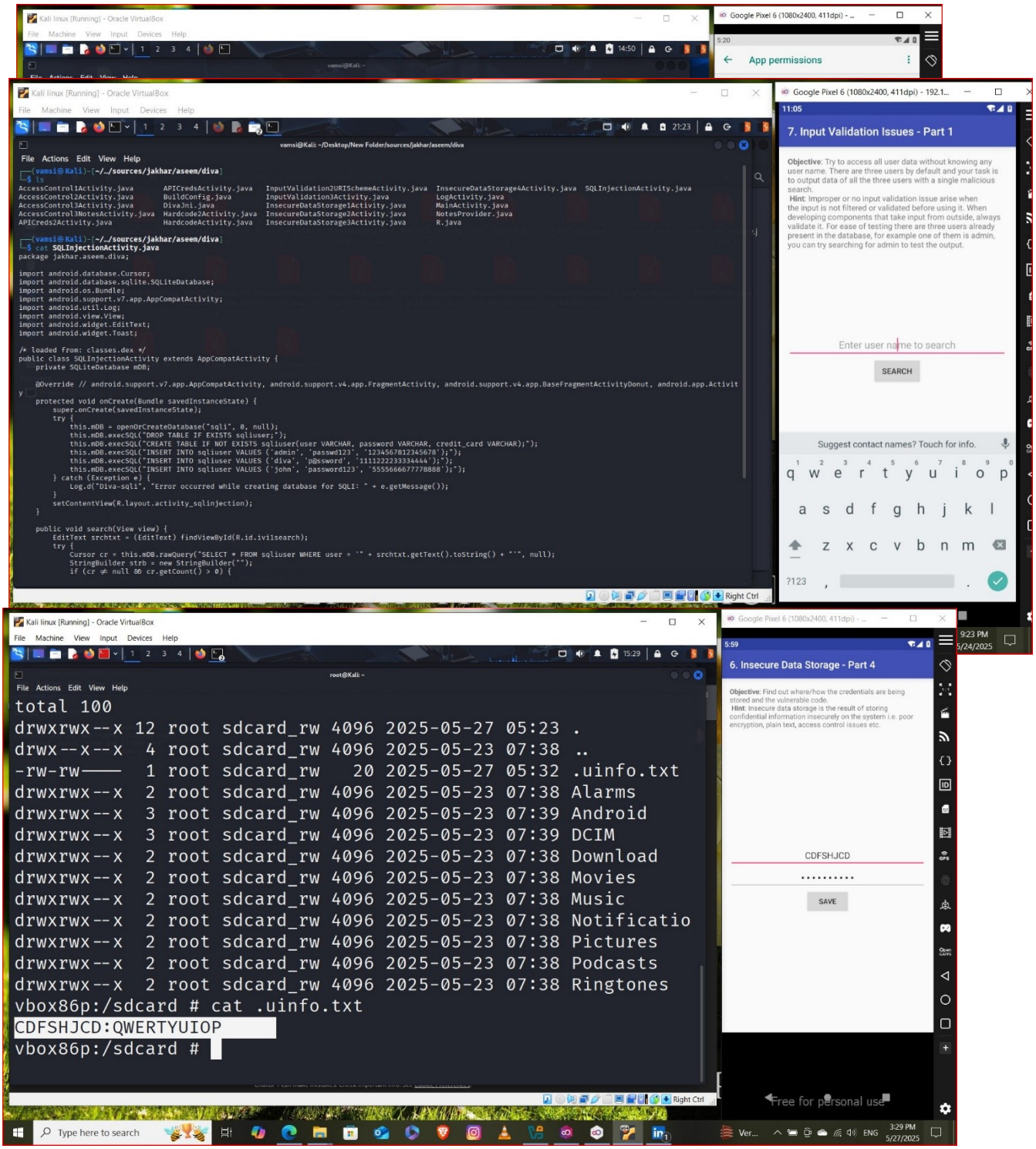

com.android.customlocale2
com.android.defcontainer
com.android.deskclock
com.android.development
com.android.development_settings
com.android.dialer
com.android.documentsui
com.android.dreams.basic
com.android.dreams.phototable
com.android.egg
com.android.email
com.android.printservice.recommendation
com.android.printspooler
com.android.providers.blockednumber
com.android.providers.calendar
com.android.providers.contacts
com.android.providers.downloads
com.android.providers.downloads.ui
com.android.providers.media
com.android.providers.settings
com.android.providers.telephony
com.android.providers.userdictionary
vbox86p:/data/data # cd jakhar.aseem.diva
vbox86p:/data/data/jakhar.aseem.diva # ls
cache code_cache databases lib shared_prefs
vbox86p:/data/data/jakhar.aseem.diva # ls -la
total 56
drwxr-x--x 6 u0_a70 u0_a70   4096 2025-05-23 20:48 .
drwxrwx--x 99 system system   4096 2025-05-23 09:09 ..
drwxrws--x 2 u0_a70 u0_a70_cache 4096 2025-05-23 09:09 cache
drwxrws--x 2 u0_a70 u0_a70_cache 4096 2025-05-23 09:09 code_cache
drwxrwx--x 2 u0_a70 u0_a70   4096 2025-05-23 21:33 databases
lrwxrwxrwx 1 root   root   62 2025-05-23 09:09 lib → /data/app/jakhar.aseem.diva-csbF
drwxrwx--x 2 u0_a70 u0_a70   4096 2025-05-23 20:50 shared_prefs
vbox86p:/data/data/jakhar.aseem.diva # cd databases
vbox86p:/data/data/jakhar.aseem.diva/databases # ls
divanotes.db divanotes.db-shm divanotes.db-wal ids2 ids2-shm ids2-wal
vbox86p:/data/data/jakhar.aseem.diva/databases # rm ids2-shm
vbox86p:/data/data/jakhar.aseem.diva/databases # rm ids2-wal
4. Insecure Data Storage - Part 2
ram
SAVE

5.INSECURE DATA STORAGE-PART 3



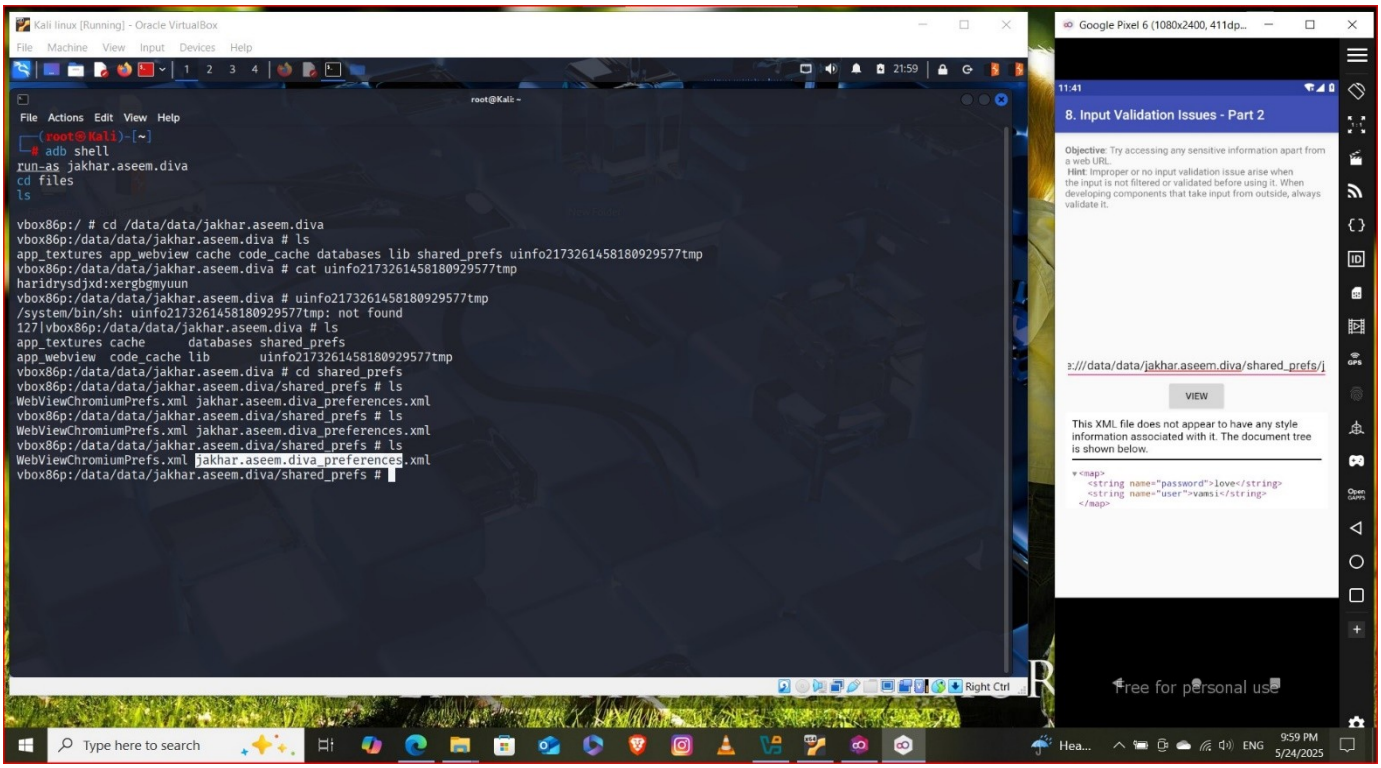


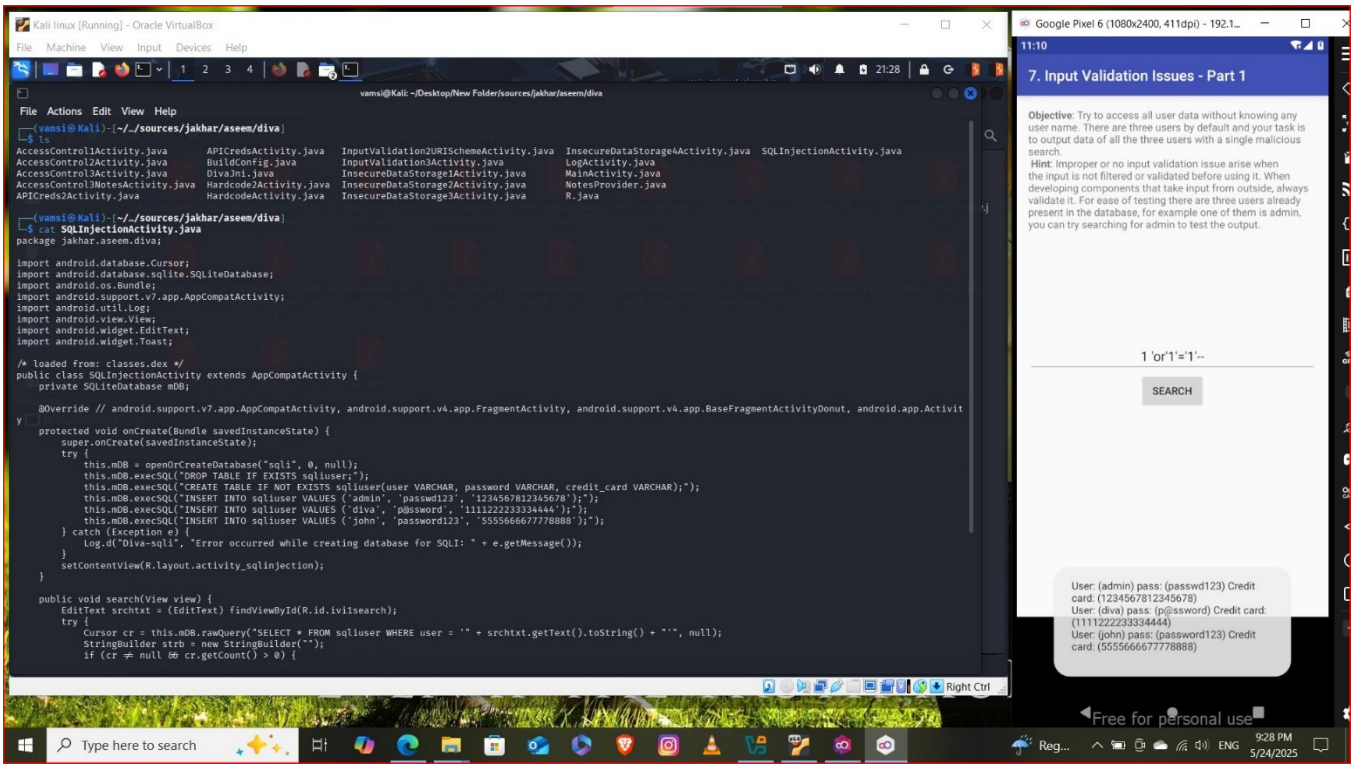
6. Insecure Data Storage-Part 4



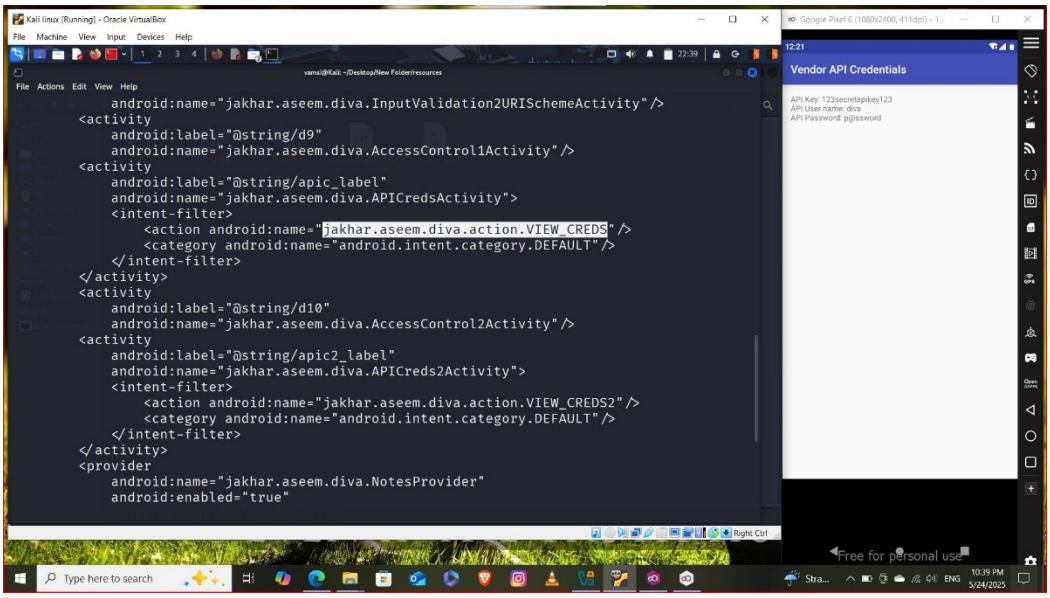
7. Input Validation Issues-Part 1

8 . Input Validation Issues-Part 2

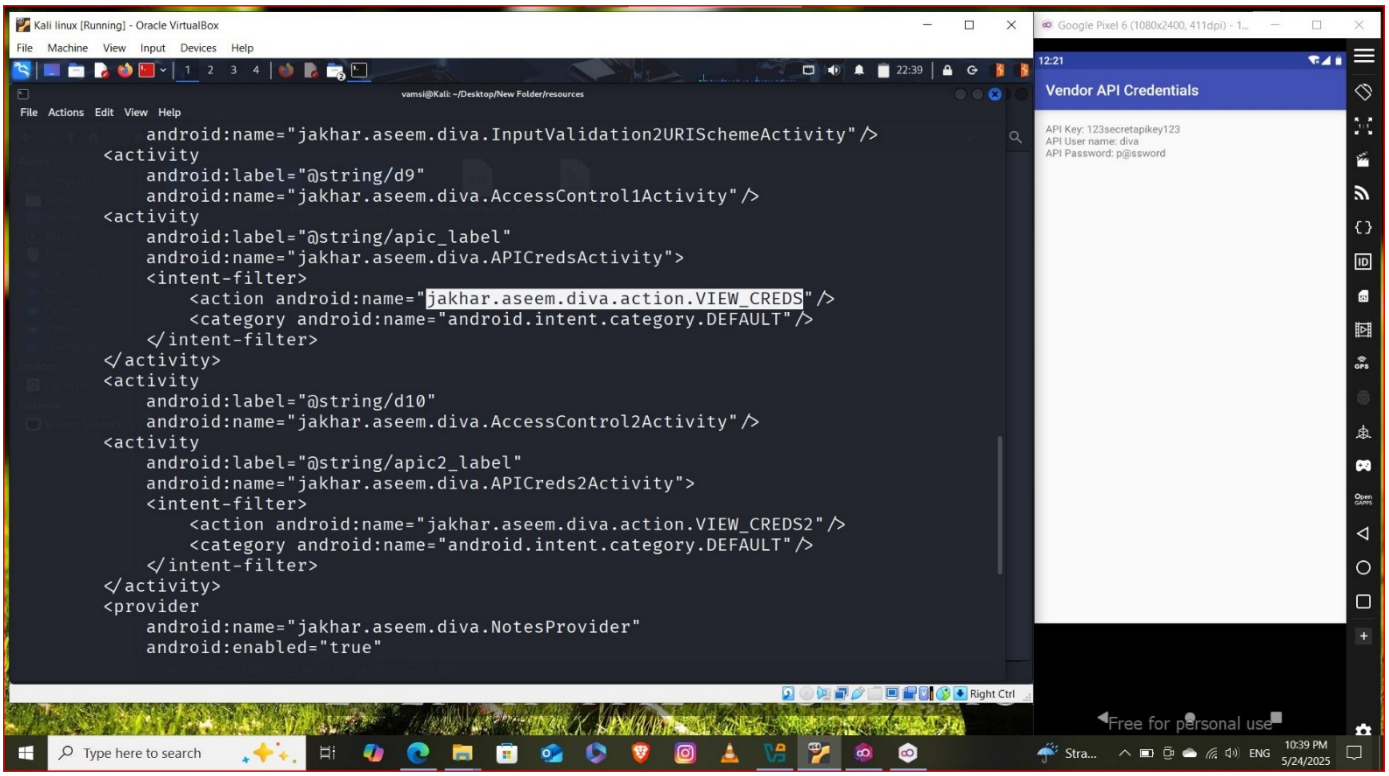


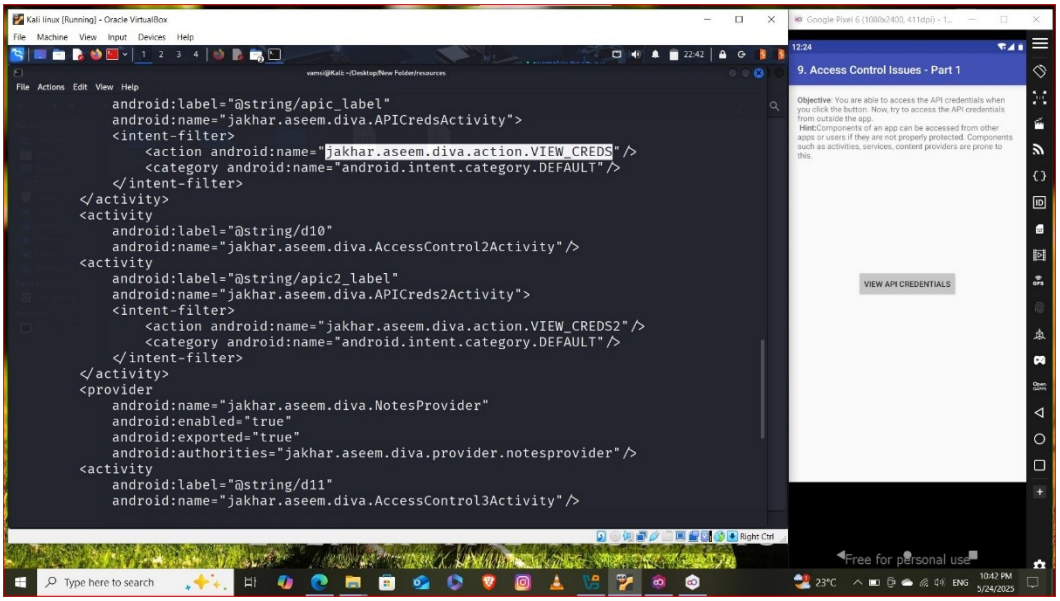


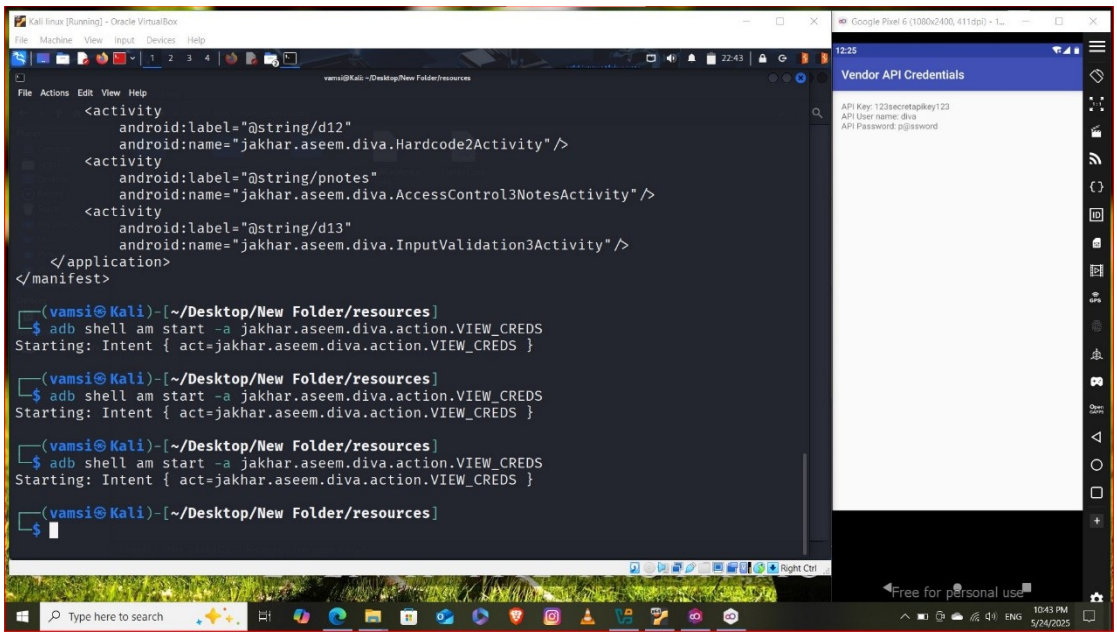
9.



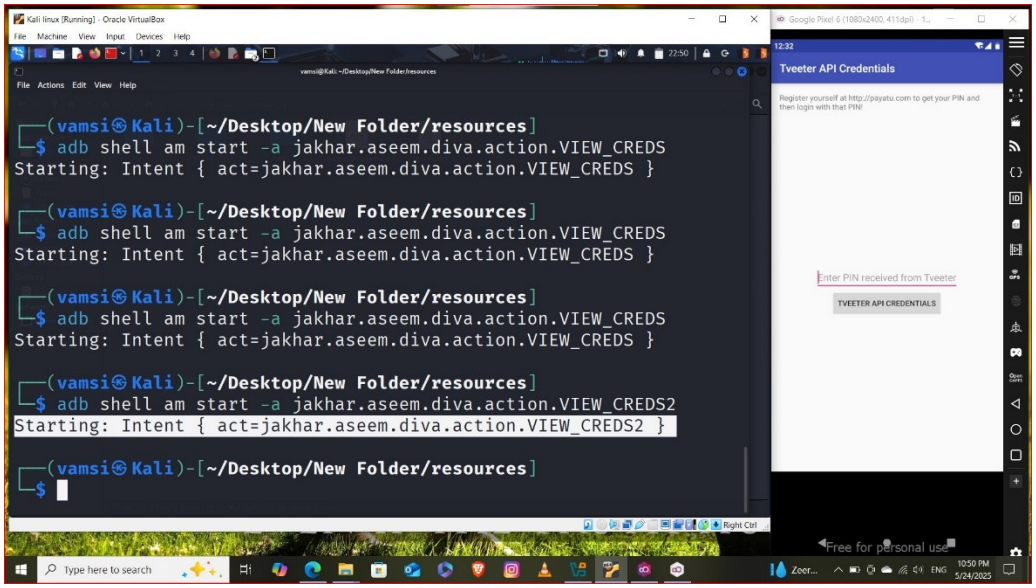
Access Control Issues-Part :1

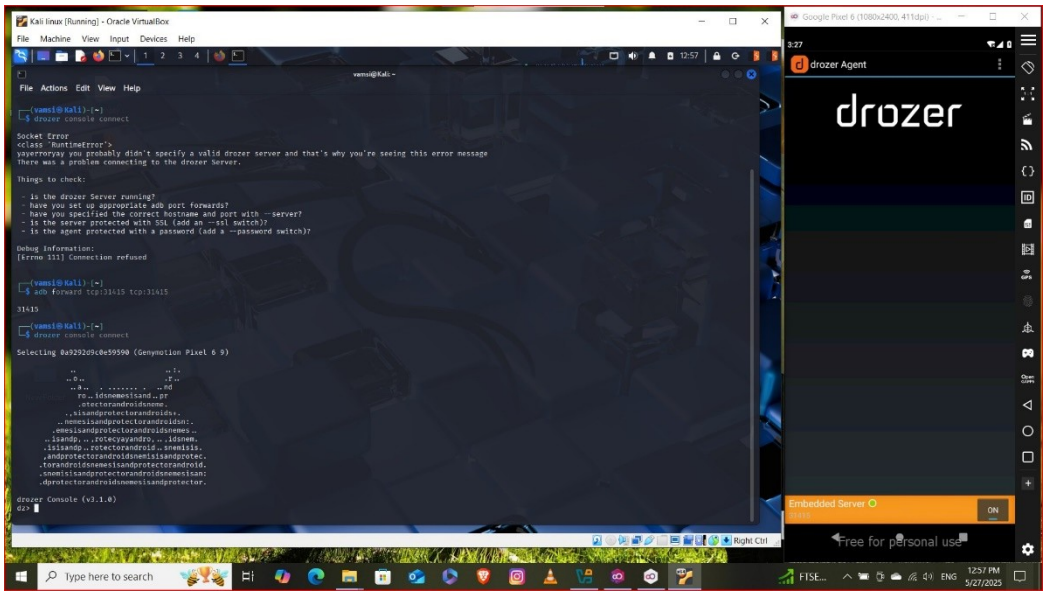


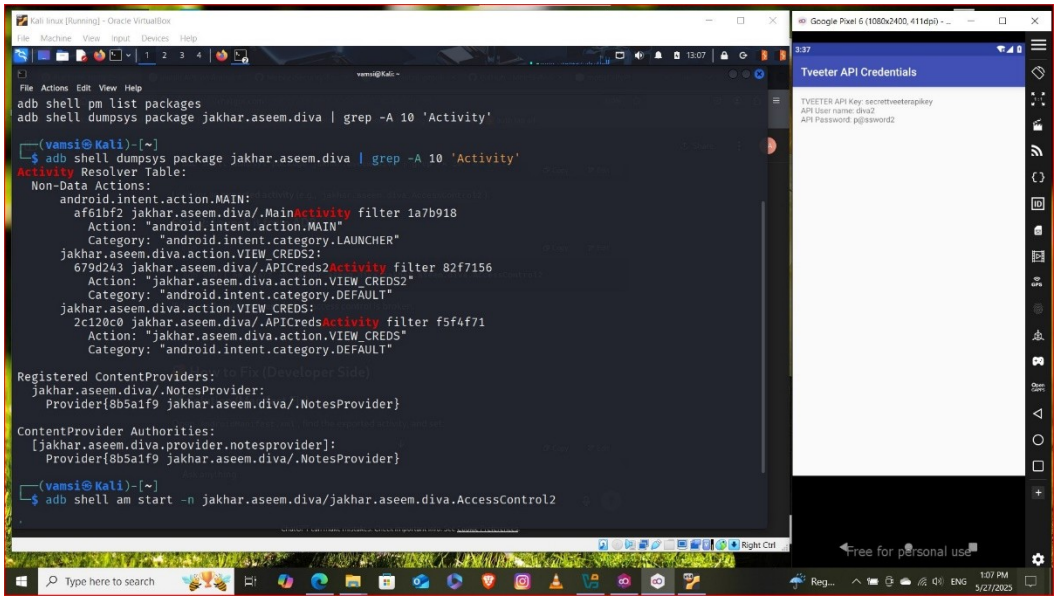

Kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vamsi@Kali: ~/Desktop/New Folder/resources
File Actions Edit View Help
android:label="@string/apic_label"
android:name="jakhar.aseem.diva.APICredsActivity">
<intent-filter>
<action android:name="jakhar.aseem.diva.action.VIEW_CREDS"/>
<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:name="jakhar.aseem.diva.NotesProvider"
android:enabled="true"
android:exported="true"
android:authorities="jakhar.aseem.diva.provider.notesprovider"/>
<activity
android:label="@string/d11"
android:name="jakhar.aseem.diva.AccessControl3Activity"/>
Google Pixel 6 (1080x2400, 411dpi) - 1...
12:24
9. Access Control Issues - Part 1
Objective: You are able to access the API credentials when you click the button. Now, try to access the API credentials from outside the app.
Hint:Components of an app can be accessed from other apps or users if they are not properly protected. Components such as activities, services, content providers are prone to this.
VIEW API CREDENTIALS
Free for personal use
Type here to search
10:42 PM
5/24/2025


Kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
vamsi@Kali: ~/Desktop/New Folder/resources
File Actions Edit View Help
<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>
</manifest>
┌──(vamsi㉿Kali)-[~/Desktop/New Folder/resources]
└─$ adb shell am start -a jakhar.aseem.diva.action.VIEW_CREDS
Starting: Intent { act=jakhar.aseem.diva.action.VIEW_CREDS }
┌──(vamsi㉿Kali)-[~/Desktop/New Folder/resources]
└─$ adb shell am start -a jakhar.aseem.diva.action.VIEW_CREDS
Starting: Intent { act=jakhar.aseem.diva.action.VIEW_CREDS }
┌──(vamsi㉿Kali)-[~/Desktop/New Folder/resources]
└─$ adb shell am start -a jakhar.aseem.diva.action.VIEW_CREDS
Starting: Intent { act=jakhar.aseem.diva.action.VIEW_CREDS }
┌──(vamsi㉿Kali)-[~/Desktop/New Folder/resources]
└─$
Google Pixel 6 (1080x2400, 411dpi) - 1...
12:25
Vendor API Credentials
API Key: 123secretapikey123
API User name: diva
API Password: p@ssword
Free for personal use
Type here to search
10:43 PM
5/24/2025

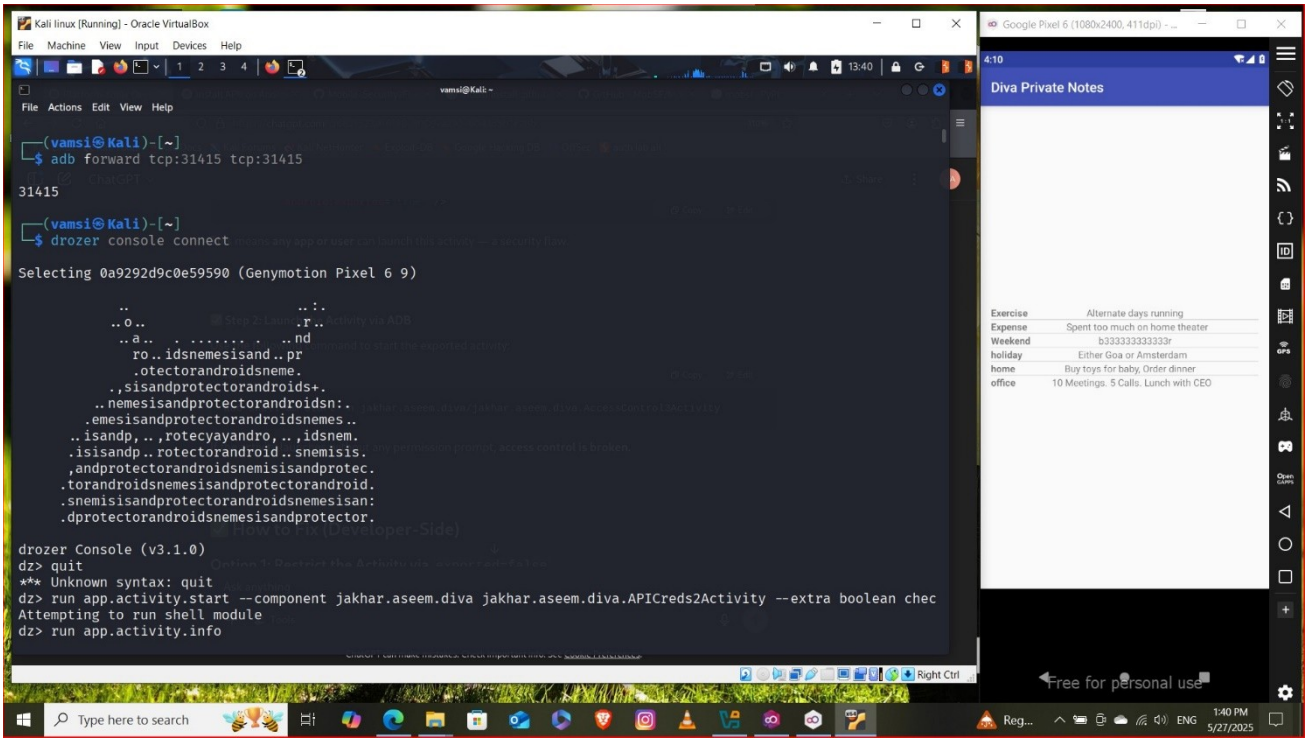
10 Acces Control Issues-Part 2

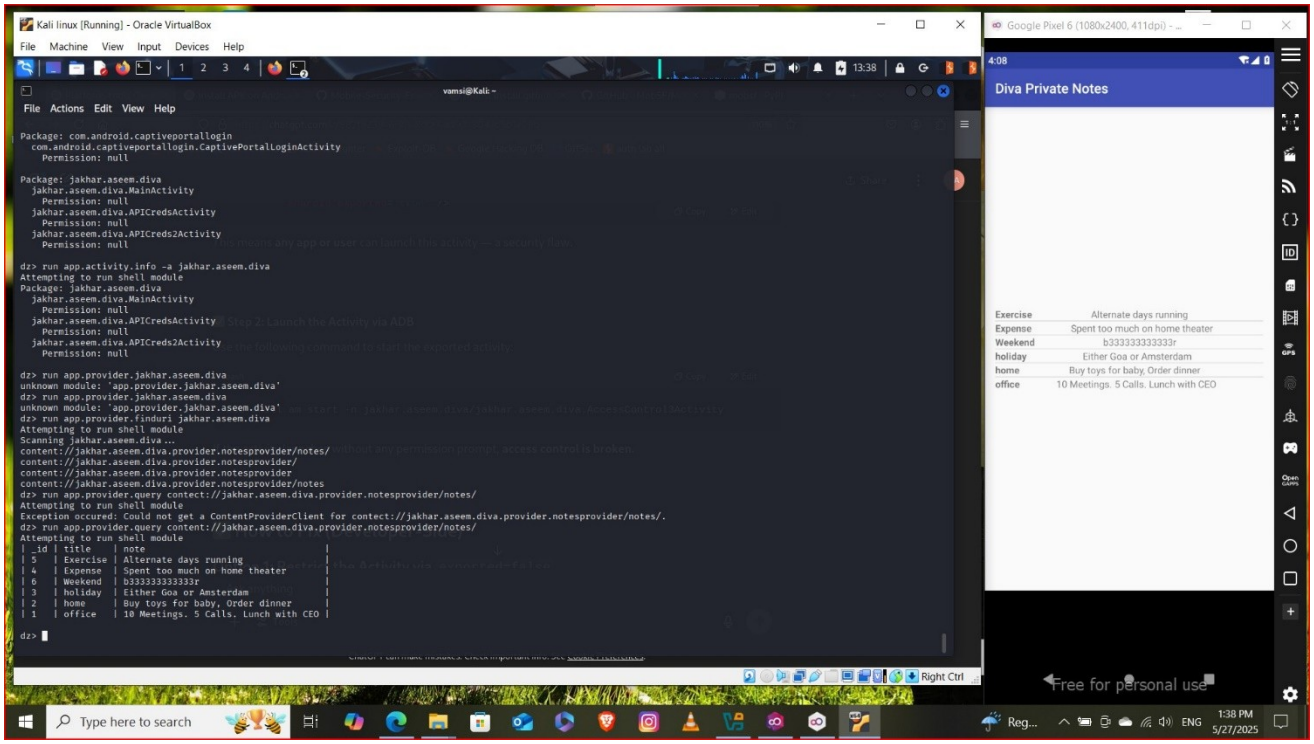


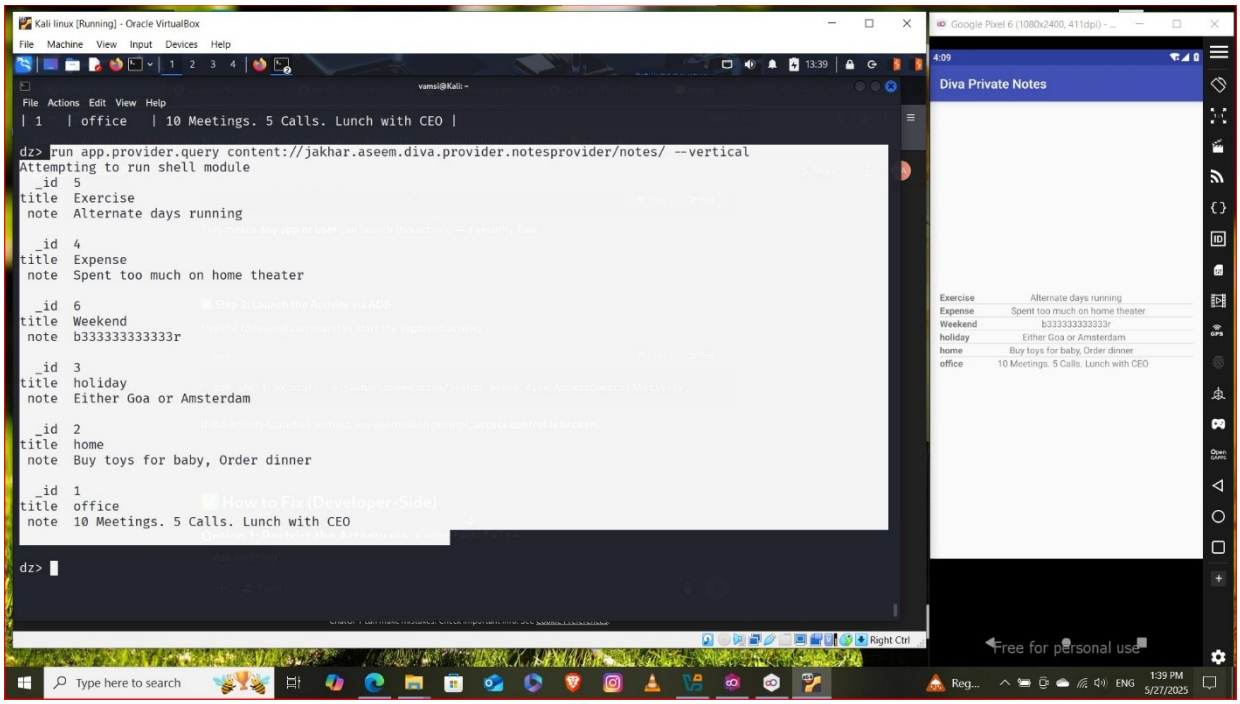




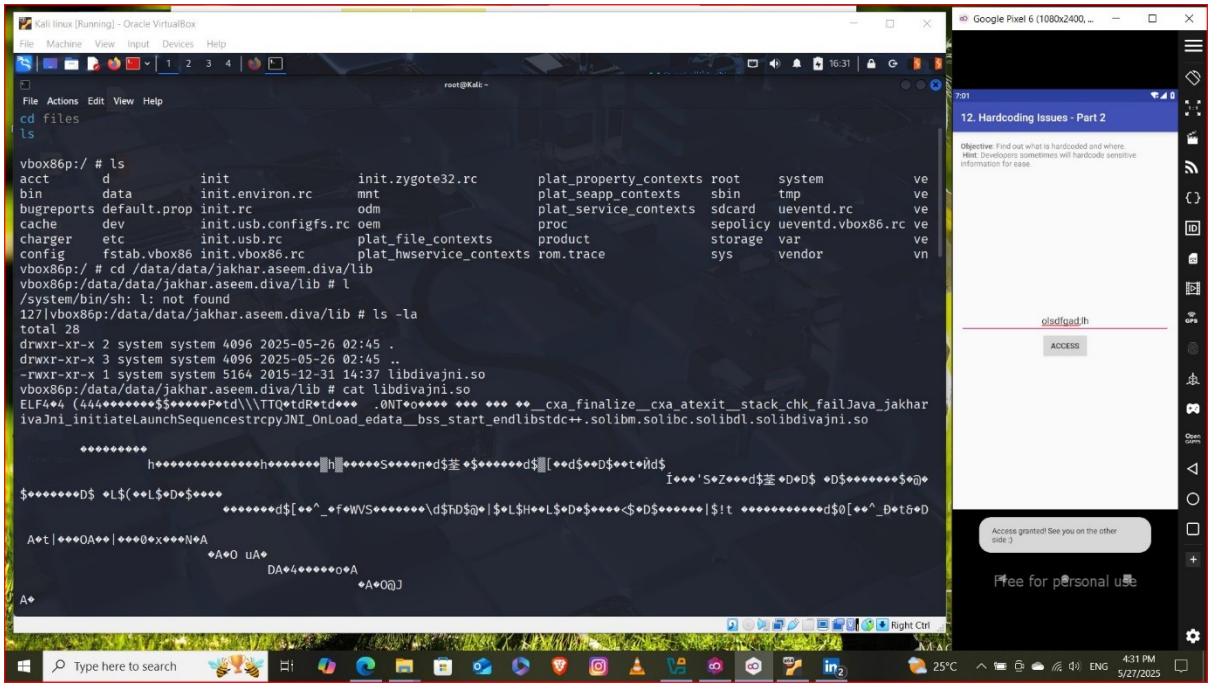
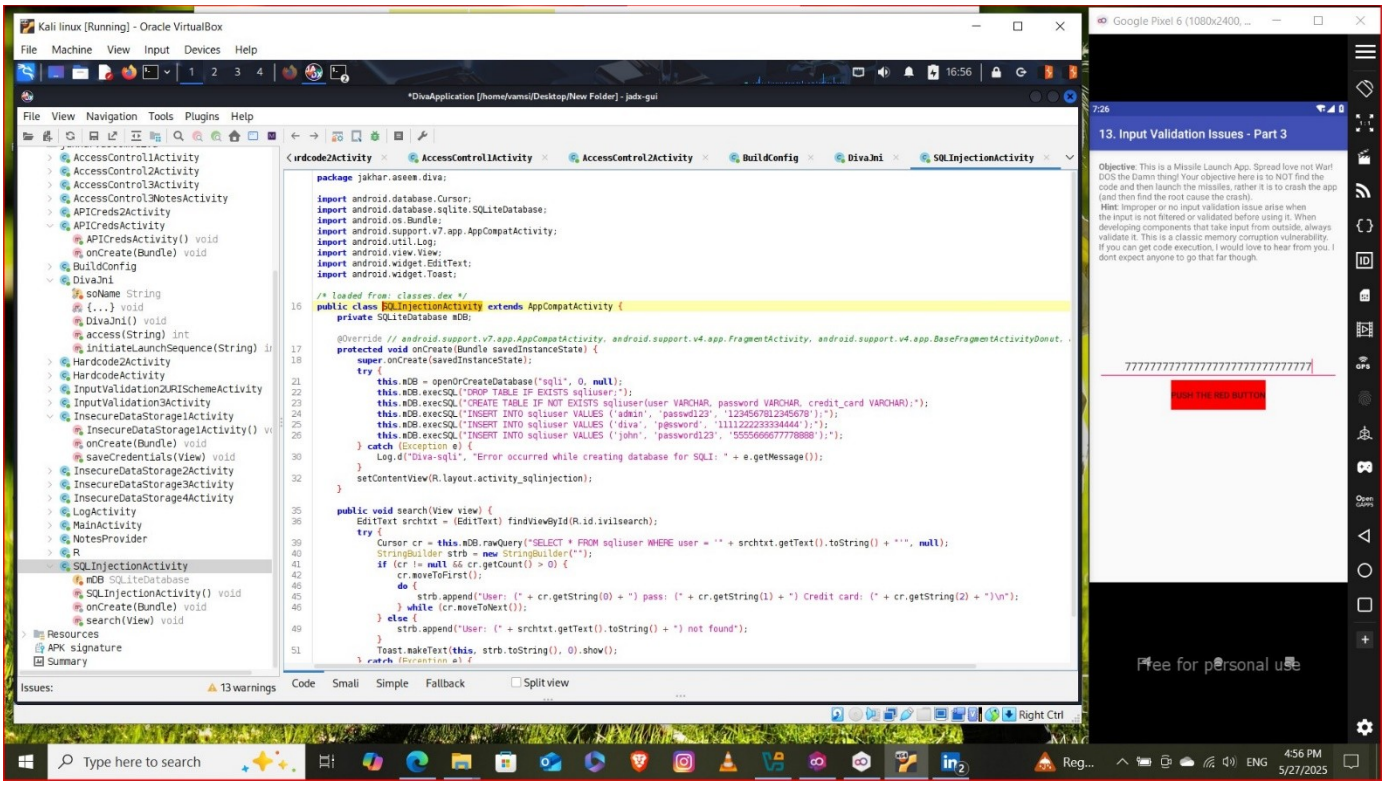
11. Access Control Issues-Part 3







12 .Hardcoding Issues-Part 2



13. Input Validation Issues-Part 3