Finding Name: Sensitive data exposure via logs

Name	Team	Role	Project	Quality Assurance	Is this a re-tested Finding?
ABDULMAJEED HUSSAIN A ALZAHRANI	PT	Senior	Gopher Guardian	Siwei Luo & Ryan Turner	

Was this Finding Successful?
Yes

Finding Description

During the penetration testing of the Guardian APK, sensitive data exposure was identified in the application logs. The issue stems from the application's logging mechanism, which records confidential information without proper sanitization or access control. This vulnerability increases the risk of unauthorized access to sensitive data and compromises user privacy

Risk Rating

Impact: Major
Likelihood: High

Impact values				
Very Minor	**Minor**	**Significant**	**Major**	**Severe**
Risk that holds little to no impact. Will not cause damage and regular activity can continue.	Risk that holds minor form of impact, but not significant enough to be of threat. Can cause some damage but not enough to impede regular activity.	Risk that holds enough impact to be somewhat of a threat. Will cause damage that can impede regular activity but will be able to run normally.	Risk that holds major impact to be of threat. Will cause damage that will impede regular activity and will not be able to run normally.	Risk that holds severe impact and is a threat. Will cause critical damage that can cease activity to be run.

Likelihood				
Rare	**Unlikely**	**Moderate**	**High**	**Certain**
Event may occur and/or if it did, it happens in specific circumstances.	Event could occur occasionally and/or could happen (at some point)	Event may occur and/or happens.	Event occurs at times and/or probably happens a lot.	Event is occurring now and/or happens frequently.

Business Impact

Addressing sensitive data exposure in logs is not just a technical necessity but a critical business requirement. Failure to mitigate this vulnerability could lead to financial penalties, legal consequences, and loss of user trust, significantly harming the business's growth and sustainability. Immediate remediation and proactive security measures are essential to minimize these risks.

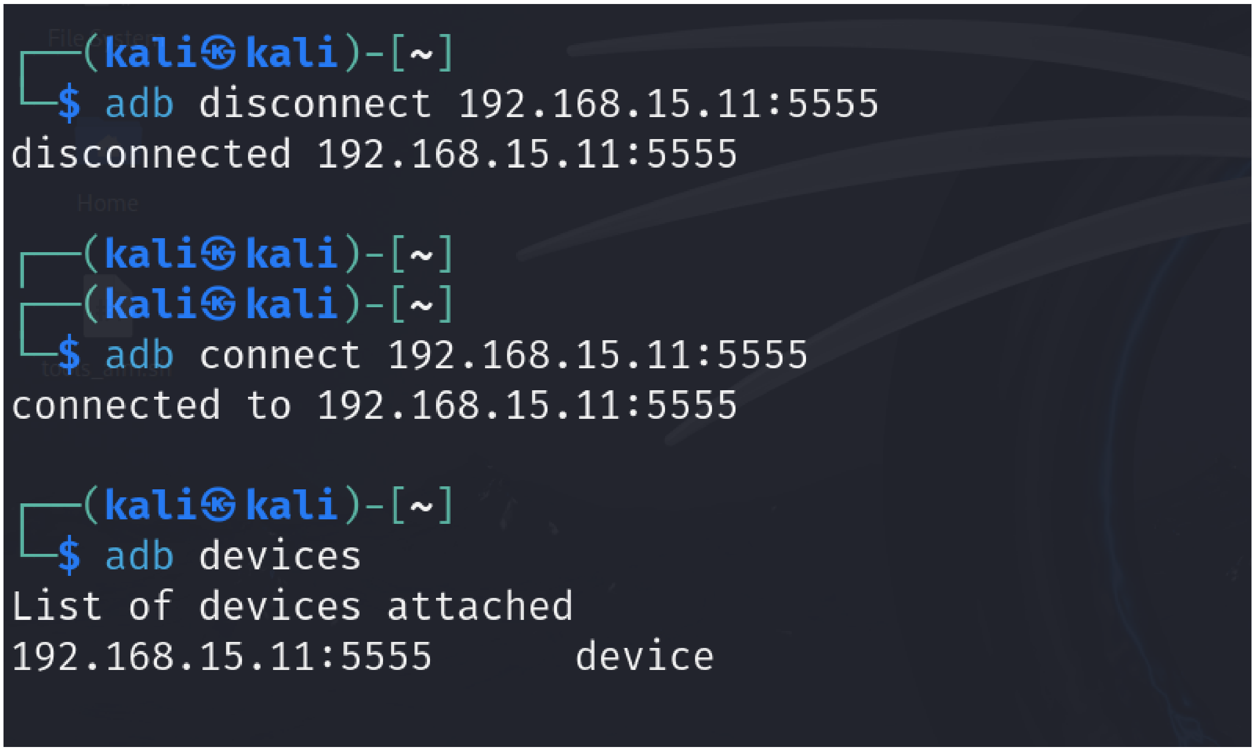
Affected Assets

Customers data like email,password or session key

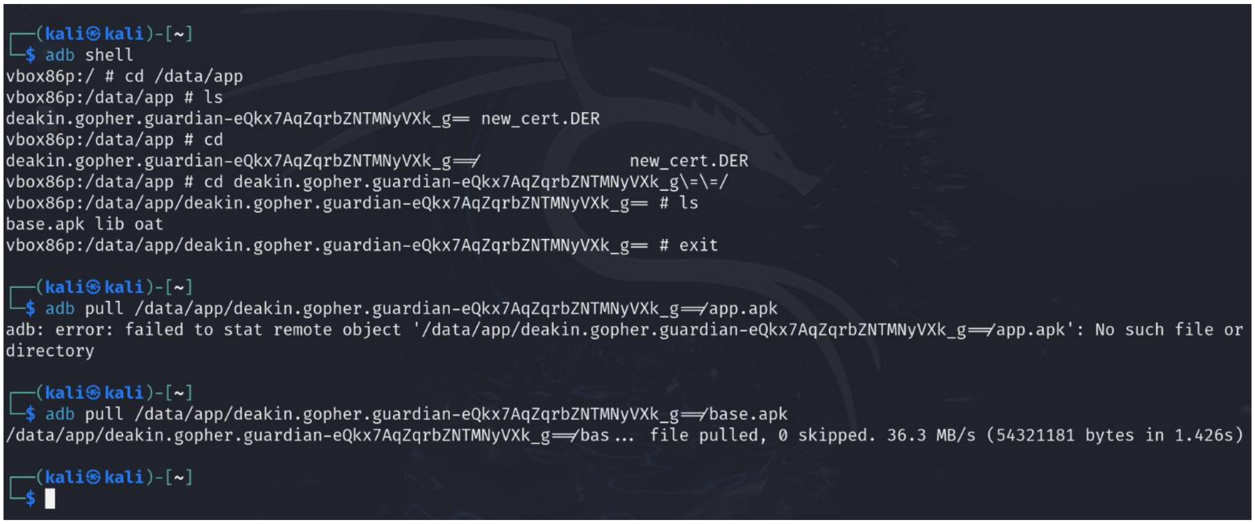
Evidence

Provide a step-by-step guide on how to reproduce the vulnerability with screenshots

Step 1. connect using adb and pull the application

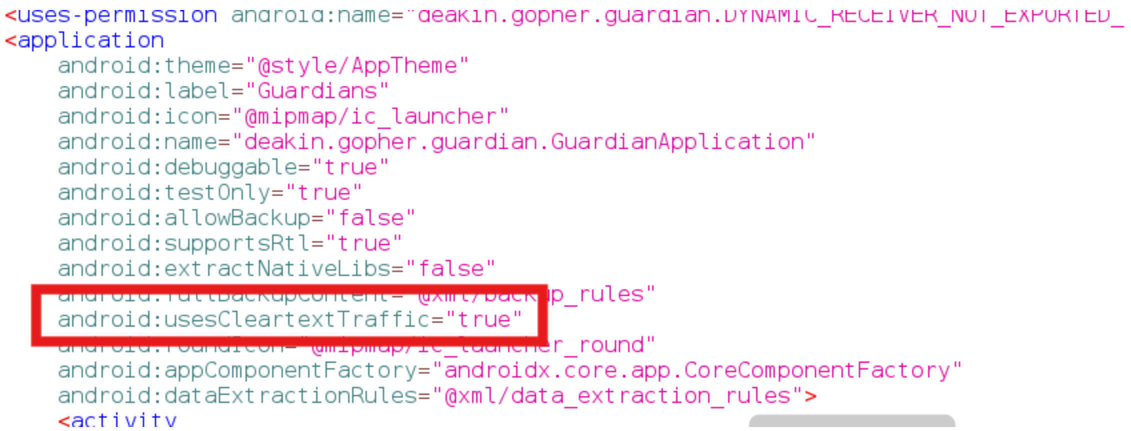


```
┌──(kali㉿kali)-[~]
└─$ adb disconnect 192.168.15.11:5555
disconnected 192.168.15.11:5555

┌──(kali㉿kali)-[~]
┌──(kali㉿kali)-[~]
└─$ adb connect 192.168.15.11:5555
connected to 192.168.15.11:5555

┌──(kali㉿kali)-[~]
└─$ adb devices
List of devices attached
192.168.15.11:5555      device
```



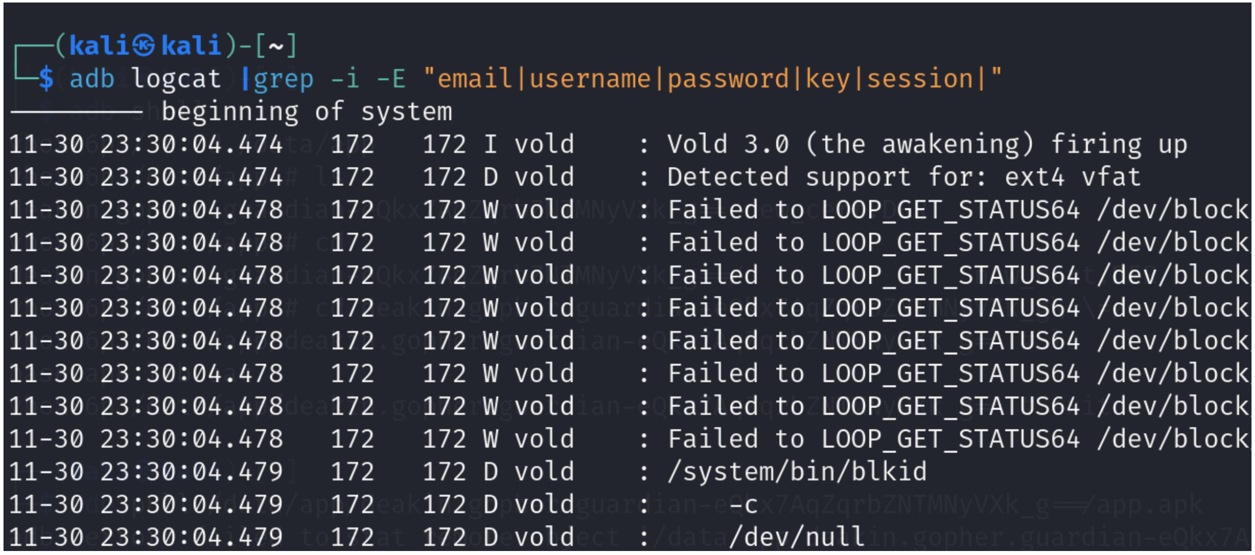
```
┌──(kali㉿kali)-[~]
└─$ adb shell
vbox86p:/ # cd /data/app
vbox86p:/data/app # ls
deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g== new_cert.DER
vbox86p:/data/app # cd
deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g==/                new_cert.DER
vbox86p:/data/app # cd deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g\=\=/
vbox86p:/data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g== # ls
base.apk lib oat
vbox86p:/data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g== # exit

┌──(kali㉿kali)-[~]
└─$ adb pull /data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g==/app.apk
adb: error: failed to stat remote object '/data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g==/app.apk': No such file or
directory

┌──(kali㉿kali)-[~]
└─$ adb pull /data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g==/base.apk
/data/app/deakin.gopher.guardian-eQkx7AqZqrbZNTMNyVXk_g==/bas... file pulled, 0 skipped. 36.3 MB/s (54321181 bytes in 1.426s)

┌──(kali㉿kali)-[~]
└─$ 
```

Step 2. decompile the application and analyze the source code using jadx .we can see usescleartraffic attribute set to true which means the app does not any obfuscate mechanism.



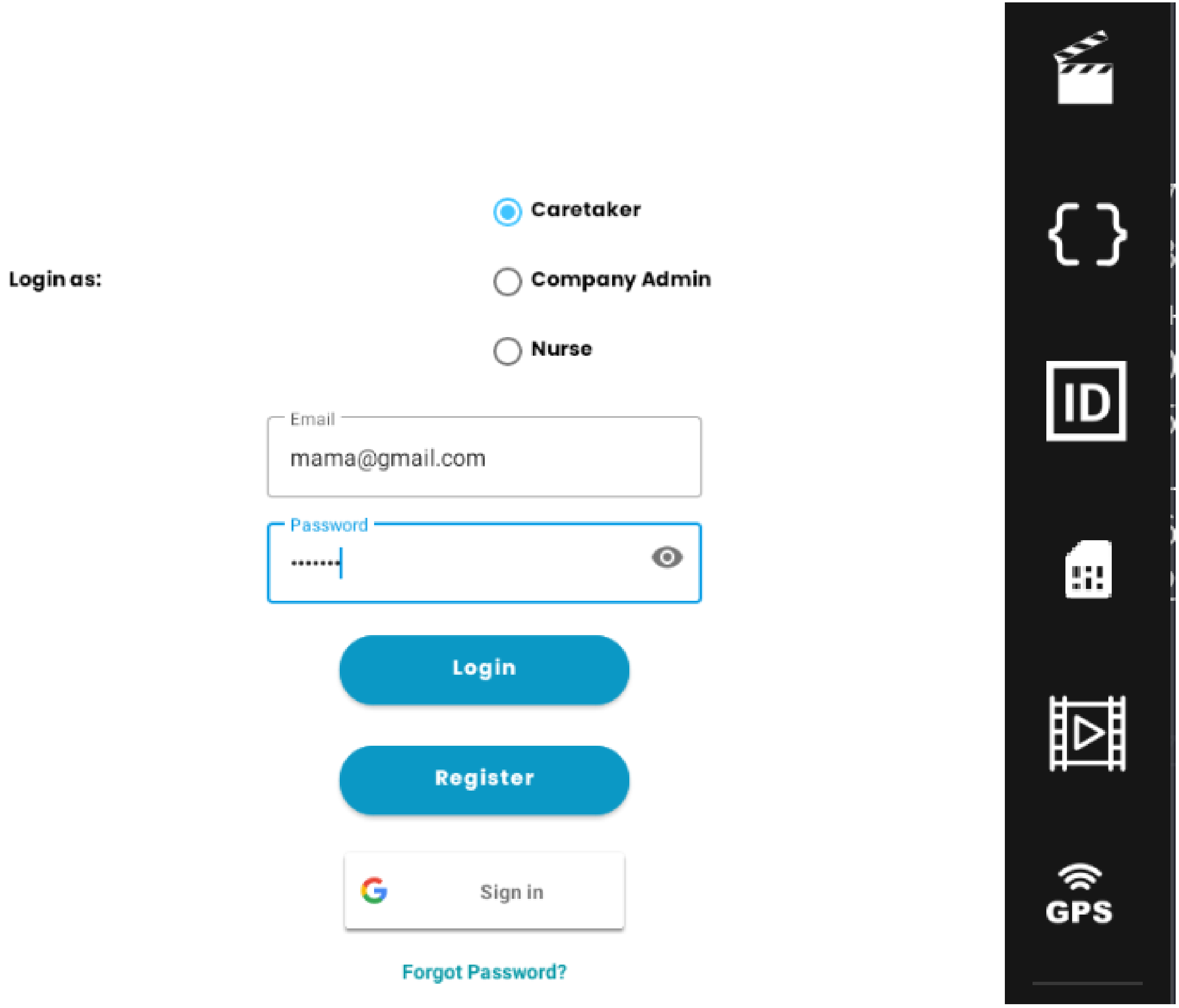
```
<uses-permission android:name="deakin.gopher.guardian.DYNAMIC_RECEIVER_NOT_EXPORTED_
<application
    android:theme="@style/AppTheme"
    android:label="Guardians"
    android:icon="@mipmap/ic_launcher"
    android:name="deakin.gopher.guardian.GuardianApplication"
    android:debuggable="true"
    android:testOnly="true"
    android:allowBackup="false"
    android:supportsRtl="true"
    android:extractNativeLibs="false"
    android:fullBackupContent="@xml/backup_rules"
    android:usesCleartextTraffic="true"
    android:roundIcon="@mipmap/ic_launcher_round"
    android:appComponentFactory="androidx.core.app.CoreComponentFactory"
    android:dataExtractionRules="@xml/data_extraction_rules">
    <activity
```

Step 3. we watch logs with logcat to reveal any sensitive information such email, passwords or application keys



```
┌──(kali㉿kali)-[~]
└─$ adb logcat |grep -i -E "email|username|password|key|session|"
──────── beginning of system
11-30 23:30:04.474   172   172 I vold    : Vold 3.0 (the awakening) firing up
11-30 23:30:04.474   172   172 D vold    : Detected support for: ext4 vfat
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.478   172   172 W vold    : Failed to LOOP_GET_STATUS64 /dev/block
11-30 23:30:04.479   172   172 D vold    : /system/bin/blkid
11-30 23:30:04.479   172   172 D vold    :     -c
11-30 23:30:04.479   172   172 D vold    :     /dev/null
```

Step 4. try to login in the application

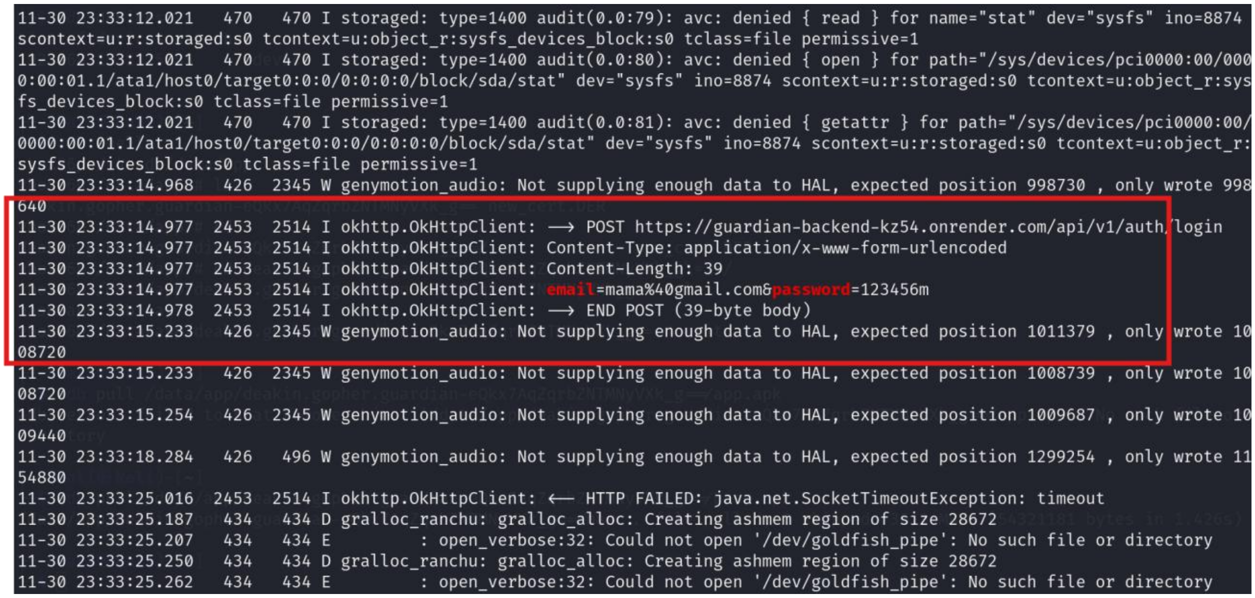


Login as: ● Caretaker ○ Company Admin ○ Nurse

Email: mama@gmail.com

Password: •••••••

Step 5. we can see the username and password that we used in clear text in the logs



```
11-30 23:33:12.021   470   470 I storaged: type=1400 audit(0.0:79): avc: denied { read } for name="stat" dev="sysfs" ino=8874
scontext=u:r:storaged:s0 tcontext=u:object_r:sysfs_devices_block:s0 tclass=file permissive=1
11-30 23:33:12.021   470   470 I storaged: type=1400 audit(0.0:80): avc: denied { open } for path="/sys/devices/pci0000:00/000
0:00:01.1/ata1/host0/target0:0:0/0:0:0:0/block/sda/stat" dev="sysfs" ino=8874 scontext=u:r:storaged:s0 tcontext=u:object_r:sys
fs_devices_block:s0 tclass=file permissive=1
11-30 23:33:12.021   470   470 I storaged: type=1400 audit(0.0:81): avc: denied { getattr } for path="/sys/devices/pci0000:00/
0000:00:01.1/ata1/host0/target0:0:0/0:0:0:0/block/sda/stat" dev="sysfs" ino=8874 scontext=u:r:storaged:s0 tcontext=u:object_r:
sysfs_devices_block:s0 tclass=file permissive=1
11-30 23:33:14.968   426  2345 W genymotion_audio: Not supplying enough data to HAL, expected position 998730 , only wrote 998
640
11-30 23:33:14.977  2453  2514 I okhttp.OkHttpClient: ⟶ POST https://guardian-backend-kz54.onrender.com/api/v1/auth/login
11-30 23:33:14.977  2453  2514 I okhttp.OkHttpClient: Content-Type: application/x-www-form-urlencoded
11-30 23:33:14.977  2453  2514 I okhttp.OkHttpClient: Content-Length: 39
11-30 23:33:14.977  2453  2514 I okhttp.OkHttpClient: email=mama%40gmail.com&password=123456m
11-30 23:33:14.978  2453  2514 I okhttp.OkHttpClient: ⟶ END POST (39-byte body)
11-30 23:33:15.233   426  2345 W genymotion_audio: Not supplying enough data to HAL, expected position 1011379 , only wrote 10
08720
11-30 23:33:15.233   426  2345 W genymotion_audio: Not supplying enough data to HAL, expected position 1008739 , only wrote 10
08720
11-30 23:33:15.254   426  2345 W genymotion_audio: Not supplying enough data to HAL, expected position 1009687 , only wrote 10
09440
11-30 23:33:18.284   426   496 W genymotion_audio: Not supplying enough data to HAL, expected position 1299254 , only wrote 11
54880
11-30 23:33:25.016  2453  2514 I okhttp.OkHttpClient: ⟵ HTTP FAILED: java.net.SocketTimeoutException: timeout
11-30 23:33:25.187   434   434 D gralloc_ranchu: gralloc_alloc: Creating ashmem region of size 28672
11-30 23:33:25.207   434   434 E         : open_verbose:32: Could not open '/dev/goldfish_pipe': No such file or directory
11-30 23:33:25.250   434   434 D gralloc_ranchu: gralloc_alloc: Creating ashmem region of size 28672
11-30 23:33:25.262   434   434 E         : open_verbose:32: Could not open '/dev/goldfish_pipe': No such file or directory
```

Remediation Advice

- Avoid logging sensitive data like passwords or PII.
- Mask sensitive fields in logs when necessary.
- Restrict access to log files with strict permissions.
- Disable debug-level logging in production environments.
- Encrypt log files and secure data in transit.

References

ADB
jadx
Logact

Abdulmajeed Hussain A AlZahrani

s223844731@deakin.edu.au