Assignment Report

---

# Analysis of Malicious Android App APK

APK File Name:  
> b57cab62c3f5089581e452d8d8b33932c426341878d22b13501ec9e78f925a80.apk

Application Name:  
> My Horror Fello

Package Name:  
> nono.myhorrorfello

Version Information:

- Version Code: 1

- Version Name: 1.1

- Minimal Supported Android Version: Jelly Bean (API 17)

- Target SDK: Pie (API 28)

Tools Used:

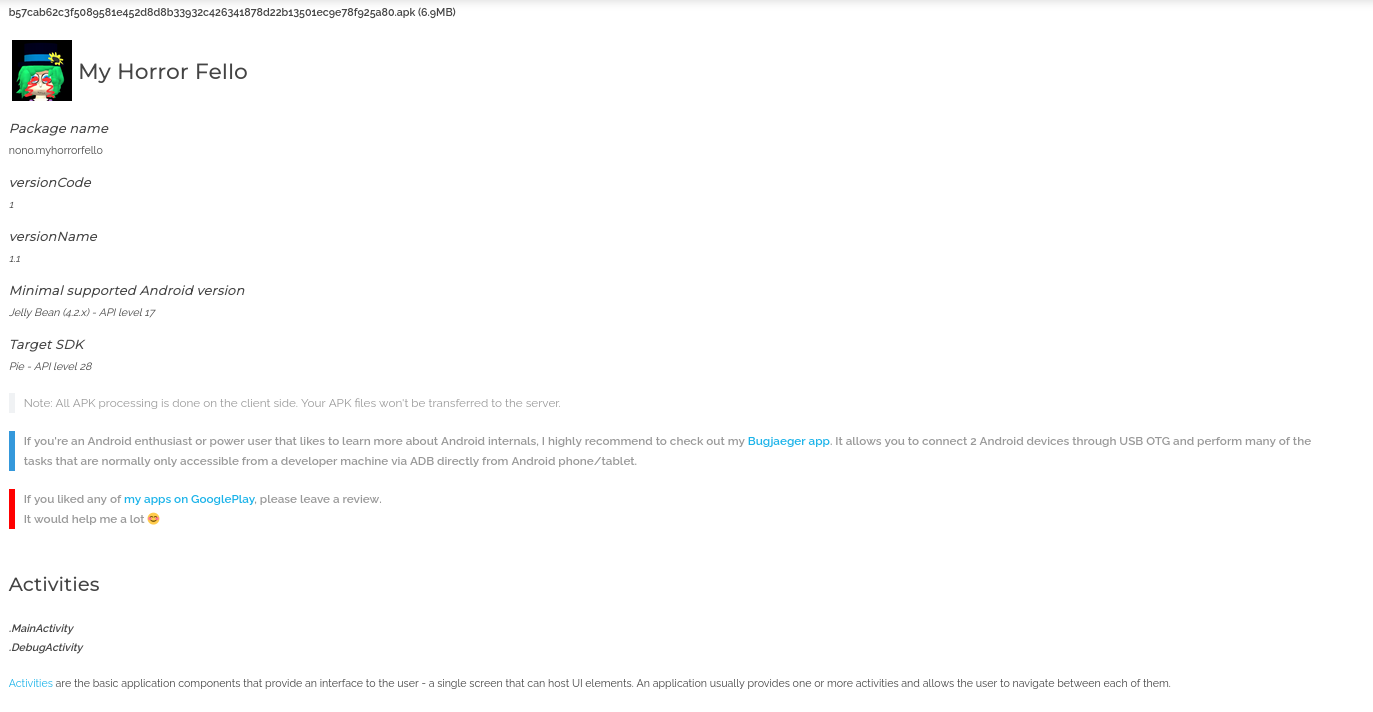
- APKTool

- JavaDecompiler

- MobSF

---

# 1. APKTool Analysis



Permissions Detected:

- android.permission.READ\_EXTERNAL\_STORAGE

- android.permission.WRITE\_EXTERNAL\_STORAGE

- android.permission.SET\_WALLPAPER

- android.permission.AMBIENT\_WALLPAPER

- android.permission.BIND\_WALLPAPER

- android.permission.READ\_WALLPAPER\_INTERNAL

- android.permission.SET\_WALLPAPER\_HINTS

- android.permission.SET\_WALLPAPER\_COMPONENT

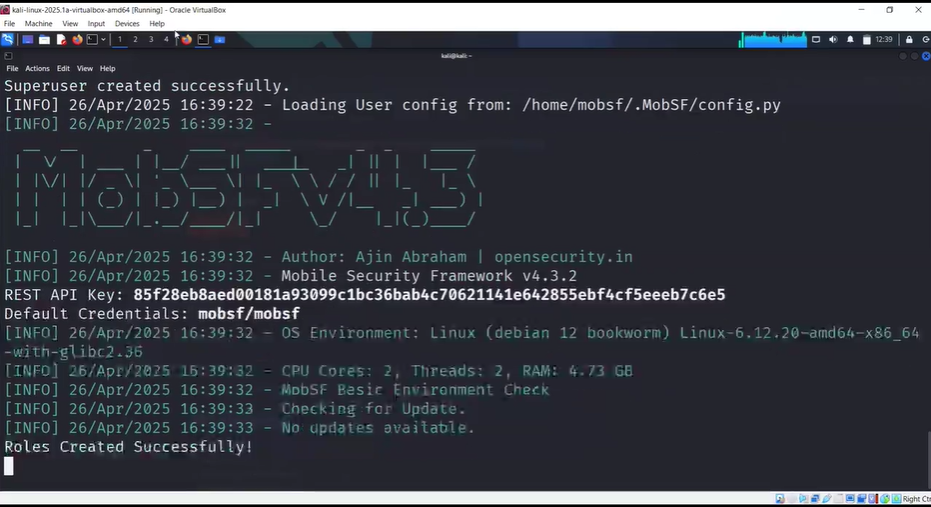
Activities Detected:  
- MainActivity  
- DebugActivity

Observations:  
- Excessive wallpaper-related permissions.  
- Allows cleartext traffic (insecure).  
- Has DebugActivity (not safe for production).  
- Access to external storage may lead to data leaks.

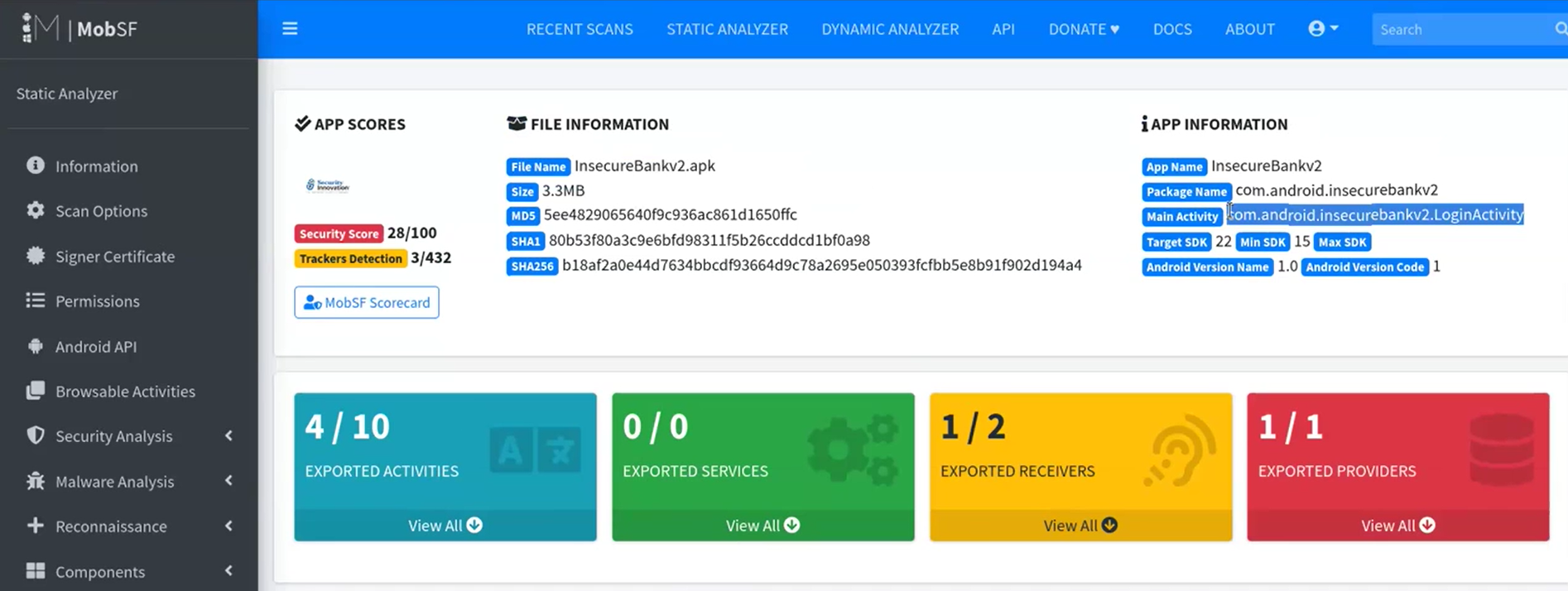
---

# 2. MobSF Analysis

MobSF Terminal Startup:



MobSF Web Report:



MobSF Summary:  
- Deprecated and risky permissions detected.  
- Score: Security 28/100.  
- Trackers found: 3/432.  
- No secure network communication (no certificate pinning).  
- Uses legacy external storage.  
- Moderate risk level.

---

# 3. JavaDecompiler Summary

- Structure shows AndroidManifest.xml, META-INF, classes.dex.  
- classes.dex needs further decompilation with JADX for code inspection.  
- Manifest confirms risky permissions and debug activity.

---

# 4. Conclusion

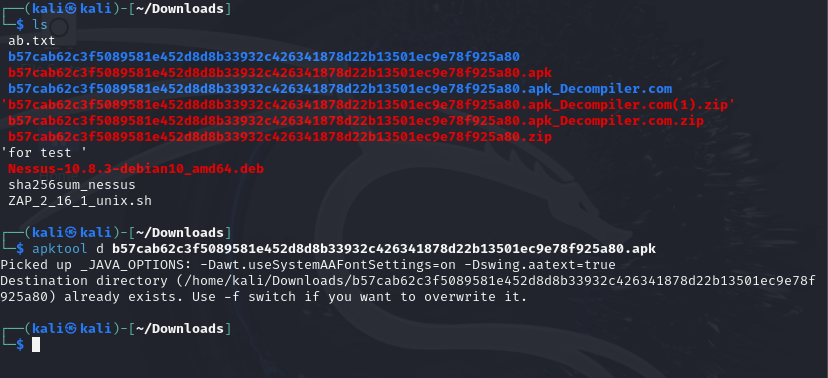
The APK appears malicious or at least suspicious due to:  
- Unsafe permission usage  
- Cleartext traffic  
- DebugActivity exposed  
- Possible unauthorized access to user storage and interface manipulation

Risk Level: Moderate to High

Recommendation:  
- Analyze classes.dex with JADX  
- Run app in sandbox for dynamic monitoring  
- Inspect traffic with Wireshark

# 5. APKTool on Kali Linux

Below is a terminal screenshot showing APKTool being used on Kali Linux to decompile the malicious APK file.



This verifies the file was properly processed using command-line tools, confirming manual APK analysis was performed.