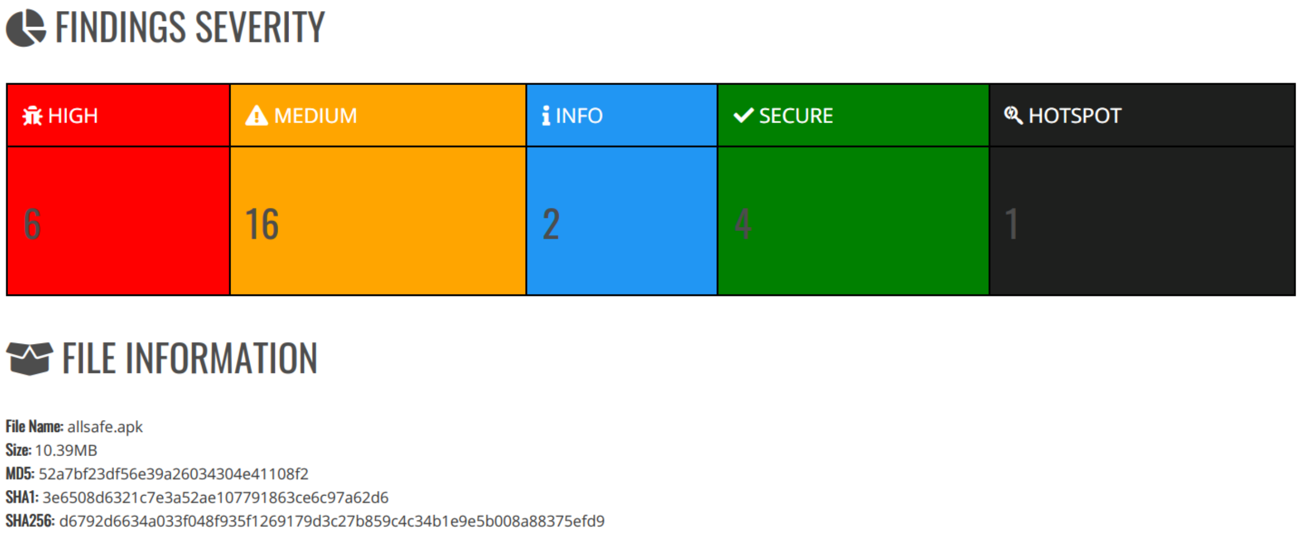
MOBILE APPLICATION PENETRATION TESTING REPORT

AllSafe Android Application
Version 1.5

Prepared by: Ankit Vishwakarma
Date: 07 December 2025

1. Executive Summary

A comprehensive security assessment was conducted on the AllSafe Android application using Mobile Security Framework (MobSF). Several high-risk, medium-risk and informational vulnerabilities were identified that may compromise confidentiality, integrity, and overall application security.



FINDINGS SEVERITY

HIGH	MEDIUM	INFO	✓ SECURE	HOTSPOT
6	16	2	4	1

FILE INFORMATION

File Name: allsafe.apk
Size: 10.39MB
MD5: 52a7bf23df56e39a26034304e41108f2
SHA1: 3e6508d6321c7e3a52ae107791863ce6c97a62d6
SHA256: d6792d6634a033f048f935f1269179d3c27b859c4c34b1e9e5b008a88375efd9

2. Scope of Assessment

APK Name	allsafe.apk
Package	infosecadventures.allsafe
Version	1.5
Platform	Android
Assessment Type	Static Analysis (MobSF)
Tools Used	MobSF

3. Methodology

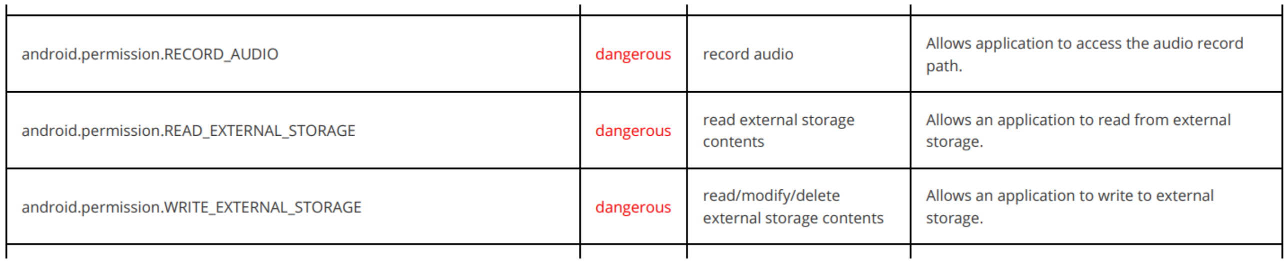
Assessment was based on:
- OWASP MASTG (Mobile Application Security Testing Guide)
- OWASP Mobile Top 10
- CWE Weakness Enumeration
- NIAP Mobile Protection Standards

Steps included APK extraction, manifest analysis, permission and component review, cryptographic evaluation, Firebase database review, and binary protection assessment.

4. Detailed Findings

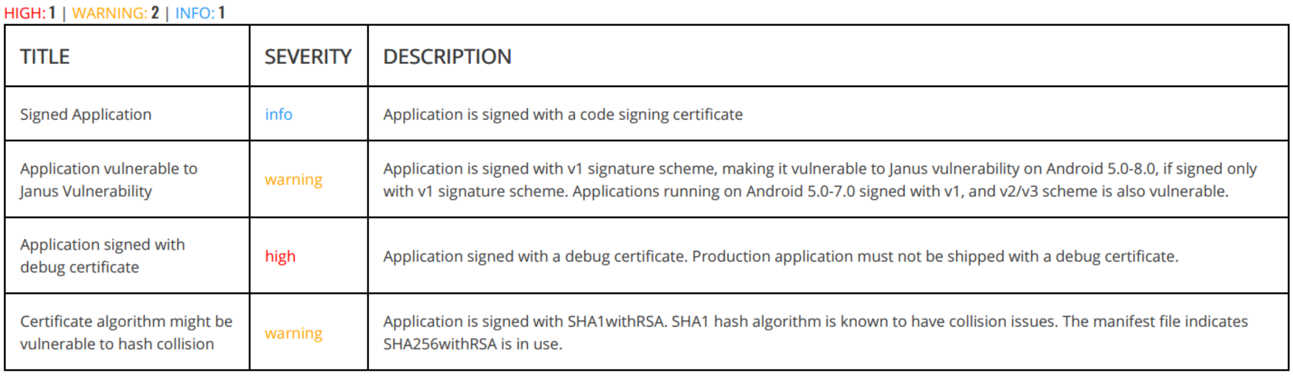
4.1 High-Risk Findings

- **Dangerous Permissions Identified**



android.permission.RECORD_AUDIO	dangerous	record audio	Allows application to access the audio record path.
android.permission.READ_EXTERNAL_STORAGE	dangerous	read external storage contents	Allows an application to read from external storage.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.

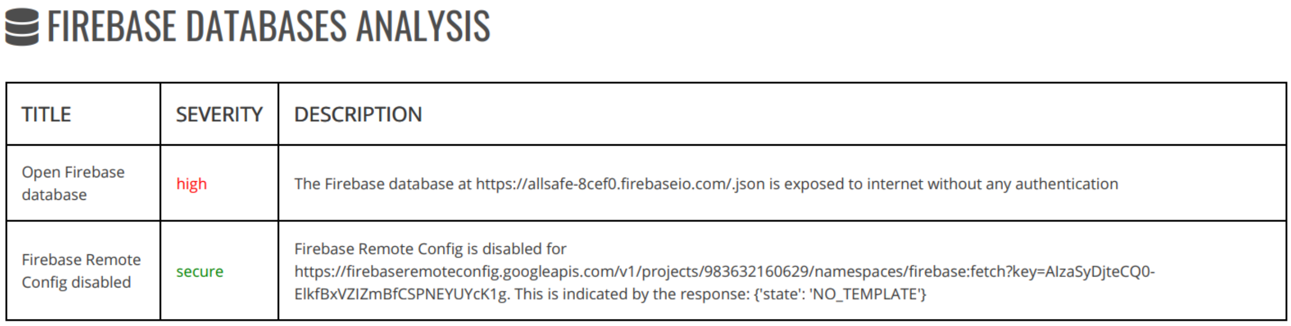
- **Application signed with Debug Certificate**



HIGH: 1 | WARNING: 2 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	warning	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Application signed with debug certificate	high	Application signed with a debug certificate. Production application must not be shipped with a debug certificate.
Certificate algorithm might be vulnerable to hash collision	warning	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues. The manifest file indicates SHA256withRSA is in use.

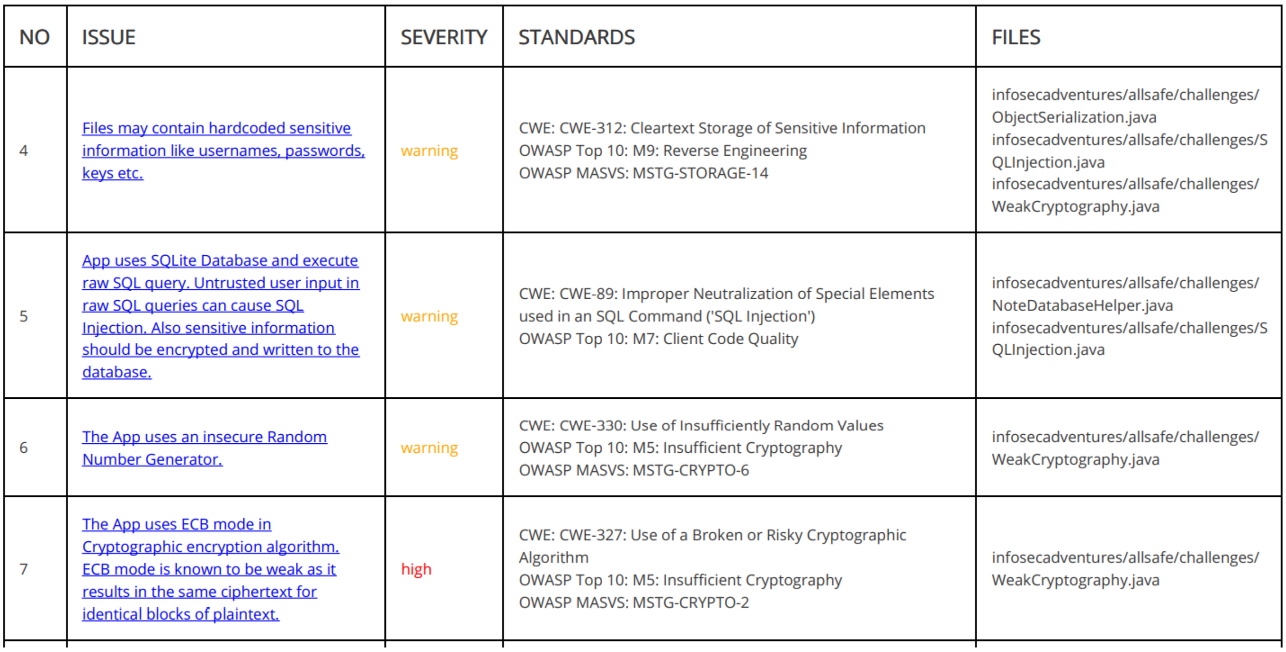
- **Public Firebase database accessible without authentication**



FIREBASE DATABASES ANALYSIS

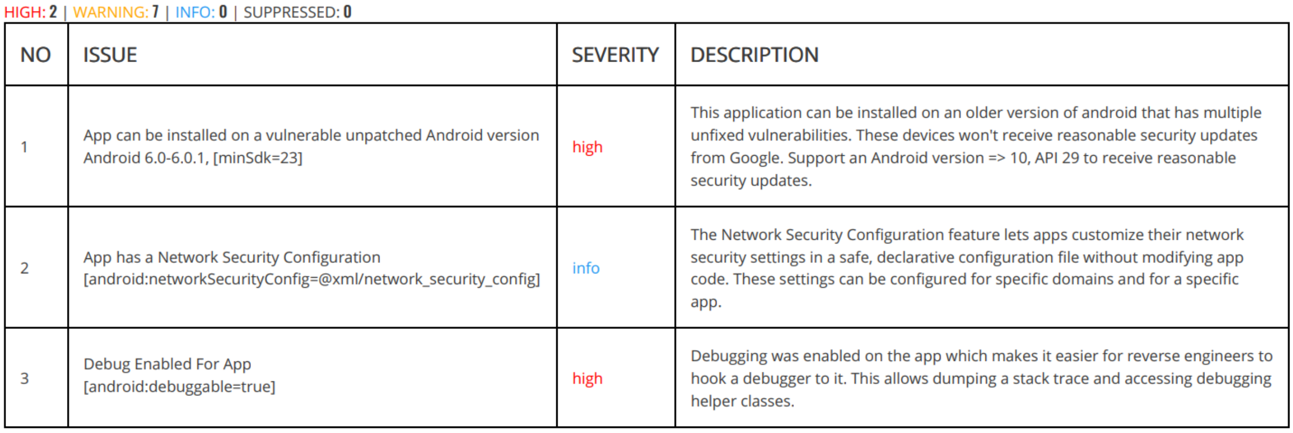
TITLE	SEVERITY	DESCRIPTION
Open Firebase database	high	The Firebase database at https://allsafe-8cef0.firebaseio.com/.json is exposed to internet without any authentication
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/983632160629/namespaces/firebase:fetch?key=AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g. This is indicated by the response: {'state': 'NO_TEMPLATE'}

- **Insecure Cryptography (ECB mode, MD5 hashing, Weak RNG)**



NO	ISSUE	SEVERITY	STANDARDS	FILES
4	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	infosecadventures/allsafe/challenges/ObjectSerialization.java infosecadventures/allsafe/challenges/SQLInjection.java infosecadventures/allsafe/challenges/WeakCryptography.java
5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	infosecadventures/allsafe/challenges/NoteDatabaseHelper.java infosecadventures/allsafe/challenges/SQLInjection.java
6	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	infosecadventures/allsafe/challenges/WeakCryptography.java
7	The App uses ECB mode in Cryptographic encryption algorithm. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.	high	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-2	infosecadventures/allsafe/challenges/WeakCryptography.java

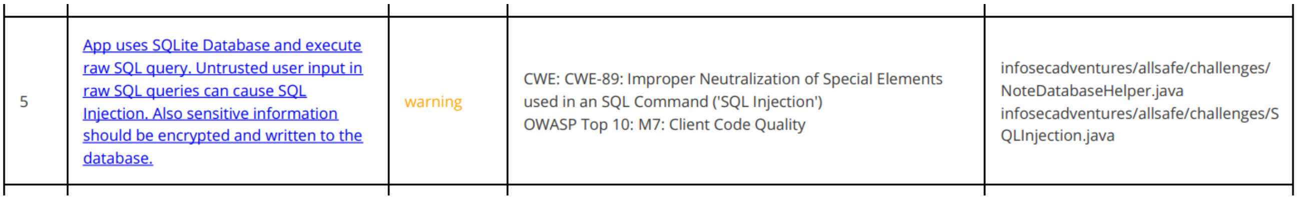
- **Exported components (Activities/Services/Receivers/Providers)**



HIGH: 2 | WARNING: 7 | INFO: 0 | SUPPRESSED: 0

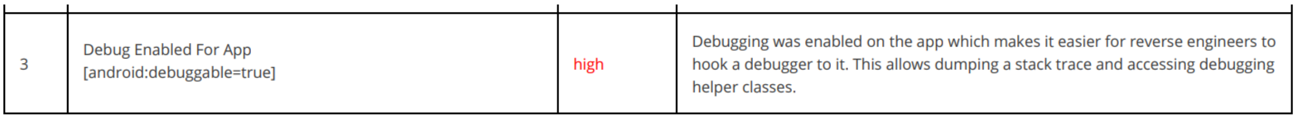
NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 6.0-6.0.1, [minSdk=23]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

- **Vulnerable SQLite operations (SQL Injection risk)**



5	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	infosecadventures/allsafe/challenges/NoteDatabaseHelper.java infosecadventures/allsafe/challenges/SQLInjection.java

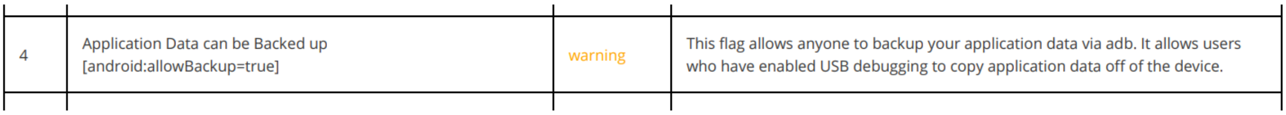
- **Debuggable flag enabled, allowing reverse engineering**



3	Debug Enabled For App [android:debuggable=true]	high	Debugging was enabled on the app which makes it easier for reverse engineers to hook a debugger to it. This allows dumping a stack trace and accessing debugging helper classes.

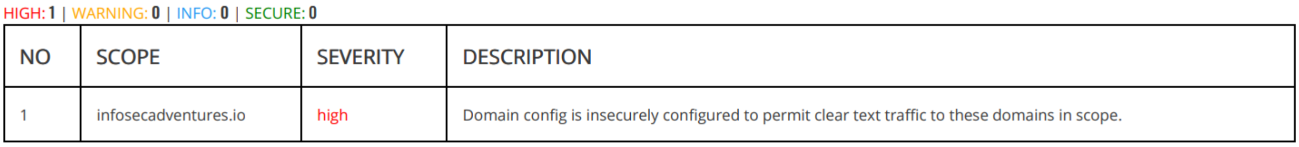
4.2 Medium-Risk Findings

- **allowBackup enabled**



4	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.

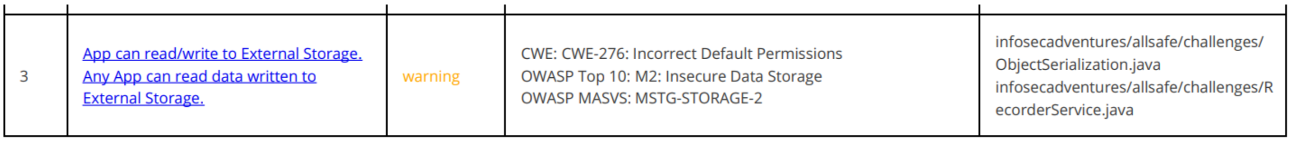
- **Clear-text network traffic allowed**



HIGH: 1 | WARNING: 0 | INFO: 0 | SECURE: 0

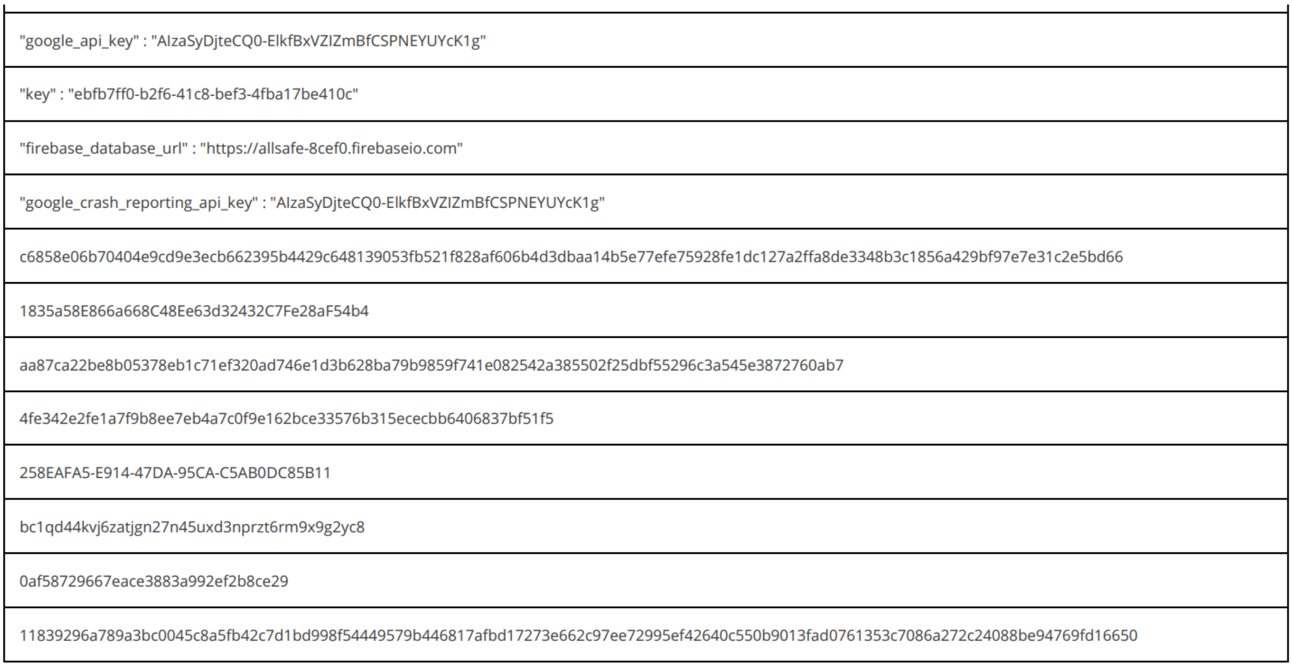
NO	SCOPE	SEVERITY	DESCRIPTION
1	infosecadventures.io	high	Domain config is insecurely configured to permit clear text traffic to these domains in scope.

- **Sensitive data stored in external storage**



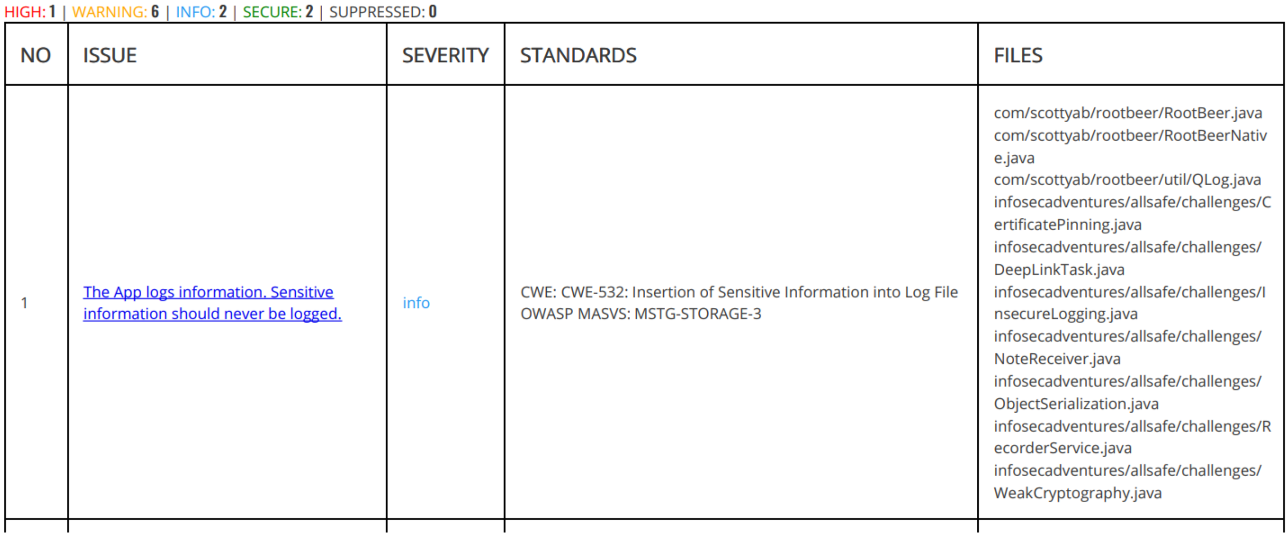
3	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	infosecadventures/allsafe/challenges/ObjectSerialization.java infosecadventures/allsafe/challenges/RecorderService.java

- **Hardcoded API keys and secrets detected**



"google_api_key" : "AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g"
"key" : "ebfb7ff0-b2f6-41c8-bef3-4fba17be410c"
"firebase_database_url" : "https://allsafe-8cef0.firebaseio.com"
"google_crash_reporting_api_key" : "AIzaSyDjteCQ0-ElkfBxVZIZmBfCSPNEYUYcK1g"
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
1835a58E866a668C48Ee63d32432C7Fe28aF54b4
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
bc1qd44kvj6zatjgn27n45uxd3nprzt6rm9x9g2yc8
0af58729667eace3883a992ef2b8ce29
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650

- **Sensitive logging present**

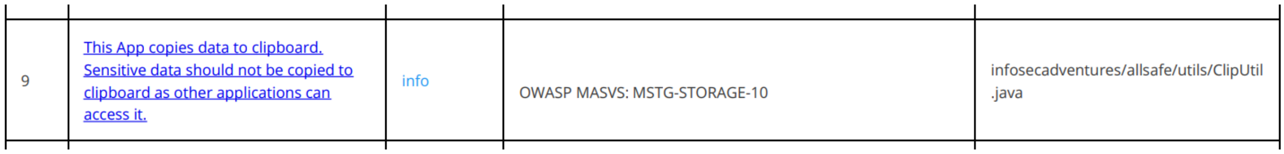


HIGH: 1 | WARNING: 6 | INFO: 2 | SECURE: 2 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	com/scottyab/rootbeer/RootBeer.java com/scottyab/rootbeer/RootBeerNative.java com/scottyab/rootbeer/util/QLog.java infosecadventures/allsafe/challenges/CertificatePinning.java infosecadventures/allsafe/challenges/DeepLinkTask.java infosecadventures/allsafe/challenges/InsecureLogging.java infosecadventures/allsafe/challenges/NoteReceiver.java infosecadventures/allsafe/challenges/ObjectSerialization.java infosecadventures/allsafe/challenges/RecorderService.java infosecadventures/allsafe/challenges/WeakCryptography.java

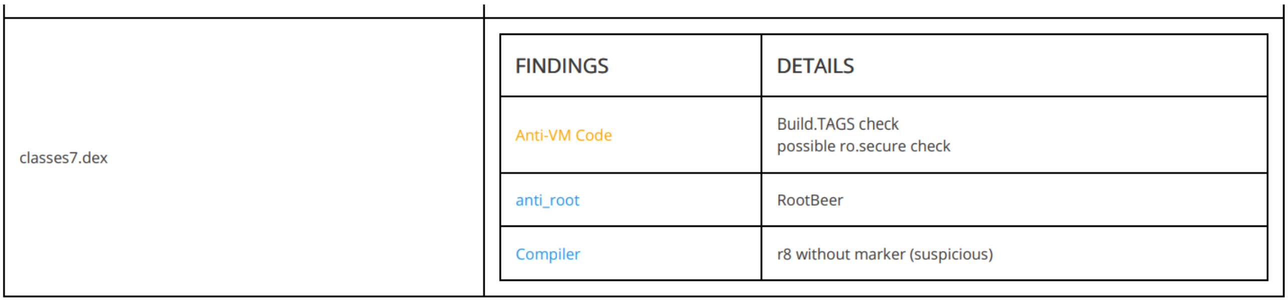
4.3 Informational Observations

- **Clipboard usage may expose sensitive data**



9	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	infosecadventures/allsafe/utils/ClipUtil.java

- **Anti-VM and Anti-Debug techniques implemented**



	FINDINGS	DETAILS
classes7.dex	Anti-VM Code	Build.TAGS check possible ro.secure check
	anti_root	RootBeer
	Compiler	r8 without marker (suspicious)

5. Recommendations

- Disable debugging and remove debuggable flags in production builds.
- Use AES-GCM or AES-CBC instead of ECB block mode.
- Replace MD5 hashing with SHA-256 or SHA-3.
- Store API keys securely using Android Keystore.
- Use parameterized SQL queries to prevent SQL Injection.
- Restrict exported components using appropriate permissions.

6. Conclusion

The AllSafe Android application exhibits several high-risk vulnerabilities that must be addressed before release. Firebase misconfiguration, insecure cryptography, exported components, and SQL injection risks pose severe security threats. Implementing the recommended remediations will significantly strengthen the application's security posture.