Tools and Apk

Keepassdroid

Androbugs - Lavkush Mani Tripati

Appsweep - Chandra Sekhar Kondeti

Mobsf - Ashutosh

PithusBazar -Bharat Kumar Koduru

Androwarn - Akash Shriwas

Issues or warnings	Androbugs	Appsweep	Mobsf	PithusBazar	Androwarn	Desc
1. Insecure Cryptography	✗	✓	✗	✓	✗	Uses an insecure PRNG
2. Insecure Cryptography-	✗	✓	✓	✓	✗	Uses ECB Mode in cryptography. ECB mode is known to be weak as it results in the same ciphertext for identical blocks of plaintext.
3. Android SQLite Data Base Vulnerability -	✓	✗	✓	✓	✗	Untrusted user input in raw SQL queries can cause SQL Injection.

4. Janus Vulnerability-	✘	✓	✓	✘	✘	The V1 app signature scheme is susceptible to the Janus vulnerability, which allows injecting code without signature modification
5. Vulnerable to hash collision-.	✘	✘	✓	✓	✘	SHA-1 is a weak hash known to have hash collisions
6. Insecure Data Storage-	✓	✘	✘	✓	✘	Allows an application to write to external storage.
7. Insecure PBCK5/PBCK7-	✘	✘	✓	✓	✘	This configuration is vulnerable to padding Oracle attacks
8. Incorrect Default Permissions-	✘	✘	✓	✓	✘	The app creates temp file. Sensitive information should never be written into a temp file.

9. Reverse Engineering -	✘	✓	✘	✓	✘	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.
10. Native library loading	✓	✘	✘	✘	✓	. Native library loading code Found
11. Logs Information -	✓	✓	✓	✓	✓	Sensitive information should never be logged.
12. Input Field does not mask- .	✘	✓	✘	✘	✘	Vulnerable to shoulder-surfing attacks. Several password input fields in the app are not using this masking
13. Tapjacking-	✘	✓	✘	✘	✘	Tapjacking is a technique that allows an attacker to capture the taps in your app (for example, on a

						virtual pin-pad)
14. Clear text communication-	✗	✓	✘	✗	✗	Disabling this should not allow the attacker to spy on the network
15. Keyboard suggestions -	✗	✓	✘	✗	✗	vulnerable to keyboard cache suggestions.
16. Stack Smashing-	✗	✓	✘	✗	✗	vulnerable to a return addresses of function call and allows an attacker redirecting control flow to malicious code
17. **HTTP** URL communication-	✗	✓	✘	✗	✗	Communicating with a backend over HTTP allows an attacker on the network to view all communication and modify the content arbitrarily.

18. Buffer Overflow-	✘	✓	✘	✘	✘	Native code doesn’t replace unsafe memory functions with safe ones.
19. Standhogg 2.0-	✓	✘	✘	✘	✘	Vulnerable to Standhogg 2.0. Please set activity launch mode to ‘SingleTask’ or ‘SingleInstance’
20. AndroidManifest Adb Backup checking-	✓	✘	✘	✘	✘	ADB Backup is enabled for this app. People who have your phone can copy all of the sensitive data for this app in your phone
21. File Unsafe delete checking-.	✓	✘	✘	✘	✘	Everything you delete may be recovered by any user or attacker, especially

						rooted devices
22. Code Setting Preventing Screenshot Capturing-	✓	✘	✘	✘	✘	code setting the prevents screenshot capturing
23. AndroidManifest Exported Components Checking-	✓	✘	✘	✘	✘	Found “exported” component(except for launcher) for receiving Google’s “Android” actions (AndroidManifest.xml)
24. Debug mode checking -	✓	✘	✘	✘	✘	Debug mode checking is OFF