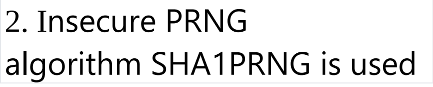
Tools: AppSweep

Apk: Keepassdroid

Issues or warnings	Description
High issues	
1. A password input field does not mask its input field	This app is vulnerable to shoulder-surfing attacks. Several password input fields in the app are not using this masking. Masking password input (e.g., by replacing the letters with dots) partially eliminates this attack vector.
 2. Insecure PRNG algorithm SHA1PRNG is used	The app uses the deprecated random number generation algorithm SHA1PRNG. To avoid using deprecated algorithms, it is recommended to not specify the algorithm, and let the system pick the best algorithm.
Medium issues	
1. Keyboard suggestions	This app is vulnerable to keyboard cache suggestions. It may be a convenient feature but it leakage to other apps while running it. Therefore disabling the keyboard cache for sensitive input fields prevents data leakage.
2. Tap-jacking	This app is vulnerable to tap-jacking attacks.
3. Clear text communication	This app is vulnerable to clear text communication. Disabling this should not allow the attacker to spy on the network.
4. Risk of AES misconfiguration for cipher	The app is using AES in mode AES/ECB, which is likely insecure or misconfigured. Using a misconfigured AES mode potentially allows an attacker to decrypt the encrypted data without a key. Possible misconfigurations could be a weak cipher mode or the usage of a predictable IV. The authenticated encryption mode AES_256/GCM/No Padding is recommended to achieve confidentiality.
5. Stack Smashing	The app is vulnerable to a stack-smashing attack. To prevent this type of attack add the stack canaries. Stack canaries are secret values added to call stack frames which are checked upon function return. They make stack smashing more difficult and can be added automatically by the compiler..
6. Native code compiled without RELRO(Relocation Read-only)	Relocation Read-Only (RELRO) is a technique that makes the Global Offset Table (GOT) of dynamically linked ELF binaries immutable.
7.HTTP URL communication	Communicating with a backend over HTTP allows an attacker on the network to view all communication and modify the content arbitrarily.

8.V1 signature scheme used	The V1 app signature scheme is susceptible to the Janus vulnerability, which allows injecting code without signature modification. This allows attackers to modify the code of the app without affecting their signatures, therefore passing all signature checks successfully.
Low issues	
1.Logs information	Logs may give important information to an attacker, in particular, once sensitive data is logged. But even the log messages in the code itself can give a reverse engineer a lot of information about what is happening and can make reverse engineering much easier.

Apk: Conversation

Issues or warnings	**Description**
High issues	
1. Insecure hashing algorithm MD5 used	Using an insecure hashing algorithm allows an attacker to potentially forge data that has the same hash. In particular, relying on insecure hashes for digital signatures, file integrity, or file identification is potentially insecure.
Medium issues	
1. HTTP URL communication	Communicating with a backend over HTTP allows an attacker on the network to view all communication and modify the content arbitrarily.
2. V1 signature scheme used	The V1 app signature scheme is susceptible to the Janus vulnerability, which allows injecting code without signature modification. This allows attackers to modify the code of the app without affecting their signatures, therefore passing all signature checks successfully.
3. Risk of AES misconfiguration for cipher	The app is using AES in mode AES/ECB, which is likely insecure or misconfigured. Using a misconfigured AES mode potentially allows an attacker to decrypt the encrypted data without a key. Possible misconfigurations could be a weak cipher mode or the usage of a predictable IV. The authenticated encryption mode AES_256/GCM/No Padding is recommended to achieve confidentiality.

4. Clear text communication	This app is vulnerable to clear text communication. Disabling this should not allow the attacker to spy on the network.
Low issues	
1. Logs information	Logs may give important information to an attacker, in particular, once sensitive data is logged. But even the log messages in the code itself can give a reverse engineer a lot of information about what is happening and can make reverse engineering much easier.
2. Unobfuscated email addresses	Hardcoded email addresses may be extracted and used by spammers.