**Mitt Arv Security Testing Report**

**Overview:**

Mitt Arv is an innovative mobile application designed to streamline and enhance personal wealth management for its users. Currently in its beta phase and available exclusively on Android devices, Mitt Arv offers features such as financial tracking, budgeting tools, and secure transaction management. As it continues to evolve, ensuring the app’s security is of paramount importance to protect user data and maintain trust.

**Objective of the Security Testing:**

This security assessment aimed to uncover and document any vulnerabilities within the Mitt Arv app that could affect its security posture. Identifying these vulnerabilities early in the beta phase is critical for addressing potential risks before the app's public release.

**Scope of Testing:**

**Functional Security Testing:**

* **Improper Data Validation:**

During the security testing of the Mitt Arv app, I have discovered that the some fields accepts the alphanumeric input but that fields are intended to accept only numeric values like the field which is taking amount.

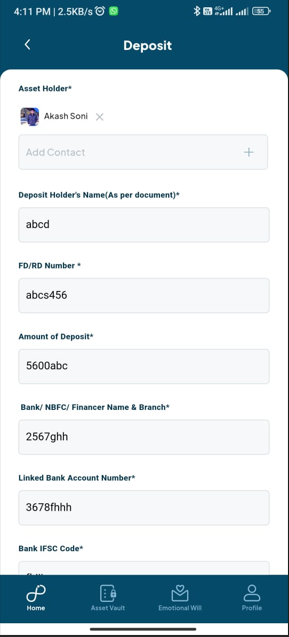
**Impact:**

**Data Integrity:** Accepting non-numeric input in a numeric field can lead to incorrect or corrupted data being stored or processed.

**Application Behavior:** The app may not handle unexpected input correctly, which can cause errors or crashes.

**User Experience:** Accepting invalid input can confuse users and undermine their trust in the app’s reliability.

**Screenshot:**



* **Taking too much Permission:**

This application is requesting a large number of permissions. However, the application does not provide clear explanations or justifications for why these permissions are needed. This lack of transparency raises concerns about user privacy and data security.

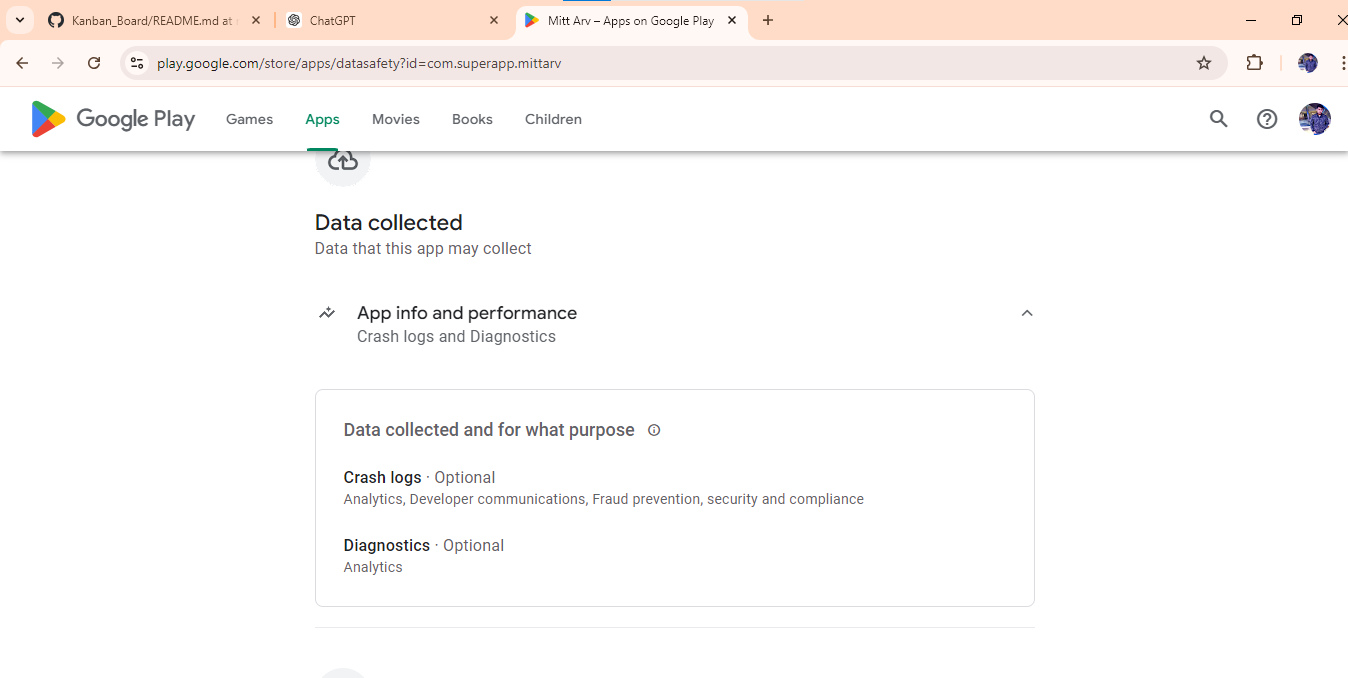
**Impact:**

**Access to Sensitive Information:** If the application requests permissions such as access to contacts, location, camera, or microphone without a clear reason, it can lead to unauthorized access to sensitive personal information.

**User Distrust:** Users may become worry of the application if they feel their personal data is being accessed without justification. This could lead to lower user engagement or even un-installation of the app.

**Data Breaches:** Excessive permissions increase the risk of data breaches, as more data is exposed to potential security vulnerabilities. If the app has access to sensitive data, a security flaw could lead to this information being compromised.

**Screenshot:**

****

**Code and Configuration Review:**

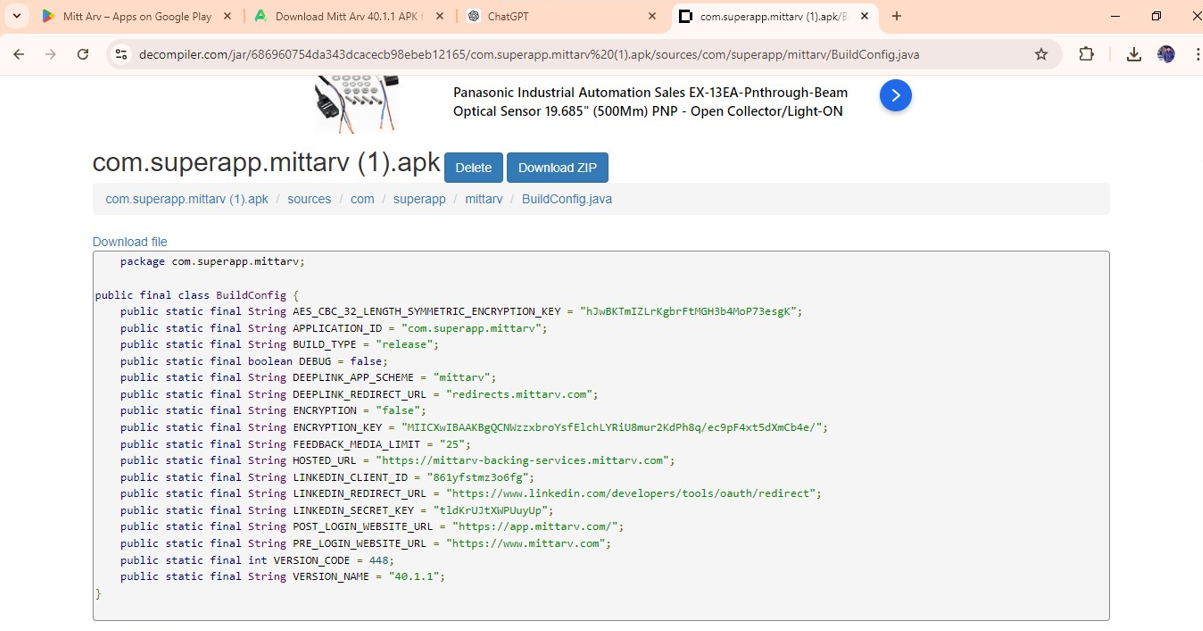
* **Exposure of Encryption keys and secret keys:**

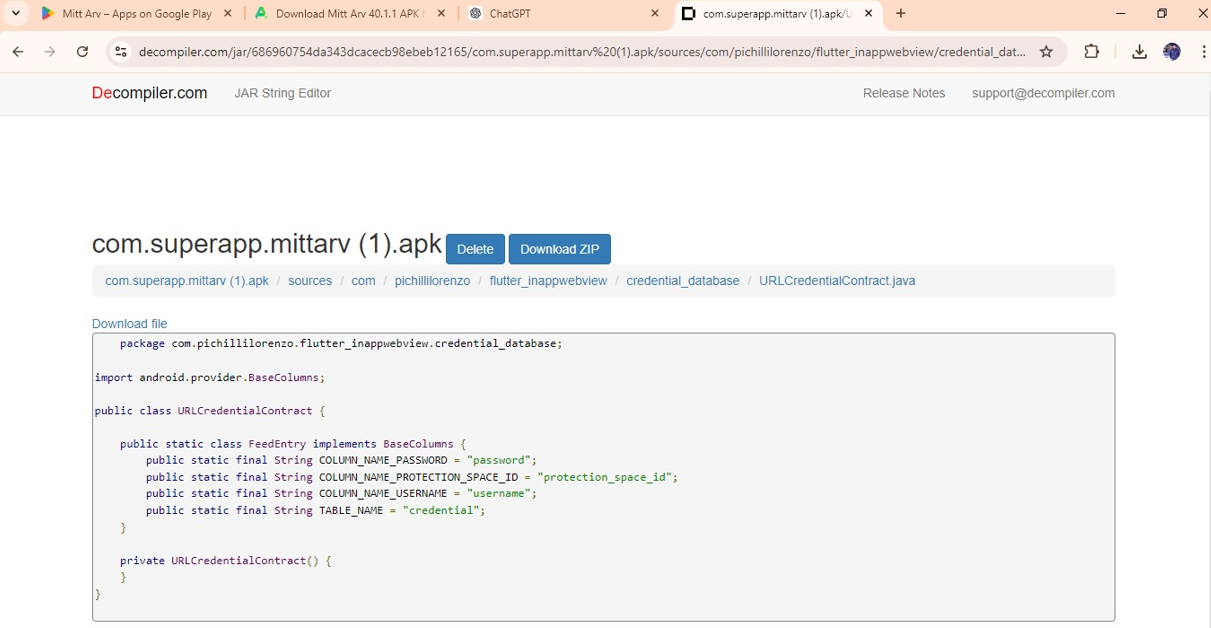
During the code and configuration review of the Mitt Arv app, I have found that sensitive encryption keys and secret keys are visible in the source code/configuration files. These keys are crucial for securing cryptographic operations and should be protected to prevent unauthorized access.

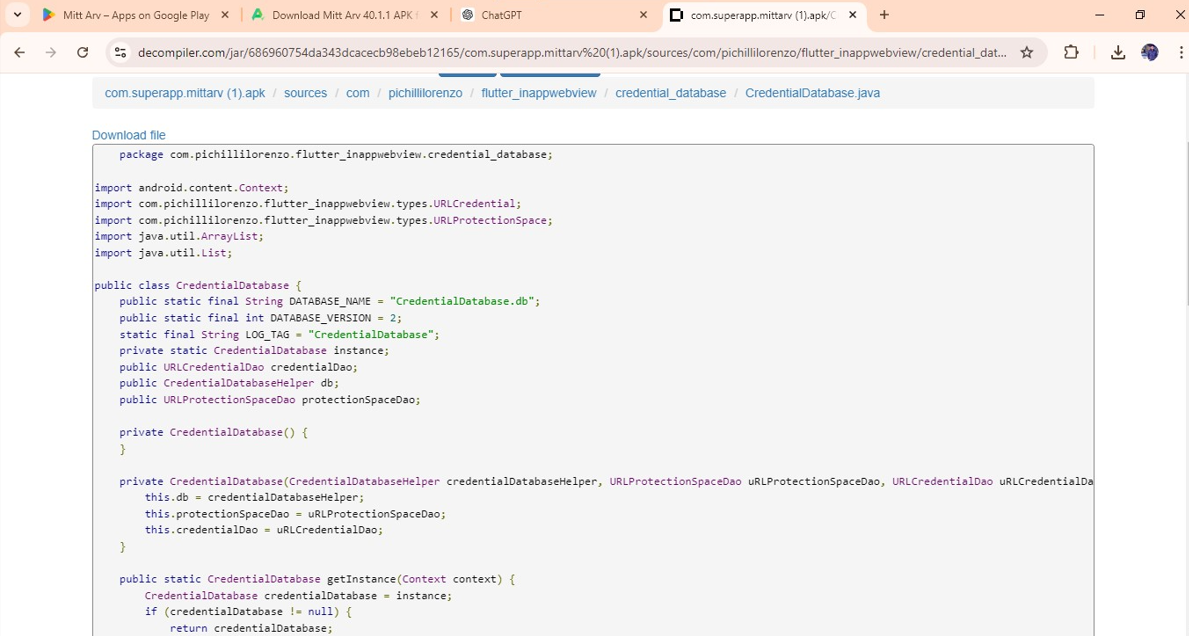
**Impact:**

* **Security Risk:** Exposure of encryption and secret keys can lead to unauthorized decryption of data, data breaches, and exploitation of the app’s security mechanisms.
* **Data Integrity and Confidentiality:** Attackers with access to these keys could compromise the confidentiality and integrity of user data.
* **Regulatory Compliance:** Keeping sensitive keys directly in the source code can break data protection rules and best practices, which could lead to compliance issues.

**Screenshots:**

****





**Conclusion:**

This report summarizes the identified issues, their impacts, and the proper screenshots to mitigate them, providing a clear path forward for improving the app’s security.