Security Analysis & Recommendations for Mitt Arv

Security Issues Identified & Recommended Solutions

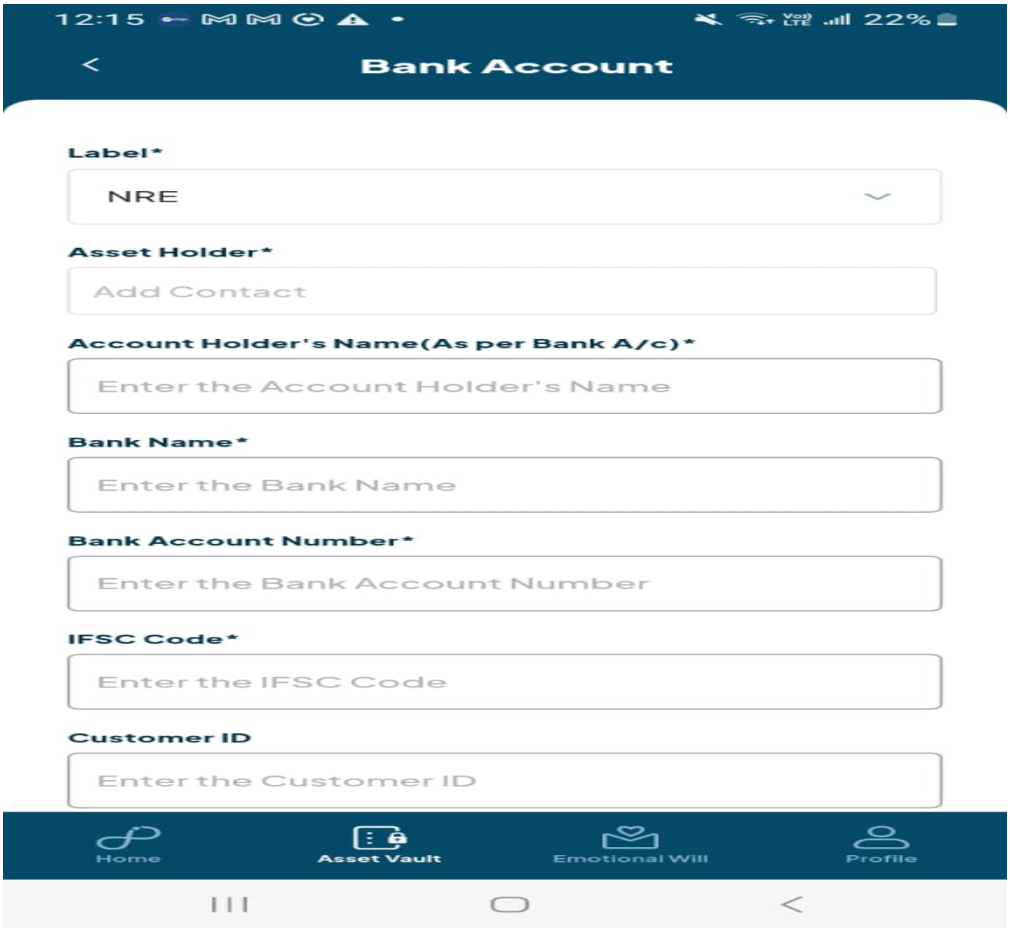
As part of the security assessment of Mitt Arv, I have identified several vulnerabilities that could compromise user data and system integrity. Below is a detailed analysis of these issues and the corresponding solutions to mitigate them.

---

1. Weak Authentication & Session Handling

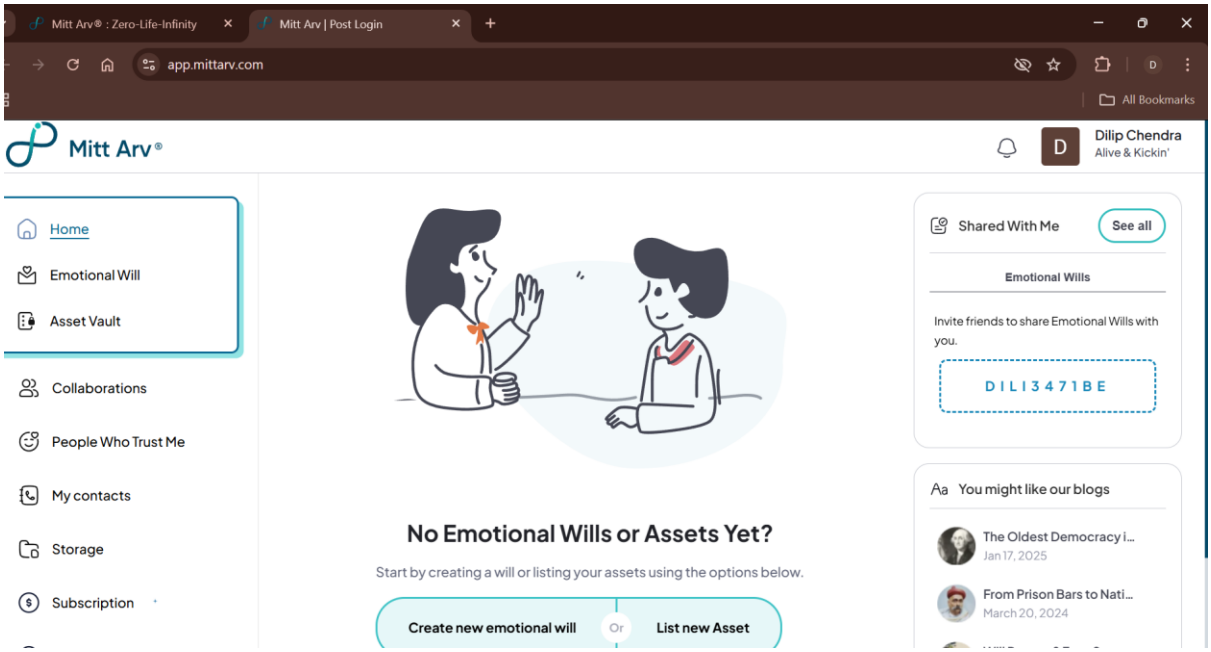
🚨 **Issue 1: No Multi-Factor Authentication (MFA)**

- **Risk:** If a hacker obtains login credentials through phishing or brute force attacks, they can gain full access to user accounts and sensitive data. ✅ **Solution:** Implement **Multi-Factor Authentication (MFA)** by integrating **OTP-based login** and **biometric authentication (Face ID, Fingerprint)** to add an extra layer of security.



🚨 **Issue 2: Weak session expiration policies**

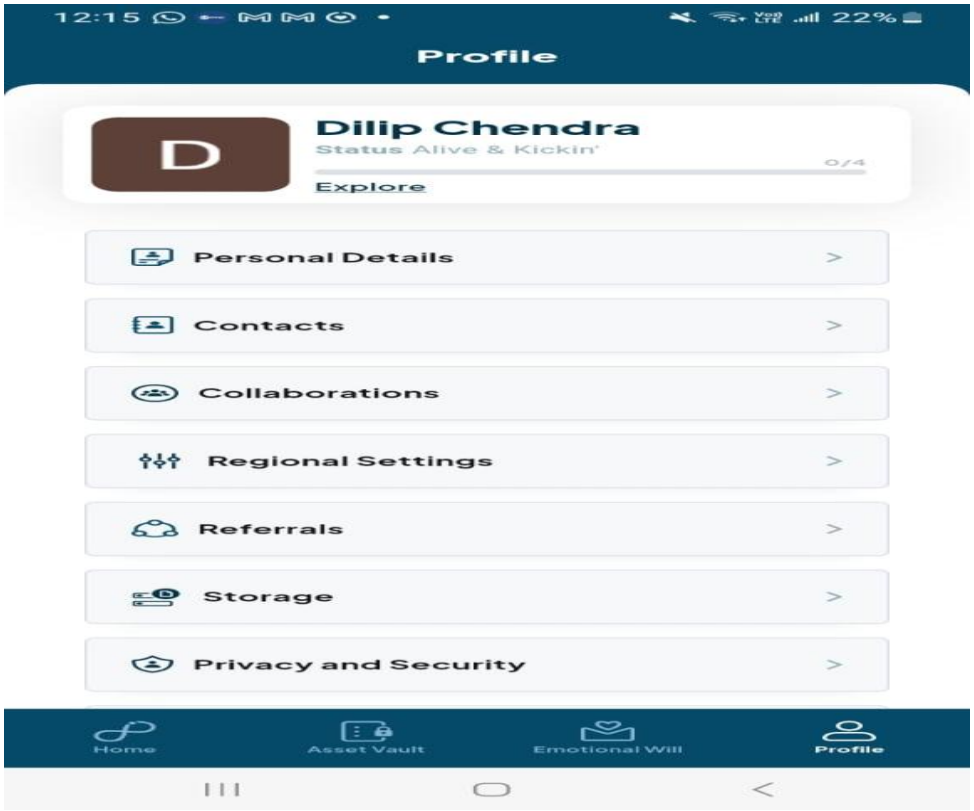
- **Risk:** If a user logs in from a shared or public device and forgets to log out, the session remains active, increasing the risk of unauthorized access. ✅ **Solution:** Enforce **automatic session expiration** after **15 minutes of inactivity** and introduce a **logout reminder** feature.

- 

---

2. API Security Issues

🚨 Issue 3: No rate limiting on login attempts

- **Risk:** Attackers can attempt unlimited login combinations, making brute-force attacks easier.
  ✅ **Solution:** Implement **rate limiting** to **restrict login attempts to a maximum of 5 per minute** and introduce **captcha verification** after multiple failed attempts.
- 

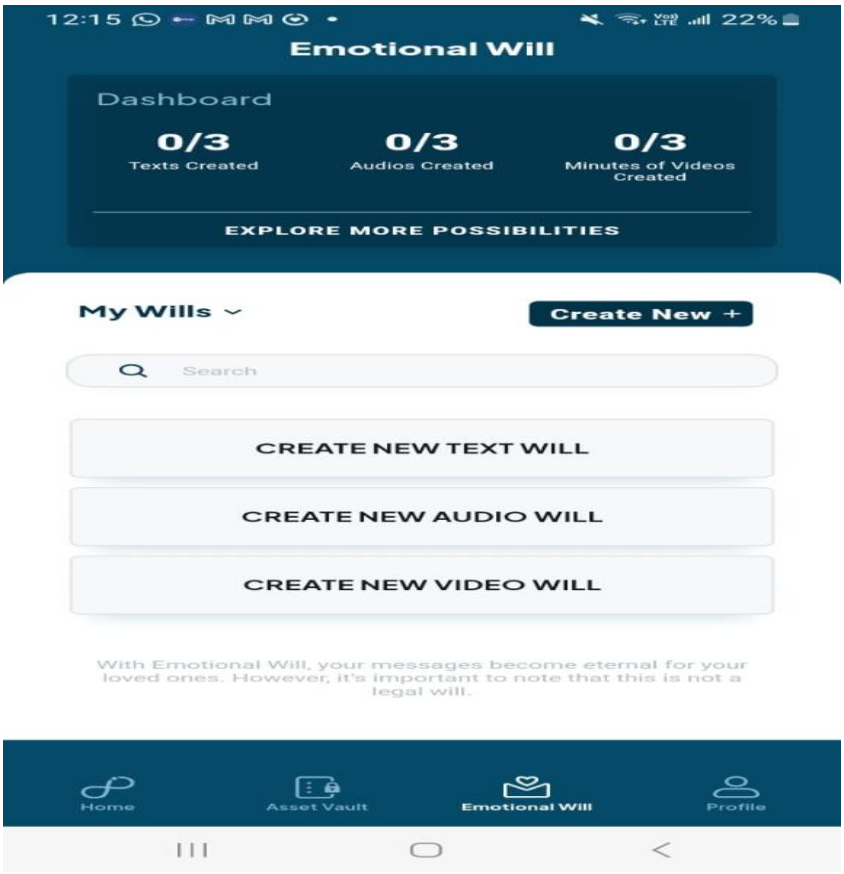
🚨 Issue 4: API keys stored in the app code

- **Risk:** If an attacker decompiles the app, they can extract API keys and exploit them to access sensitive system functions. ✅ **Solution:** Store API keys securely on the **server-side**, using **environment variables** or a **secure vault** instead of hardcoding them into the app.

---

3. Data Privacy & Encryption Gaps

🚨 **Issue 5: Lack of End-to-End Encryption for Messages & Vault**

- **Risk:** Messages and sensitive data stored in the vault are vulnerable to interception or unauthorized access. ✅ **Solution:** Implement **AES-256 encryption** for all stored and transmitted data, ensuring that only intended recipients can decrypt the messages.
- 

🚨 **Issue 6: No Self-Destructing Messages**

- **Risk:** Sensitive messages remain accessible indefinitely, increasing the risk of data exposure. ✅ **Solution:** Introduce a **self-destructing message feature**, allowing users to set messages to delete automatically after being viewed once.

---

4. Legal & Financial Security Enhancements

🚨 **Issue 7: No AI-Powered Legal Will Drafting**

- **Risk:** Users may struggle with structuring wills according to legal requirements, leading to potential disputes. ✅ **Solution:** Integrate **AI-powered legal templates** based on country-specific inheritance laws, offering **automated suggestions** for will drafting.

🚨 **Issue 8: No Secure Financial Institution Integration**

- **Risk:** Users cannot link their bank accounts securely to track asset values, increasing manual errors and risks. ✅ **Solution:** Enable **secure bank account linking** with **multi-layer encryption** and **automatic updates on asset values**.

---

5. Additional Security Enhancements

✅ **Periodic Update Reminders**: Notify users every **3-6 months** to update their asset details and emotional messages. ✅ **Digital Executor Role**: Allow users to assign a trusted person to validate and execute their final wishes securely. ✅ **Encrypted Cloud Backup & Secure Export Options**: Provide **cloud storage** with **end-to-end encryption** and allow users to **securely download and store wills**.

Conclusion

By addressing these vulnerabilities and implementing the proposed solutions, Mitt Arv can significantly enhance its security, protecting users' sensitive information and ensuring compliance with modern cybersecurity standards. Further advancements, such as **blockchain-based asset verification** and **decentralized identity management**, can be explored in the future to strengthen system integrity even further.
