# **Project Phase 6: Security Recommendations**

a. What is your security recommendation? Why did you choose it?

a. Security Recommendation: To improve the protection of user accounts and sensitive financial data, implement secure authentication procedures like multi-factor authentication (MFA). Secure authentication is crucial for preventing unauthorized access to the expense tracker app and safeguarding users' financial information. By implementing MFA, we can add an extra layer of security beyond traditional password-based authentication, reducing the risk of account compromise due to stolen or weak passwords.

b. Who does the recommendation benefit (end-user, developer, etc.)?

b. The advice to utilize secure authentication is advantageous to developers as well as end users. While developers gain by lowering the risk of security breaches and associated liabilities, end users gain from enhanced security and protection of their financial data.

c. If the recommendation was found somewhere other than the provided checklist, include a link to it.

c. While the recommendation for implementing secure authentication is not explicitly listed in the provided Android App Security Checklist, it is widely recognized as a best practice for securing mobile applications. Resources such as OWASP Mobile Security Project (https://owasp.org/www-project-mobile-security/) provide guidance on implementing secure authentication in mobile apps.

d. When would the recommendation have to be implemented (based on how serious the security risk is)?

d. Given the sensitivity of financial data handled by the expense tracker app, the recommendation for implementing secure authentication should be prioritized and implemented as soon as possible. Timely implementation is essential to mitigate the risk of unauthorized access and potential financial losses for users.

e. Why do you think your project needs your recommendation?

e. Since our project handles the management of sensitive financial data, the proposal for integrating secure authentication is necessary. Insufficient authentication protocols may leave user accounts and financial information open to unwanted access, which could result in privacy violations and financial fraud.

f. How do you think your recommendation could be applied?

f. By including authentication measures in the app's login procedure, users can put the advice to implement safe authentication—such as multi-factor authentication—into practice. To securely authenticate users' identities, this entails putting in place technologies like OTP (one-time password), biometric authentication, or device-based authentication.

i. How feasible would the implementation be?

i. It is possible to implement safe authentication mechanisms like multi-factor authentication (MFA), but doing so needs careful preparation and integration with the app's architecture. Secure authentication features in mobile applications may be implemented rather easily due to modern authentication frameworks and libraries, though they may add some complexity to the development process. The security advantages, when properly implemented, greatly exceed the drawbacks.