Financial Applications Features

Security Guidelines

version 1.0

securing

FINANCIAL APPLICATIONS FEATURES – SECURITY GUIDELINES (FAFSG)

Author

Łukasz Bobrek

Introduction

Financial Applications Features - Security Guidelines (FAFSG) is a set of two FREE checklists created to provide guidelines on the security features which you can implement to make your mobile app more secure. It is meant for continuous development as well as use in current application improvements.

The project is based on the actual state of banking applications, but keep in mind that FAFSG is not a technical standard. It does not cover implementation guidelines and quality of the proposed features. For such guidelines, please refer to *OWASP ASVS* for web applications and *OWASP MASVS* for mobile applications.

Objectives

The goal of FAFSG is to help to make security decisions for developers, architects, reviewers and vendors in order to implement essential security features in financial applications. Those features would help to protect users' data and increase overall security of the application.

Use cases

You can use the FAFSG checklist in multiple ways: - As a starting point for application design phase.

- As a measure of application security and maturity.
- As a formal security features list for third parties developing the application for you.
- To point areas which need further development regarding security.

The entire checklist is in a form similar to OWASP APPLICATION SECURITY VERIFICATION STANDARD v4.0.
Every category has a brief description of the control objectives and a list of security features verification requirements.

Key areas that have been included

Web applications

- V1: Authentication
- V2: Authorization
- V3: Session Management
- V4: Credentials Quality
- V5: Payment Cards
- V6: Limits
- V7: Notification
- V8: Contact

Mobile applications

- V1: Authentication
- V2: Autorization
- V3: Session Management
- V4: Credentials Quality
- V5: Payment Cards
- V6: Limits
- V7: Notifications
- V8: Contact
- V9: Mobile Platform

Contribution

All kinds of suggestions and requests are highly appreciated! If you want to improve the project in any way - please contact me on Linkedin or Twitter. Also, pull requests are more than welcome!

License

WEB APPLICATIONS

V1: Authentication

Control Objective

Category "V1" lists security features related to authentication mechanism in the financial applications.

Security Features Verification Requirements

#	Description	
1.1	Enable two factor authentication (for instance, login/password and trusted browser or mobile confirmation).	
1.2	Do not use authentication with a masked password.	
1.3	Encourage or enforce users to use 2FA (gamification/reward is a plus).	
1.4	Ensure that user enumeration is not possible. Application should respond in exactly the same way and with the same delay in all authorization scenarios.	
1.5	Verify if the authorization message (PUSH, SMS or email) contains detailed information regarding authorized operation. In case of a trusted browser, authorization messages should contain its location, name etc.	
1.6	Allow users to choose whether they want to authorize only single access or save browser as trusted. Remember that for PSD2 compliant applications, 2FA should be repeated in less than 90 days.	

References

For more information, see also:

- OWASP ASVS V2 Authentication
- CWE 287 (Improper Authentication)

V2: Authorization

Control Objective

Category "V2" lists security features related to authorization mechanism in the financial applications.

Security Features Verification Requirements

#	Description	
2.1	Each authorization message should contain details about the authorized operation. For instance, for a new transaction, the authorization message should contain the operation date, amount and the beneficiary account (to protect against man-in-the-browser malware).	
2.2	Allow users to choose from multiple authorization channels (PUSH, SMS OTP, email OTP), according to their preferences.	
2.3	Ensure that any change to authorization method requires authorization with the previously used channel.	
2.4	Encourage PUSH authorization as it is considered most secure.	
2.5	In case of OTP, code must be unique, random and at least 6 character long. OTP codes shoud also be protected against brute-force attacks with request throttling.	
2.6	OTP codes should be protected against brute-force attacks with request throttling.	
2.7	Each security sensitive operation, such as transaction, adding trusted account or any user account changes should require authorization.	
2.8	User interface should list previous and current authorization requests and their results.	

References

For more information, see also:

- OWASP Authorization Cheat Sheet
- CWE 285 (Improper Authoriation)

V3: Session Management

Control Objective

Category “V3” lists security features related to session management in the financial applications.

Security Features Verification Requirements

#	Description	
3.1	User interface should list current and past sessions and failed login attempts.	
3.2	Ensure that application logs out after a predefined inactivity period.	
3.3	Implement a list of paired mobile devices and allow the user to deactivate any mobile device in case of its theft, loss or compromise.	

References

For more information, see also:

- OWASP ASVS V3 Session Management

V4: Credentials Quality

Control Objective

Category "V4" lists security features related to credentials quality in the financial applications.

Security Features Verification Requirements

#	Description	
4.1	Password change should require old password, new password and second factor authorization.	
4.2	Do not accept short passwords (shorter than 12 characters).	
4.3	If you limit password length, enforce users to use at least one character, one special sign and one number.	
4.4	Do not accept re-use of previously used passwords.	

References

For more information, see also:

- OWASP Web Application Security Testing Guide 4.1
- CWE 521 (Weak Password Requirements)

V5: Payment Cards

Control Objective

Category "V5" lists security features related to payment cards management in the financial applications.

Security Features Verification Requirements

#	Description	
5.1	Allow users to temporarily and reversibly lock their payment cards.	
5.2	Allow users to enable and disable payment card integration with Google Pay and Apple Pay. Do not implement HCE on your own.	
5.3	Implement PIN change functionality from the web application level.	
5.4	Application should let the user to configure which payment options are allowed (internet, contactless, magnetic, abroad etc.).	
5.5	Payment card number should be considered as sensitive data and should not be fully visible in the application UI without additional authorization.	
5.6	Introduce virtual payment cards, which can be used only for single internet transactions.	

V6: Limits

Control Objective

Category "V6" lists security features related to limits management in the financial applications.

Security Features Verification Requirements

#	Description	
6.1	Limits should be predefined by default for each user.	
6.2	Allow users to configure limits upon their needs and preferences.	
6.3	Limits settings should be highly customizable and granular. User should be able to modify limits for each channel separately (web, internet, credit card etc.), by daily amount, monthly amount and by the number of transactions.	
6.4	Implement temporary limits, which allow users to change limits only till the end of the day.	

V7: Notification

Control Objective

Category "V7" lists security features related to notifications management in the financial applications.

Security Features Verification Requirements

#	Description	
7.1	Verify if the users can configure which notification to receive.	
7.2	Allow users to choose which channel should they receive notifications to.	
7.3	Allow users to specify exactly which operation should the users be additionally notified.	
7.4	Disabling notifications for key operations (password or 2-FA device change) must require 2-FA authorization.	

V8: Contact

Control Objective

Category "V8" lists security features related to secure contact channel with the customer support of the financial applications.

Security Features Verification Requirements

#	Description	
8.1	Implement authorized contact functionality. Users should be able to initiate authorized chat/call from the authorized web application session.	
8.2	Send users encrypted documents. Allows users to define in configuration options to set encryption passwords.	

MOBILE APPLICATIONS

V1: Authentication

Control Objective

Category "V1" lists security features related to authentication mechanism in the mobile financial applications.

Security Features Verification Requirements

#	Description	
1.1	Implement application pairing - when implemented, the unique and random application instance identifier can be treated as a second factor in user authorization alongside knowledge of PIN code. Instance identifier should be stored in dedicated, encrypted storge.	
1.2	Use additional data to pair an application, for example QR code from an authorized web session.	
1.3	Ensure that user enumeration is not possible. Application should respond in exactly the same way and with the same delay in cases of providing valid username with invalid password, and invalid username - both for pairing and authorization.	
1.4	Use different authentication methods for web and mobile applications. Avoid situations when users can login both to web and mobile with exactly the same credentials. Password for web and PIN or biometrics for mobile is a good solution.	

References

For more information, see also:

- OWASP MASVS V4 Authentication and Session Management
- CWE 287 (Improper Authentication)

V2: Autorization

Control Objective

Category "V2" lists security features related to authorization mechanism in the mobile financial applications.

Security Features Verification Requirements

#	Description	
2.1	Each authorization message should contain details about authorized operation. For instance, for the new transaction, the authorization message should contain the operation date, amount and the destination account.	
2.2	Ensure that authorization method is different from authentication - for instance use PIN for authentication and biometry for authorization or use different PIN codes.	
2.3	Ensure that any change to authorization method requires authorization with the previously used channel.	
2.4	Do not use authorization with SMS codes because of the risk of SIM-swapping attacks and MiTM on GSM protocols.	
2.5	Encourage PUSH-alike authorization as it is considered the most secure.	
2.6	Each security sensitive operation, such as transaction, adding a trusted account or any user account changes should require authorization.	
2.7	User interface should list previous and current authorization requests and their results.	

References

For more information, see also:

- OWASP Authorization Cheat Sheet
- CWE 285 (Improper Authoriation)

V3: Session Management

Control Objective

Category "V3" lists security features related to session management in the mobile financial applications.

Security Features Verification Requirements

#	Description	
3.1	User interface should list current and past sessions and failed login attempts.	
3.2	Ensure that application logs out after a predefined inactivity period.	
3.3	Verify that the logout button is visible and easily accessible in the application. Ensure that logout terminates the session on the server side.	
3.4	Allow the user to remove application data, which results in "unpairing" of the application.	

References

For more information, see also:

- OWASP MASVS V4 Authentication and Session Management

V4: Credentials Quality

Control Objective

Category "V4" lists security features related to credentials quality in the mobile financial applications.

Security Features Verification Requirements

#	Description	
4.1	Password change should require the old password/PIN, the new one and 2-FA authorization.	
4.2	Do not accept short passwords (shorter than 12 characters) and short PINs (shorter than 6 digits).	
4.3	If you limit password length, enforce users to use at least one character, one special sign and one number. In case of PINs, deny incremental numbers (i.e. 1234) and repetitions of one number (i.e. 111111).	

References

For more information, see also:

- OWASP Web Application Security Testing Guide 4.1
- CWE 521 (Weak Password Requirements)

V5: Payment Cards

Control Objective

Category "V5" lists security features related to payment cards management in the mobile financial applications.

Security Features Verification Requirements

#	Description	
5.1	Allow users to temporarily and reversibly lock their payment cards.	
5.2	Allow users to enable and disable payment card integration with Google Pay and Apple Pay. Do not implement HCE on your own.	
5.3	Implement PIN change functionality from the mobile application level.	
5.4	Mobile Application should let the user to configure which payment options are allowed (internet, contactless. magnetic, abroad etc.).	
5.5	Payment card number should be considered as sensitive data and should not be fully visible in the application UI without additional authorization.	
5.6	Introduce virtual payment cards, which can be used only for single internet transactions.	

V6: Limits

Control Objective

Category "V6" lists security features related to limits management in the mobile financial applications.

Security Features Verification Requirements

#	Description	
6.1	Limits should be predefined by default for each user.	
6.2	Allow users to configure limits upon their needs and preferences.	
6.3	Limits settings should be highly customizable and granuar. User should be able to modify limits for each channel separately (web, internet, credit card etc.), by daily amount, monthly amount and by the number of transactions.	
6.4	Implement temporary limits, which allow users to change limits only till the end of the day.	

V7: Notifications

Control Objective

Category “V7” lists security features related to notifications management in the mobile financial applications.

Security Features Verification Requirements

#	Description	
7.1	Verify if the users can configure which notification to receive.	
7.2	Allow users to choose which channel should they receive notifications to.	
7.3	Allow users to specify exactly which operation should the users be additionally notified.	

V8: Contact

Control Objective

Category "V8" lists security features related to the secure contact channel with the customer support of the mobile financial application.

Security Features Verification Requirements

#	Description	
8.1	Implement authorized contact functionality. Users should be able to initiate authorized chat/call from the authorized mobile application session.	

V9: Mobile Platform

Control Objective

Category "V9" lists security features specific for financial applications dedicated for mobile platforms.

Security Features Verification Requirements

#	Description	
9.1	Implement root/jailbreak detection.	
9.2	Implement anti-tampering checks accordingly (check for debuggers, instrumentation tools, memory tampering etc.)	
9.3	On Android, additionally implement vendor and integrity verification. On iOS, use DevieceCheck and AppAttest mechanisms.	
9.4	Use certificate pinning mechanism in order to protect communication between mobile device and the server.	
9.5	To protect sensitive data, override application snapshots from views with sensitive data.	
9.6	Implement a dedicated keyboard for sensitive data fields input, such as PIN or passwords.	
9.7	Obfuscate source code in order to make reverse engineering harder.	
9.8	Use external libraries visely - introduce libraries verification and updating policy.	

References

For more information, see also:

- OWASP MASVS V8 resiliency Against Reverse Engineering
- OWASP MSTG

Need more help?

Our services:

- **App Security Testing** (web, mobile, blockchain)
- Infrastructure Security Testing (traditional, cloud, macOS)
- Device Security Testing
- Thread Modeling
- Red Teaming

Our trainings:

- Security Aware Developer
- Practical AWS Security Training
- Purple Teaming
- Hackflix & Skill

Contact the author:

lukasz.bobrek@securing.pl

SecuRing sp. z o.o. sp. k | Kalwaryjska 65/6 | 30-504 Krakow

www.securing.pl