API SECURITY AUDIT

Presented By: VIKRAM GHADGE

API SECURITY AUDIT INDEX

Security of the application is depend on many factors.

AUTHENTICATION

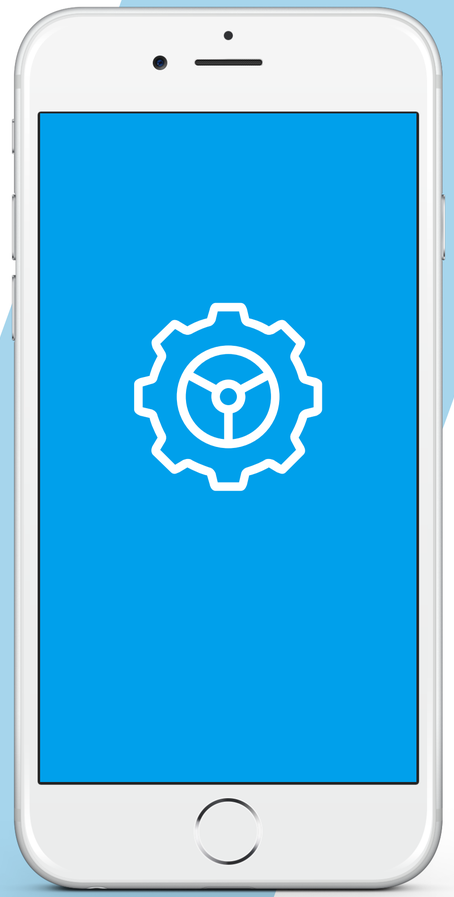
Having a good authentication system will always help to keep hackers away.

RESOURCE ACCESS

Quick response for API is very important for the performance of the application

SECURITY

App security is compromised if there is no standard used in the API implementation



AUTHENTICATION

Having a good authentication system will always help to keep hackers away.

Risk	Control Objective	Expected Control	Assessment Approach
Using an outdated method for securing user login may lead to unauthorized access.	To ensure user data and access right is been protected.	Latest standards must be used to secure login for the user. Which may include OAUTH2 or more security layers according to core architecture. The policy, its associated procedures, and standards include: • Policy/method used to protect user identity needs to documented. • User data access encryption policy and document related to the same. • Test cases to protect authorization. • Third party verification for authorization.	Confirm that the managing agent has: i) A written authorisation strategy documentation approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Written documentation supporting authorisation policy and access methods. iii) Details description for authorisation architecture usage. • communication of the encryption policy, associated procedures, and standards to the relevant stakeholders and individuals responsible for ownership and management of architecture used in the internal model. • Test cases related to authorisation • third party validation and verification.
To avoid access from other network and unknown devices we need two-factor authentication.	Two-factor authentication will ensure protect the access of your data with OPT or any other medium.	Two factor Authentication policy and document about how to generate specific OTP for users. The policy, its associated procedures, and standards include: • Two Factor Authentication framework document • Which are the ways used to protect users OTP access • Documents which support Preventing unauthorised access using OTP. • Third party verification for TFA.	Confirm that the managing agent has: i) A written strategy to providing Two Factor Authentication approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Test cases to about two factor authentication and unauthorised access. iii) Third party verification documents

RESOURCE ACCESS

Quick response for API is very important for the performance of the application

Risk	Control Objective	Expected Control	Assessment Approach
Caching will help the server to reduce load when a request for the same data.	To help server to balance the load. Using this performance of mobile will increase.	Policy for caching API’s and which API's need to cache. The policy, its associated procedures, and standards include: • define a strategy for caching of API’s. • Server caching and image caching strategy • Image and Filestore strategy, also accessing without impacting API layers. • Test cases to verify these strategies been implemented.	Confirm that the managing agent has: i) A written document about accessing and storing files approved by management with an appropriate degree of challenge and oversight in its development as evidenced through discussions. ii) Caching mechanism for API with verified API's which been cashed. iii) Test cases to verify strategies.

SECURITY

App security is compromised if there is no standard used in the API implementation

Risk	Control Objective	Expected Control	Assessment Approach
1. Different auth layer will protect current business logic and user data	To ensure after DDOS attach our data will be protected by auth layer.	Detailed technical document to verify the auth server. The policy, its associated procedures, and standards include: • The policy must contain detail about auth server and its implication. • Resource acceding strategy • DDOS protection policies and implementation • Third party verification about auth layer.	Confirm that the managing agent has: i) Documentation supporting auth layer implementation approved by specific management. ii) DDOS attach scenario process and recovery policies. iii) Third party verification.
1. Third party API integration and access are one of the major areas where unauthorized access happen.	To ensure the protection of data third-party API integration or access must be monitored with proper guidelines.	Detailed technical document to enforce guidelines to integrate third-party API's or allowed access. The policy, its associated procedures, and standards include: • Third party API registration and verification • Third party libraries and alternatives decision document. • Policy for third-party data theft and recovery. • Third party libraries test and verification.	Confirm that the managing agent has: i) Third party library integration document and decision document approved by the authority. ii) Third party API integration test cases and test reports