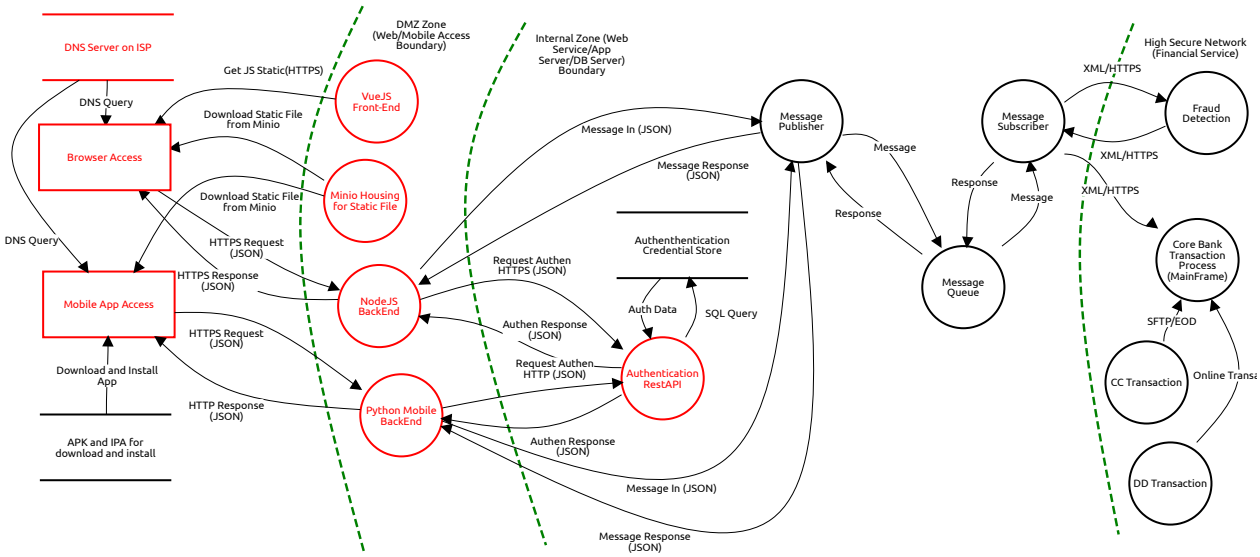
Threat model report for Online Banking Transaction

Owner:
Praparn Lueangphoonlap
Reviewer:
Praparn Lueangphoonlap
Contributors:

High level system description

Online Banking System



VueJS Front-End (Process)

Description:
Download Front-End as JS Script (Static Web)

Possibly target of DDOS on single target

Denial of service, Open, Medium Severity

Description:
For static web front will be target for attacker to operate DDOS for bring front-end out-of-service

Mitigation:

Minio Housing for Static File (Process)

Description:
- Image
- Video

Unauthorize request for update/delete static file

Tampering, Open, Medium Severity

Description:
As static file was allowed accessible from public network. Attacker possible to mitigate and update/delete static file with malicious file for spread to client

Mitigation:

Possibly target of DDOS on single target

Denial of service, Open, Medium Severity

Description:
Attacker can operate DDOS to Minio as static file for make it out-of-service and risk to public ip will get into black list

Mitigation:

Get JS Static(HTTPS) (Data Flow)

Description:

No threats listed.

Download Static File from Minio (Data Flow)

Description:

No threats listed.

NodeJS BackEnd (Process)

Description:

Vulnerability assessment for RestAPI

Elevation of privilege, Open, High Severity

Description:
Need process to check vulnerability/security enhancement for make sure nodejs have properly secure configuration enough for operate on production (A6:Security Misconfiguration)

Mitigation:

Penetration testing for RestAPI

Tampering, Open, Medium Severity

Description:
Unauthorize access to RestAPI will make attacker can stolen sensitive information and critical transaction operate (A2:Broken Authentication)

Mitigation:

Lack of Module Log and Monitoring

Tampering, Open, Medium Severity

Description:
Lack of module log and monitoring will make security bind and hard to track when attack event occur (A10: Insufficient Logging & Monitoring)

Mitigation:

Validation for deserialize data from web browser

Elevation of privilege, Open, High Severity

Description:
All restapi need to validate data come from browser for make sure all data receive was validated (A8: Insecure Deserialization)

Mitigation:

Mobile App Access (External Actor)

Description:

Out-of-date mobile device's version cause vulnerability on OS

Repudiation, Open, High Severity

Description:
Android and IOS with out-of-date version will bring huge of "know vulnerability" and make device infected (A9: Know Vulnerability)

Mitigation:

Sensitive data classification

Information disclosure, Open, Medium Severity

Description:
Any information cache, databaselite store on mobile need to classified (A3:Sensitive data classification)

Mitigation:

APK and IPA for download and install (Data Store)

Description:
-APK housing on google play
-IPA housing on app store

No threats listed.

Download Static File from Minio (Data Flow)

Description:

No threats listed.

HTTPS Request (JSON) (Data Flow)

Description:

No threats listed.

HTTPS Request (JSON) (Data Flow)

Description:

No threats listed.

Python Mobile BackEnd (Process)

Description:
Response all main transaction of online banking

Vulnerability assessment for RestAPI

Elevation of privilege, Open, High Severity

Description:
Need process to check vulnerability/security enhancement for make sure nodejs have properly secure configuration enough for operate on production (A6:Security Misconfiguration)

Mitigation:

Penetration testing for RestAPI

Tampering, Open, Medium Severity

Description:
Unauthorize access to RestAPI will make attacker can stolen sensitive information and critical transaction operate (A2:Broken Authentication)

Mitigation:

Lack of Module Log and Monitoring

Tampering, Open, Medium Severity

Description:
Lack of module log and monitoring will make security bind and hard to track when attack event occur (A10: Insufficient Logging & Monitoring)

Mitigation:

Validation for deserialize data from mobile

Elevation of privilege, Open, High Severity

Description:
All restapi need to validate data come from browser for make sure all data receive was validated (A8: Insecure Deserialization)

Mitigation:

Authenthentication Credential Store (Data Store)

Description:
Database for customer authentication

No threats listed.

Download and Install App (Data Flow)

Description:
Android from play store
Iphone from app store

No threats listed.

DNS Server on ISP (Data Store)

Description:

DNS Cache Poisoning

Spoofing, Open, High Severity

Description:
Attacker from outside can attack for redirect traffic of user to malicious web front, restfulapi. This can bring customer's information leak/infected and finally indirect attack to online banking system

Mitigation:

DNS Attack for Denied of Service

Denial of service, Open, High Severity

Description:
For indirect attack system. Attacker can positioning to attack dns server instend of system directly. This make client unable to access system due to dns cannot be resolve

Mitigation:

DNS Query (Data Flow)

Description:

No threats listed.

DNS Query (Data Flow)

Description:

No threats listed.

HTTPS Response (JSON) (Data Flow)

Description:

No threats listed.

HTTP Response (JSON) (Data Flow)

Description:

No threats listed.

Authentication RestAPI (Process)

Description:

Single factor authentication

Spoofing, Open, Medium Severity

Description:
Authentication with single factor may bring risk for authorize access. If attacker stolen credential from user side/bruce force/forget password funcation as A2 Broken Authentication on OWASP

Mitigation:

Request Authen HTTPS (JSON) (Data Flow)

Description:

No threats listed.

Authen Response (JSON) (Data Flow)

Description:

No threats listed.

Request Authen HTTP (JSON) (Data Flow)

Description:

No threats listed.

Authen Response (JSON) (Data Flow)

Description:

No threats listed.

Auth Data (Data Flow)

Description:

No threats listed.

Message Publisher (Process)

Description:

No threats listed.

Core Bank Transaction Process (MainFrame) (Process)

Description:

No threats listed.

SQL Query (Data Flow)

Description:

No threats listed.

Message (Data Flow)

Description:

No threats listed.

Message In (JSON) (Data Flow)

Description:

No threats listed.

Message (Data Flow)

Description:

No threats listed.

Message Response (JSON) (Data Flow)

Description:

No threats listed.

Message Response (JSON) (Data Flow)

Description:

No threats listed.

Message Queue (Process)

Description:

No threats listed.

Message Subscriber (Process)

Description:

No threats listed.

Fraud Detection (Process)

Description:

No threats listed.

Message In (JSON) (Data Flow)

Description:

No threats listed.

XML/HTTPS (Data Flow)

Description:

No threats listed.

XML/HTTPS (Data Flow)

Description:

No threats listed.

Response (Data Flow)

Description:

No threats listed.

Response (Data Flow)

Description:

No threats listed.

DD Transaction (Process)

Description:

No threats listed.

XML/HTTPS (Data Flow)

Description:

No threats listed.

CC Transaction (Process)

Description:

No threats listed.

Online Transaction (Data Flow)

Description:

No threats listed.

SFTP/EOD (Data Flow)

Description:

No threats listed.

Browser Access (External Actor)

Description:

Out-of-Data Web Browser cause arbility code execution (ACE)

Repudiation, Open, Medium Severity

Description:
Old web browser and never update may cause many vulnerability for allow attacker run "arbitrary code execution" on target machine. This will bring client to repudiation for access system and increase risk for system security

Mitigation:

Unclassified web browser access to system

Repudiation, Open, Medium Severity

Description:
Many web browser will bring problem for control security standard and a lot of them is discontinoute support from product owner (Such as Internet Explorer etc). This may cause mitigated client with know vulnerability for access system (A9: Know Vulnerability)

Mitigation:

Sensitive data classification

Information disclosure, Open, Medium Severity

Description:
Any data leave on browser/cookie need to classified and prevent sensitive data (A3:Sensitive Data Explosure)

Mitigation: