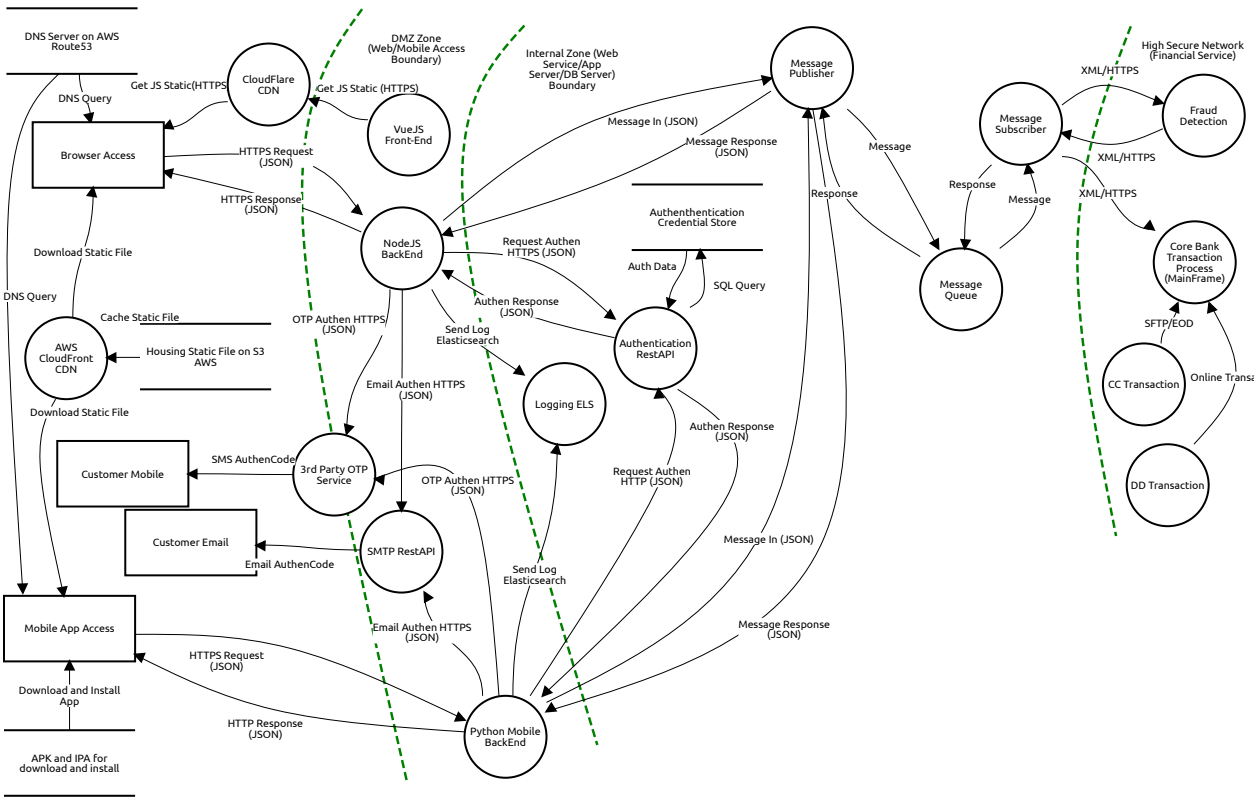
Threat model report for Online Banking Transaction

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)

Activated Desktop Report Controller

Possibly target of DDOS on single target

Denial of service, Mitigated, Medium Severity

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

Mitigation:
Enhance solution with "CloudFlare CDN" for distributed cache around 115 edge location

Get JS Static(HTTPS) (Data Flow)

Description:

No threats listed.

NodeJS BackEnd (Process)

Description:

Vulnerability assessment for RestAPI

Elevation of privilege, Mitigated, 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:
Design VA scan on pipeline

Penetration testing for RestAPI

Tampering, Mitigated, Medium Severity

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

Mitigation:
Add penetration test on pipeline

Lack of Module Log and Monitoring

Tampering, Mitigated, 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:
Enhance design for logging module

Validation for deserialize data from web browser

Elevation of privilege, Mitigated, High Severity

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

Mitigation:
Add on requirement of sprint

Mobile App Access (External Actor)

Description:
-Android (Version 9.1.0 and Upper)
-IOS (Version 13.1.0 and Upper)

Out-of-date mobile device's version cause vulnerability on OS

Repudiation, Mitigated, 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Android and IOS with out-of-date version will bring huge of "know vulnerability" and make device infected (A9: Know Vulnerability)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:
Specific Mobile Version for Install App
-Android (Version 9.1.0 and Upper)
-IOS (Version 13.1.0 and Upper)

Sensitive data classification

Information disclosure, Mitigated, Medium Severity

Description:

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

Mitigation:
No data store on mobile side

APK and IPA for download and install (Data Store)

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

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, Mitigated, 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:
Design VA scan on pipeline

Penetration testing for RestAPI

Tampering, Mitigated, Medium Severity

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

Mitigation:
Add penetration test on pipeline

Lack of Module Log and Monitoring

Tampering, Mitigated, 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:
Enhance design for logging module

Validation for deserialize data from mobile

Elevation of privilege, Mitigated, High Severity

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

Mitigation:
Add on requirement of sprint

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 AWS Route53 (Data Store)

Description:
Distr

DNS Cache Poisoning

Spoofing, Mitigated, 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:
Turnon Feature "DNSSEC" for ensure dns record via tls

DNS Attack for Denied of Service

Denial of service, Mitigated, 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:
Move dns to AWS route 53 for distributed dns service around region of aws site

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, Mitigated, 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:
Enhance 2Factor authentication with Email/OTP

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) Activated Desktop Report Controller

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, Mitigated, 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:
Front-end will check version of web browser compatibility
- Chrome (Version 81 and upper)
- MS Edge Chrome (Version 83.0.478.45 and upper)
- Firefox (Version 76.0 and upper)
- Safari (Version 13.0 and upper)

Unclassified web browser access to system

Repudiation, Mitigated, 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:
Front-End will allow only
- Chrome
- MS Edge Chrome
- Firefox
- Safari

Sensitive data classification

Information disclosure, Mitigated, Medium Severity

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

Mitigation:
No data store on browser side (use session only)

3rd Party OTP Service (Process)

Description:

No threats listed.

Customer Mobile (External Actor)

Description:

No threats listed.

SMTP RestAPI (Process)

Description:

No threats listed.

Housing Static File on S3 AWS (Data Store)

Description:

No threats listed.

SMS AuthenCode (Data Flow)

Description:

No threats listed.

OTP Authen HTTPS (JSON) (Data Flow)

Description:

No threats listed.

Customer Email (External Actor)

Description:

No threats listed.

Email AuthenCode (Data Flow)

Description:

No threats listed.

Email Authen HTTPS (JSON) (Data Flow)

Description:

No threats listed.

Email Authen HTTPS (JSON) (Data Flow)

Description:

No threats listed.

CloudFlare CDN (Process)

Description:
Take advantage of CDN from cloud flare with more than 115 edge location for static cache

No threats listed.

Get JS Static (HTTPS) (Data Flow)

Description:

No threats listed.

AWS CloudFront CDN (Process)

Description:
Placement all picture/video

No threats listed.

Cache Static File (Data Flow)

Description:

No threats listed.

Download Static File (Data Flow)

Description:

No threats listed.

Download Static File (Data Flow)

Description:

No threats listed.

Logging ELS (Process)

Description:

No threats listed.

Send Log Elasticsearch (Data Flow)

Description:

No threats listed.

Send Log Elasticsearch (Data Flow)

Description:

No threats listed.

OTP Authen HTTPS (JSON) (Data Flow)

Description:

No threats listed.