Making Malaysian Cashless Transactions Secure

Application: Mobile e-Wallet Platform

Service Offered: Security Testing

Tools: Application Penetration Testing Tool | Burp Suite, Vega, ZAP, IronWASP, Kali Linux, etc. | OWASP ZAP

Key Highlights

Domain: Fin Tech

QA Team:
The team comprised of Certified Ethical Hackers, Remediation Experts with an average team experience of 6+ years.

Duration: 1 month for the first rollout | Subsequent engagement for ongoing feature development and release

Client

Our client is a leading e-wallet provider in Malaysia. They have been in this business for more than a decade helping local businesses and consumers conduct cashless online transaction.

Application Overview

World over, people are transitioning to a cashless economy and have a variety of payment modes to choose from - be it through a physical point-of-sale (POS), or mobile e-commerce payments through an app or web browser. A Statist study suggests that by 2019, worldwide mobile payments will surpass $1 trillion dollars. According to one report by Zion Market Research, the global mobile wallet market share is expected to grow from $594.00 billion in 2016 to approximately $3,142.17 billion by 2022, growing at a CAGR of around 32 per cent from 2017 to 2022.

The Risks

However, this growth is fraught with frauds and risks. An Accenture survey reveals that cybercrime is 23 percent higher than last year, costing organizations, on an average, US$11.7 million.

Successful breaches have increased by more than 27 percent, from an average of 102 to 130, of which Ransomeware attacks alone have doubled in frequency, from 13 percent to 27 percent.

The six layers of security threats that such financial service providers need to protect themselves against include:

- Network
- Application
- Data
- Human
- Physical

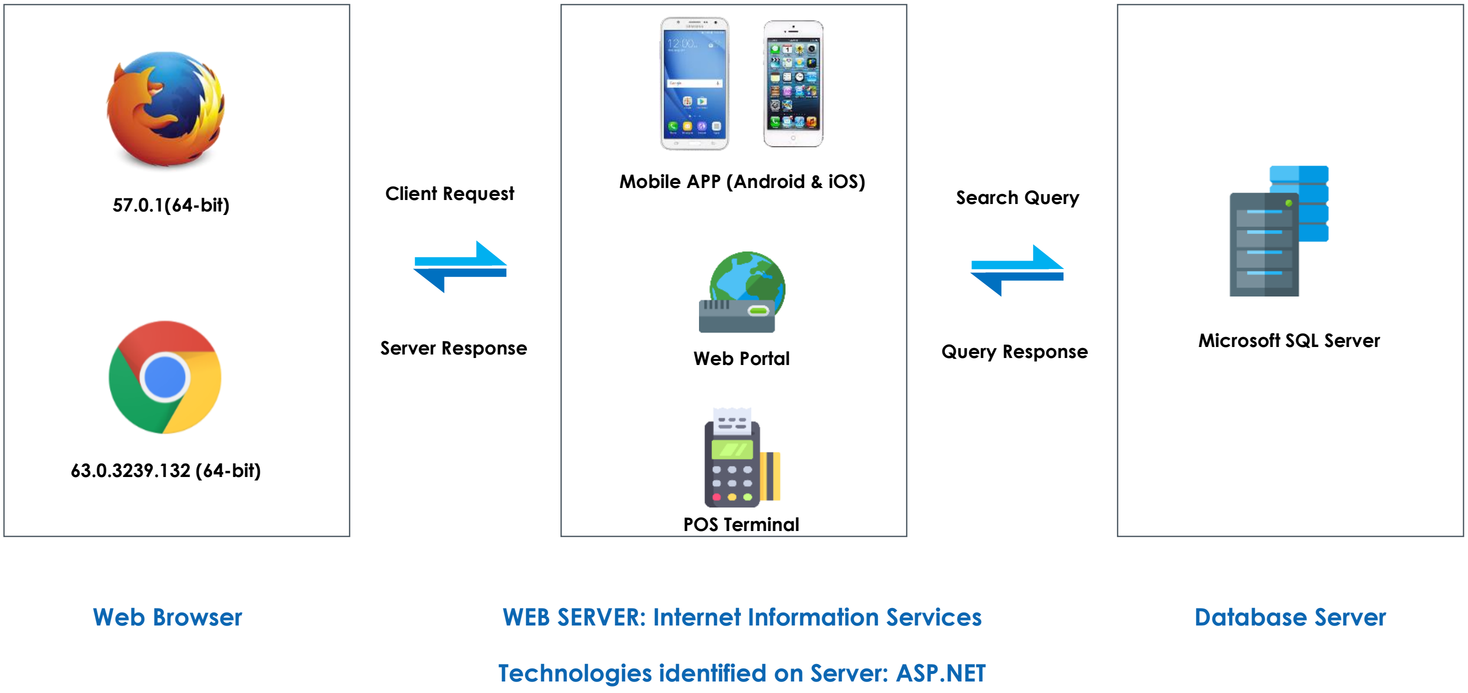
Our Approach

The Indium Security Testing Practice evaluates data and integrity and ensures confidentiality, authenticity and continuity while assessing vulnerabilities across the six layers.

Our comprehensive security testing framework (iAVA) validates all layers of an application, exposing vulnerabilities and security anomalies, to ensure:

- Confidentiality
- Data Integrity
- Authentication
- Authorization
- Availability
- Non-repudiation

Client - Server Architecture



Indium has domain as well as technical experience that made it a suitable partner to meet the client's requirements. Indium had also earlier worked with the client on another project, proving its credibility and capability.

Additionally, Indium validation framework conforms to OWASP Top 10, which helps testers build their own testing programs and lists the latest security breaches to watch out for.

Indium also helps financial institutions prepare for PCI compliance. Though it cannot certify an app as PCI compliant, it has the testing capability, we prepare our clients for first-pass certification.

The Indium Solution

Indium undertook security testing on Android, iOS, the POS device as well as Windows covering the following seven threats to the payment app:

- Malicious code attack
- Malware
- Denial of services
- Phishing
- Ransomware
- Web based attacks

Indium Advantage

While Indium uses all the right tools for security testing, they alone cannot produce insights into the gravity and relevance of a problem. Therefore, we also supplemented it with manually test, using:

- Python Basic level Scripting
- Burp Suite (Trial Version)

The proprietary Python scripts we used to find hidden:

- Form field / page / links but was not able to find the hidden form field since it is been protected from the source code.
- To find banner grabbing. We were able to run the script and find the server version (information leakage).
- For SQL detection and was unable to run the script

Breach of Security or not,
Our Security Testing Services are a must
Click Here

Impact

The security vulnerabilities found by Indium were,

For Web - Vulnerabilities in broken authentication and session management, sensitive data exposure and cross-site request forgery

For Mobile - Insecure data storage, insecure authentication and insecure authorization.

This helped the developers fix the bugs and roll out a secure app and procure the PCI certification. Indium also provided remediation measures to prevent security threats in the future.

Ongoing Requirement

As new features gets added, as the technology evolves, the threats too get compounded. OWASP periodically updates the list of threats and Indium keeps abreast of these developments. This enables Indium to work closely with developers to constantly strengthen their products and apps against security threats release after release, on an ongoing basis.