OWASP
Open Web Application
Security Project

API Security

Wong Onn Chee
OWASP Singapore Chapter Lead

OWASP : Core Mission

- The Open Web Application Security Project (OWASP) is a 501c3 not-for-profit also registered in Europe as a worldwide charitable organization focused on improving the security of software.

- Our mission is to make application security visible, so that people and organizations can make informed decisions about true application security risks.

- Everyone is welcomed to participate in OWASP and all of our materials are available under free and open software licenses.

Agenda

- OWASP API security artefacts
- Case study of how API was exploited to gain access to personal data
- Major security requirements in Singapore Personal Data Protection Act

OWASP API Security Artefacts

- OWASP API Security Top 10 2019 (https://owasp.org/www-project-api-security/)
- OWASP Enterprise Security API (ESAPI) (https://owasp.org/www-project-enterprise-security-api/)

OWASP API Security Top 10 2019

API1:2019 Broken Object Level Authorization	**API6:2019** Mass Assignment
API2:2019 Broken User Authentication	**API7:2019** Security Misconfiguration
API3:2019 Excessive Data Exposure	**API8:2019** Injection
API4:2019 Lack of Resources & Rate Limiting	**API9:2019** Improper Assets Management
API5:2019 Broken Function Level Authorization	**API10:2019** Insufficient Logging & Monitoring

OWASP ESAPI

- ESAPI (The OWASP Enterprise Security API) is
  - a free, open source, web application security control library that consists of a set of security control interfaces.
  - makes it easier for programmers to write lower-risk applications
  - currently available for Java

Case Study: A leading ecommerce player X

- Uses enterprise Github for development and a leading cloud service provider Y for production environment.

- For rapid CI/CD, chef (https://www.chef.io/products/chef-automate) and hubot (https://hubot.github.com/) were used.

- However, 2FA was not enforced on their enterprise Github account and neither was geographical restriction imposed.

- Threat actor(s) originating from Europe probably used credential stuffing to gain access to X's enterprise Github account private repos. X does not have any offices in Europe.

Case Study: A leading ecommerce player X

- Unprotected Chef API key was inadvertently checked in their private Github repo but was discovered and removed promptly. The Chef API key was supposed to be obsoleted due to the exposure. A new Chef API key was generated but the exposed Chef API key was inadvertently not removed.

- With access to their private Github repos, the threat actor(s) cloned all the private Github repos and managed to recover the removed Chef API key from the commit history of one of their private Github repo.

- With the stolen Chef key, the threat actor(s) from Europe accessed X's production cloud environment hosted in Y.

- Hubot API key was discovered from a private storage location hosted in Y.

Case Study: A leading ecommerce player X

- With the stolen Hubot key, the threat actor(s) managed to spawn new virtual machines, new firewall rules and exfiltrate personal data from within X’s production environment.

Case Study: A leading ecommerce player X

- So what went wrong?
  - **API4:2019** Lack of Resources & Rate Limiting

    Limiting the Github, Chef and Hubot access to legitimate geographical regions can limit the exposure surface.

  - **API9:2019** Improper Assets Management

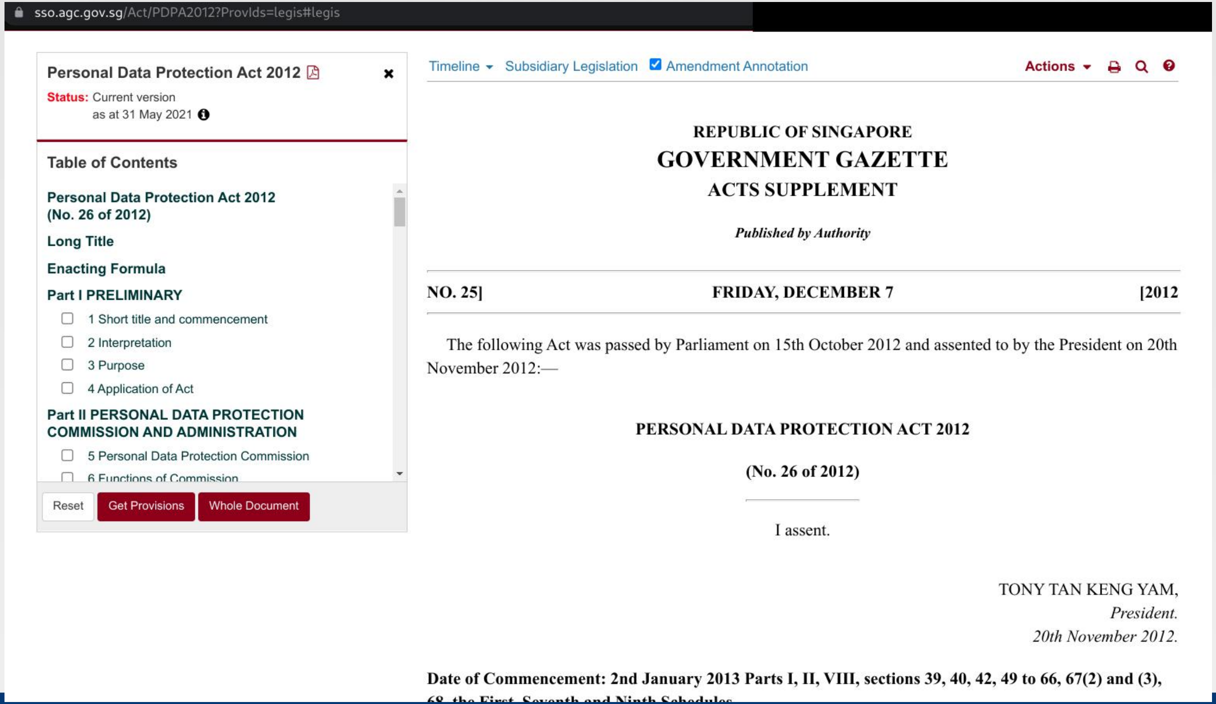
    Improper key management, e.g. leaving behind exposed, deprecated API keys, contributed to the exposed keys being exploited to steal personal data.

Case Study: A leading ecommerce player X

- So what went wrong?
  - **API10:2019** Insufficient Logging & Monitoring

  Absence of logging resulted in X not knowing rogue access, via stolen API keys, to their production cloud environment in Y.

Singapore Personal Data Protection Act (2012) (Amended on Feb 2021)



Personal Data Protection Act 2012

Status: Current version as at 31 May 2021

Table of Contents

REPUBLIC OF SINGAPORE
GOVERNMENT GAZETTE
ACTS SUPPLEMENT

Published by Authority

NO. 25] FRIDAY, DECEMBER 7 [2012

The following Act was passed by Parliament on 15th October 2012 and assented to by the President on 20th November 2012:—

PERSONAL DATA PROTECTION ACT 2012

(No. 26 of 2012)

I assent.

TONY TAN KENG YAM,
President.
20th November 2012.

Date of Commencement: 2nd January 2013 Parts I, II, VIII, sections 39, 40, 42, 49 to 66, 67(2) and (3), 68, the First, Seventh and Ninth Schedules

Source: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=legis#legis

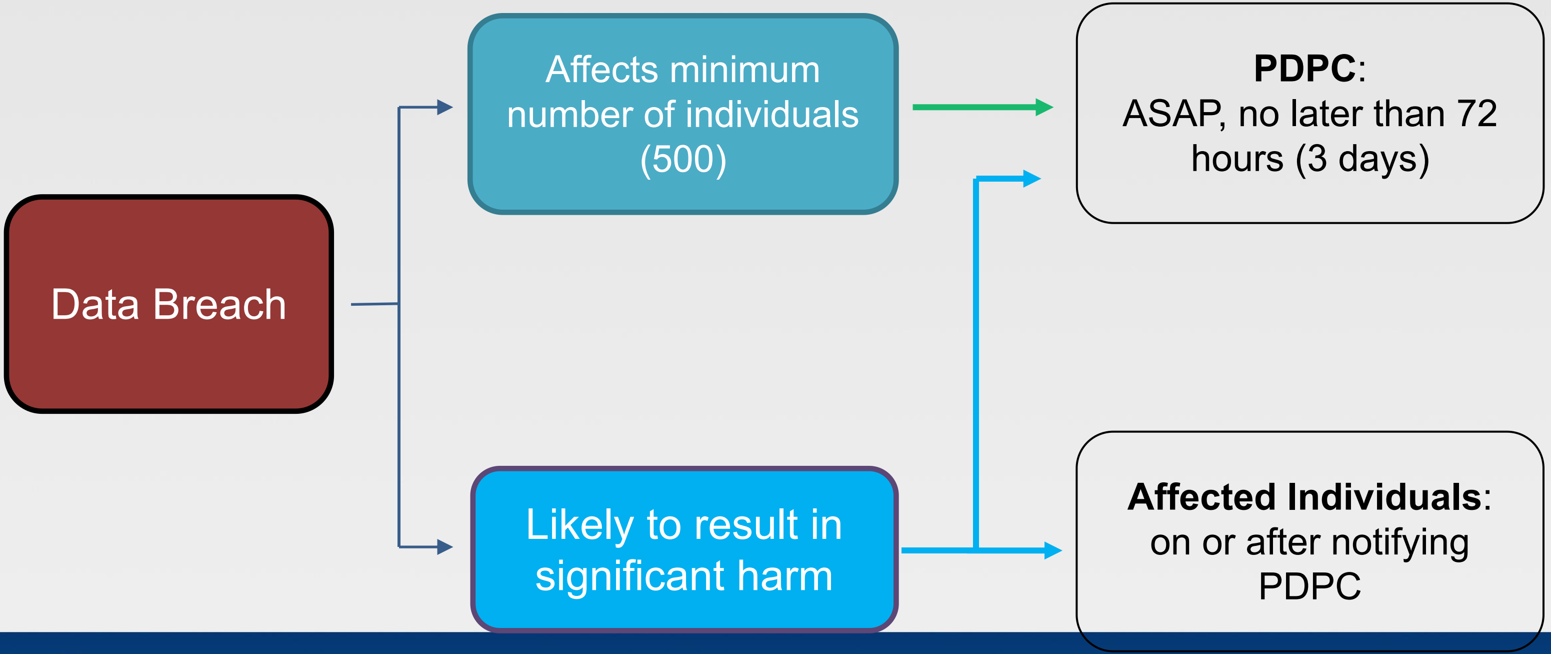
Mandatory Data Breach Requirements

Mandatory Breach Notification (s.26A to E)

- Previously, notifying the PDPC and affected individuals of data breaches was encouraged but not required
- Amendments introduce **mandatory** legal obligation to notify PDPC and/or affected individuals, depending on the **harm/scale** of the breach

But no specific penalties stated for breach of notification requirements. Therefore, general penalties (S$10k fine, 3 yrs jail or both) apply.

Mandatory Data Breach Requirements



Criteria to be met

Timeframe for notifying

Data Breach

Affects minimum number of individuals (500)

Likely to result in significant harm

PDPC:
ASAP, no later than 72 hours (3 days)

Affected Individuals:
on or after notifying PDPC

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

Storage Encryption is no longer an acceptable defence

Surprise! Encryption does not prevent loss of storage medium or device.

"Protection Obligation" (s.24)

An organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent –

(a) *unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; or*

(b) the loss of any storage medium or device on which personal data is stored.

Unauthorised disclosure of personal data

Unauthorised Disclosure of PD (s.48D)

(a) *If an individual discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person;*

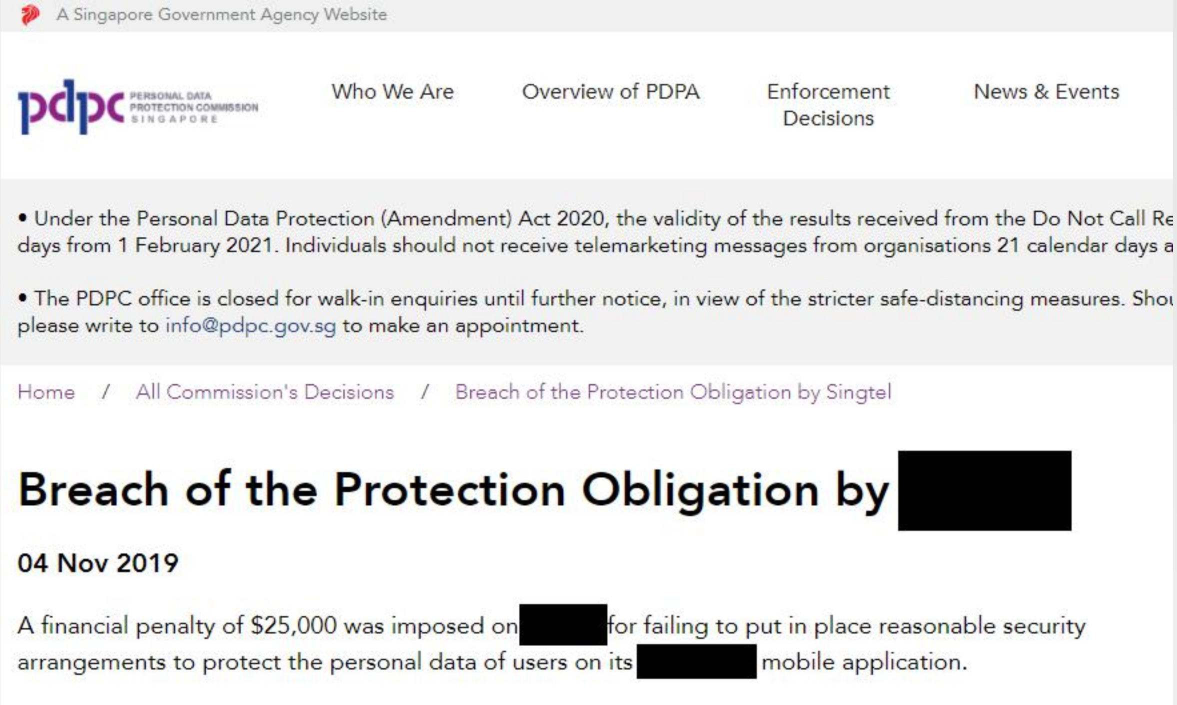
(b) *the disclosure is not authorised by the organisation or public agency; and*

(c) *the individual does so –*

(i) ***knowing*** *that the disclosure is not authorised by the organisation or public agency; or*

(ii) ***reckless*** *as to whether the disclosure is or is not authorised by the organisation or public agency.*

Actual enforcement case by SG PDPC – S$25k fine and reputation damage



A Singapore Government Agency Website

- Under the Personal Data Protection (Amendment) Act 2020, the validity of the results received from the Do Not Call Re days from 1 February 2021. Individuals should not receive telemarketing messages from organisations 21 calendar days a

- The PDPC office is closed for walk-in enquiries until further notice, in view of the stricter safe-distancing measures. Shou please write to info@pdpc.gov.sg to make an appointment.

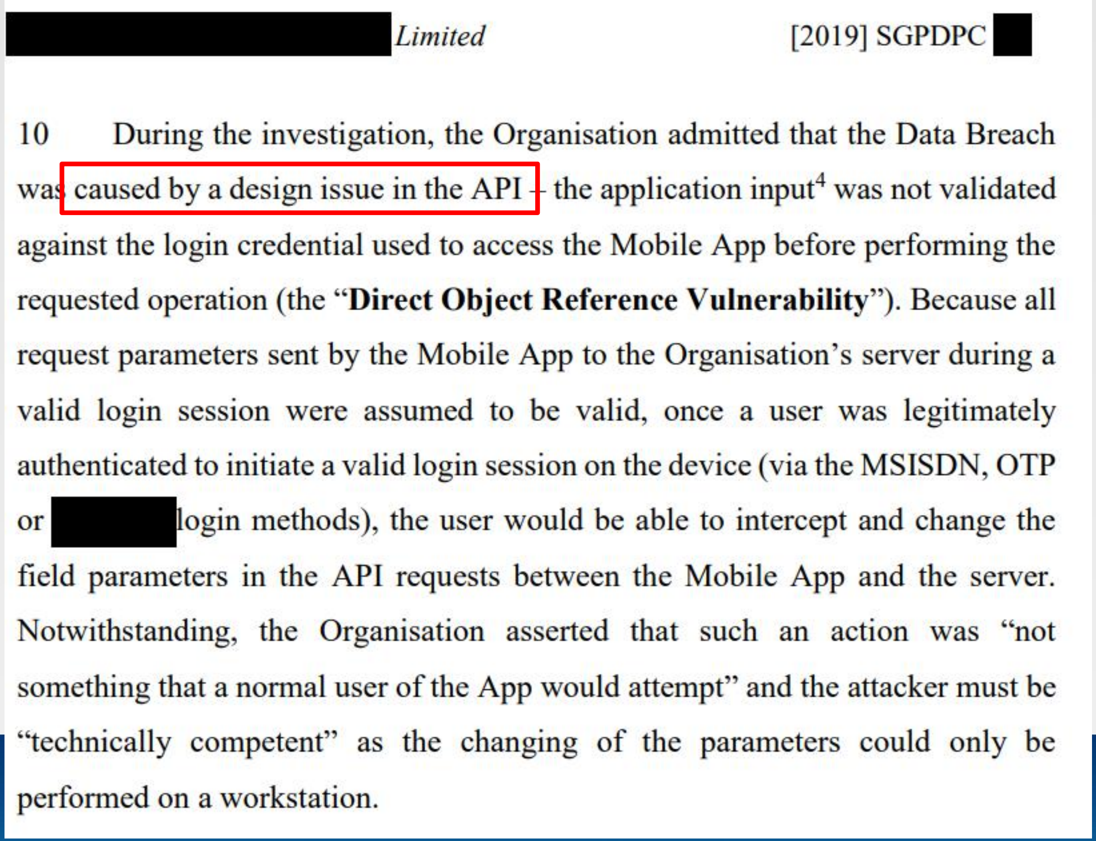
Home / All Commission's Decisions / Breach of the Protection Obligation by Singtel

Breach of the Protection Obligation by [redacted]

04 Nov 2019

A financial penalty of $25,000 was imposed on [redacted] for failing to put in place reasonable security arrangements to protect the personal data of users on its [redacted] mobile application.

Actual enforcement case by SG PDPC – Insecure API design



[redacted] *Limited* [2019] SGPDPC [redacted]

10 During the investigation, the Organisation admitted that the Data Breach was caused by a design issue in the API – the application input[4] was not validated against the login credential used to access the Mobile App before performing the requested operation (the "**Direct Object Reference Vulnerability**"). Because all request parameters sent by the Mobile App to the Organisation's server during a valid login session were assumed to be valid, once a user was legitimately authenticated to initiate a valid login session on the device (via the MSISDN, OTP or [redacted] login methods), the user would be able to intercept and change the field parameters in the API requests between the Mobile App and the server. Notwithstanding, the Organisation asserted that such an action was "not something that a normal user of the App would attempt" and the attacker must be "technically competent" as the changing of the parameters could only be performed on a workstation.

API Security

Thank you for your attention.