



# OWASP

Open Web Application  
Security Project

# API 安全

Wong Onn Chee  
OWASP Singapore Chapter Lead

# OWASP：核心使命

- 开放 Web 应用程序安全项目 (OWASP) 是一个 501c3 非营利组织，也在欧洲注册为专注于提高软件安全性的全球慈善组织。
- 我们的使命是使应用程序安全可视化，以便人员和组织能够就真正的应用程序安全风险做出明智的决定。
- OWASP 欢迎所有参与，且我们所有的资料均可透过免费和开放的软件许可证获得。

# 议程

- OWASP API 安全工作件
- 如何滥用 API 获取个人数据的案例研究
- 新加坡个人资料保护法的主要安全要求

# OWASP API 安全工作

- 2019 年 OWASP API 安全 10 大漏洞 (<https://owasp.org/www-project-api-security/>)
- OWASP 企业安全 API (ESAPI) (<https://owasp.org/www-project-enterprise-security-api/>)

# 2019 年 OWASP API 安全 10 大漏洞

|                                |                             |
|--------------------------------|-----------------------------|
|                                |                             |
| <b>API1 : 2019 遭到破坏的对象级授权</b>  | <b>API6 : 2019 大规模分配</b>    |
| <b>API2 : 2019 遭到破坏的用户身份验证</b> | <b>API7 : 2019 安全配置错误</b>   |
| <b>API3 : 2019 数据暴露过多</b>      | <b>API8 : 2019 注入</b>       |
| <b>API4 : 2019 缺乏资源和速率限制</b>   | <b>API9 : 2019 不当的资产管理</b>  |
| <b>API5 : 2019 遭到破坏的功能级授权</b>  | <b>API10 : 2019 记录和监控不足</b> |

# OWASP ESAPI

- ESAPI (OWASP 企业安全 API)
  - 是一个免费的、开源的、Web 应用程序安全控制库，由一组安全控制接口组成。
  - 使开发者更容易编写风险较低的应用程序。
  - 目前可用于 Java。

# 案例研究：行业领先的电子商务业者 X

- 其开发环境使用企业 Github，而生产环境使用行业领先的云服务提供商 Y。
- 对于快速 CI/CD，其使用 Chef (<https://www.chef.io/products/chef-automate>) 及 Hubot (<https://hubot.github.com/>)。
- 但是，2FA 并未应用于企业 Github 帐户，并且没有设置地域限制。
- 来自欧洲的攻击者可能使用撞库来访问 X 的企业 Github 帐户私人存储库。X 业者在欧洲没有任何办事处。

# 案例研究：行业领先的电子商务业者 X

- 未受保护的 Chef API 密钥无意中检查了他们的私人 Github 存储库，但被及时发现并删除。Chef API 密钥由于暴露而应废弃。一个新的 Chef API 密钥产生，但无意间却未删除已暴露的 Chef API 密钥。
- 通过访问其私有的 Github 存储库，攻击者复制了所有私有 Github 存储库，并设法从其私有 Github 存储库之一的提交历史记录中恢复了已删除的 Chef API 密钥。
- 使用窃取的 Chef 密钥，来自欧洲的攻击者访问了 X 业者在 Y 提供商中托管的生产云环境。
- Hubot API 密钥是从 Y 提供商托管的私有存储位置发现的。

# 案例研究：行业领先的电子商务业者 X

- 攻击者使用被盗的 Hubot 密钥设法生成新的虚拟机、新的防火墙规则并从 X 业者的生产环境中窃取个人数据。

# 案例研究：行业领先的电子商务业者 X

- 什么地方出了错？

- API4 : 2019 缺乏资源和速率限制

透过限制 Github、Chef 和 Hubot 对合法地理区域的访问权限可以限制暴露面。

- API9 : 2019 不当的资产管理

密钥管理不当，例如留下暴露的、弃用的 API 密钥，导致暴露的密钥被利用来窃取个人数据。

# 案例研究：行业领先的电子商务业者 X

- 什么地方出了错？
  - API10 : 2019 记录和监控不足

没有日志记录导致 X 业者对于攻击者透过窃取的 API 密钥对其在 Y 提供商的生产云环境进行恶意访问的行为一无所知。

# 新加坡個人資料保護法（2012） (2021年2月修订)

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

Personal Data Protection Act 2012 

Status: Current version  
as at 31 May 2021 

Table of Contents

Personal Data Protection Act 2012 (No. 26 of 2012)

Long Title

Enacting Formula

Part I PRELIMINARY

- 1 Short title and commencement
- 2 Interpretation
- 3 Purpose
- 4 Application of Act

Part II PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION

- 5 Personal Data Protection Commission
- 6 Functions of Commission

Reset  Get Provisions  Whole Document 

Timeline  Subsidiary Legislation  Amendment Annotation

Actions    

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.

来源：

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

# 强制性数据泄露要求

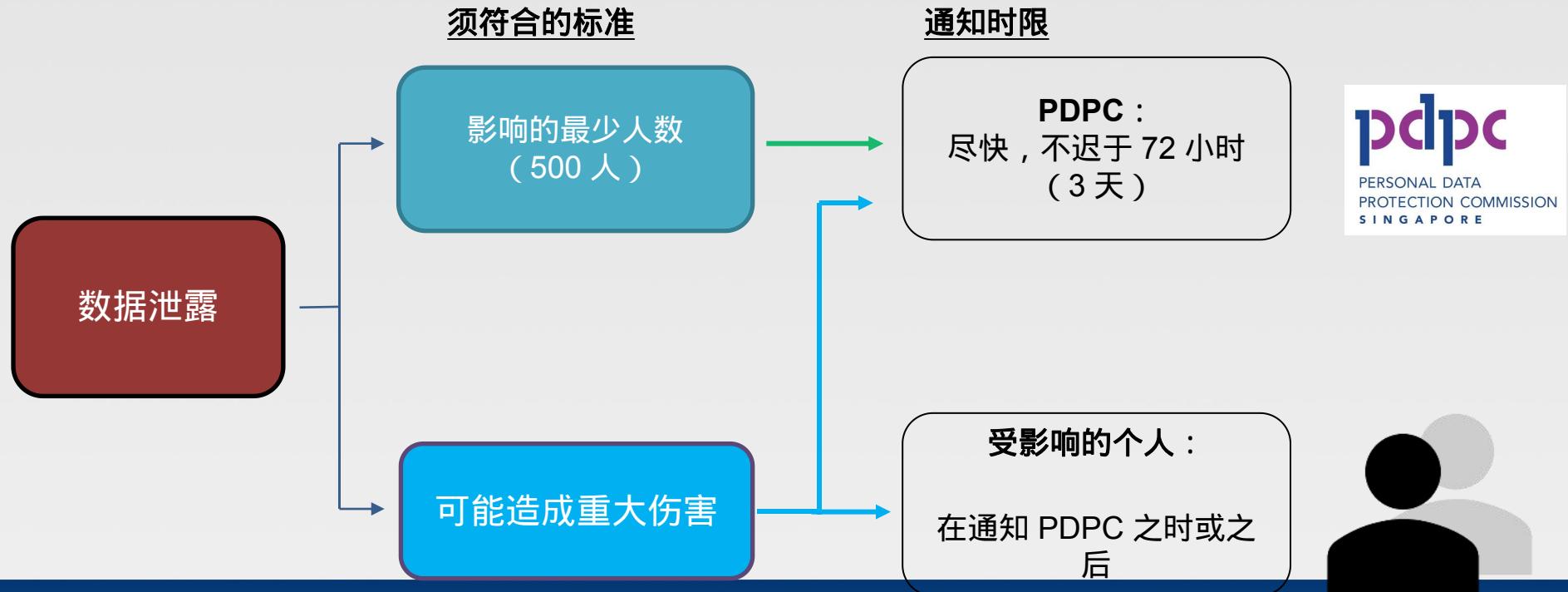
## 强制性数据泄露通知（第 26A 至 E 条）

- 以前，建议但不强制性地要求将数据泄露通知 PDPC 和受影响的个人。
- 修正案**强制**要求根据数据泄露的**损害和规模**通知 PDPC 和/或受影响的个人。



但没有规定对违反通知要求的具体处罚。因此，适用一般处罚（1 万新币罚款、3 年监禁或两者兼施）。

# 强制性数据泄露要求



# 存储加密不再是可接受的防御

## “保护义务”（第 24 节）

组织必须通过采取适当的安全措施来保护其拥有或控制的个人信息，以防止：

- (a) 未经授权的访问、收集、使用、披露、复制、修改或处置或类似风险；或者
- (b) 存储个人数据的任何存储媒介或设备的丢失。



令人惊讶的是，加密并不能防止存储媒介或设备的丢失。

# 未经授权披露个人资料

## 未经授权披露个人资料（第 48D 条）

- (a) 如果个人向他人披露或个人的行为导致向他人披露组织或公共机构拥有或控制的个人数据；
- (b) 披露未经该组织或公共机构授权；
- (c) 个人的行为是在
  - (i) 知道披露未经组织或公共机构授权的情况下；或
  - (ii) 对披露是否受组织或公共机构授权毫不在意。



# SG PDPC 的实际执法案例 — 2.5 万新币罚款和声誉损害



A Singapore Government Agency Website



Who We Are

Overview of PDPA

Enforcement  
Decisions

News & Events

- Under the Personal Data Protection (Amendment) Act 2020, the validity of the results received from the Do Not Call Registry ends on 1 February 2021. Individuals should not receive telemarketing messages from organisations 21 calendar days after this date.
- The PDPC office is closed for walk-in enquiries until further notice, in view of the stricter safe-distancing measures. Should you require assistance, please write to [info@pdpc.gov.sg](mailto: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.

# SG PDPC 的实际执法案例 — 不安全的 API 设计

Limited

[2019] Limited

[2019] SGPDPC

10 During the investigation, the Organisation admitted that it was caused by a design issue in the API – the application input<sup>4</sup> was against the login credential used to access the Mobile App before requested operation (the “**Direct Object Reference Vulnerability**”). request parameters sent by the Mobile App to the Organisation’s valid login session were assumed to be valid, once a user was authenticated to initiate a valid login session on the device (via the or [REDACTED] login methods), the user would be able to intercept field parameters in the API requests between the Mobile App. Notwithstanding, the Organisation asserted that such an action was something that a normal user of the App would attempt” and the “technically competent” as the changing of the parameters performed on a workstation.

10 在调查期间，该组织承认数据泄露是由 API 中的一个设计问题引起——在执行请求的操作之前，应用程序输入没有根据用于访问移动应用程序的登录凭据进行验证（“直接对象引用漏洞”）。因为移动应用程序在有效登录会话期间发送到组织服务器的所有请求参数都被假定为有效，一旦用户经过合法身份验证以在设备上启动有效登录会话（通过 MSISDN、OTP 或 [REDACTED] 登录方法），用户将能够拦截和更改移动应用程序和服务器之间的 API 请求中的字段参数。尽管如此，该组织声称这样的行为“不是应用程序的普通用户会尝试的事情”，并且攻击者必须“技术上胜任”，因为参数的更改只能在工作站上执行。



# OWASP

Open Web Application  
Security Project

## API 安全

感谢您的关注。