



巨匠線上真人

# 資訊安全概論 與 網站軟體安全建構實務

[www.pcschoolonline.com.tw](http://www.pcschoolonline.com.tw)

## 同學，歡迎你參加本課程

- ☑ 請關閉你的FB、Line等溝通工具，以免影響你上課。
- ☑ 考量頻寬，請預設關閉麥克風、攝影機，若有需要再打開。
- ☑ 隨時準備好，老師會呼叫你的名字進行互動。
- ☑ 如果有緊急事情，你必需離開線上教室，請用聊天室私訊給老師，以免老師癡癡呼喚你的名字。
- ☑ 先倒好水、上個洗手間，準備上課囉^^

# 課程檔案下載

巨匠電腦線上真人

開課查詢 免費體驗專區 課程總覽 專業師資

學員專區 講師專區 最新消息

登入 360 f YouTube

您好! 登出

## 程式語言好難學?

那是因為  
你還沒學過Python!

(線上老師 **LIVE** 直播教學 · 搶先看)

點數卡產品兌換

APCS檢測專區

公告專區

我的課表

IT真人課程劃位

電腦分校課程劃位

外語真人課程劃位

美語分校課程劃位

取消劃位

**課程檔案下載**

上課權益查詢

教學平台測試

學習諮詢

常見問題

個資維護

忘記密碼

登出

### 課程檔案下載

巨匠電腦真人課程

# ZOOM 學員操作說明

The screenshot shows the Zoom interface with several callouts:

- 5 查看選項/共同註記/筆 (連連看)**: Points to the '查看選項' (View Options) dropdown menu, which includes '原始大小' (Original Size), '請求遠端控制' (Request Remote Control), '共同註記' (Annotate), and '退出全螢幕' (Exit Full Screen). The '共同註記' option is highlighted with an orange box.
- 筆**: Points to the '筆' (Pen) icon in the toolbar, which is also highlighted with an orange box.
- 2 共享螢幕 (指導演練；點評作品)**: Points to the '共享螢幕' (Share Screen) button in the bottom toolbar. The text below it says: '老師須先停止共享螢幕才能請學生共享螢幕' (The teacher must first stop sharing the screen before asking the student to share the screen).
- 1 聊天**: Points to the '聊天' (Chat) button in the bottom toolbar.
- 3 與會者/舉手**: Points to the '與會者' (Participants) button in the bottom toolbar, which has a small '1' next to it.
- 4 解除靜音**: Points to the '解除靜音' (Unmute) button in the bottom toolbar.

Other visible elements include the Zoom logo, the URL 'www.pcschool.com.tw', a green status bar at the top saying '您正在觀看綠世界的螢幕', and a list of participants on the left side of the screen.



巨匠線上真人

資訊安全概論與網站軟體安全建構實務

# 第四堂：Web API 安全性設計

# 本堂教學重點

1. Web API 設計概念
  2. API 資料傳輸 JSON 劫持
- ◆ 下堂教學重點

# 本堂教學重點

1. Web API 設計概念

2. API 資料傳輸 JSON 劫持

◆ 下堂教學重點

# 1. Web API 設計概念



# OPEN API

- ◆ 財金公司金融開放API平臺
  - ◆ 2019/10/16啟用
  - ◆ 第一批上架API銀行23家
  - ◆ 做為數位金融API的統一交換平台

# OPEN API

## 三、開放API架構



# OPEN API

## 三、開放API架構(續)



### 開放API技術標準設計準則

#### 共通性

參考國際Open API Initiative組織之**Open API Specification**(簡稱**OAS**)，作為**Open API**技術規格之一致性標準，並遵循OAS規範之RESTful APIs (programming language-agnostic interface)定義，使**API互通介面不受程式語言限定**。此技術規格也是國發會開放政府資料標準所使用的規格標準，有利於推廣以及未來跟其他產業或政府開放資料之介接。

<https://www.ithome.com.tw/news/131648>

參考國際標準，  
開發速度快，效率高!!!

# OPEN API

## 三、開放API架構(續)

### 開放API技術標準設計準則

#### 輕便性

- ✓ 採RESTful(Representational State Transfer)風格設計API：消耗資源少。
- ✓ 採JSON資料格式設計API：相容性高、格式容易瞭解、閱讀及修改方便、支援許多資料格式，提供易懂且有意義的路徑。
- ✓ 易操作解讀介面(EX：Swagger UI)及少量的實作邏輯，提供快速測試與遠端API服務互動，讓TSP業者易於了解API輸出入資料格式及內容。

<https://www.ithome.com.tw/news/131648>

簡短規格，  
易解讀訊息用途!!

本文內容由本公司之專業編譯，不得複製、散佈，如有違者將依法追究。

40

# OPEN API

## 三、開放API架構(續)



### 開放API各階段安控共通性需求 (符合網站安全檢測實務):

- ✓ 進行欄位格式檢查
  - 防範常見之網站資料竊取及執行非法程式碼攻擊
- ✓ 採用TLS 1.2(含)以上之通訊協定
  - 採合乎時宜之傳輸加密標準以防範資訊外洩
- ✓ 正面表列並限制僅接受所需之HTTP 請求方法
  - 限定通訊方式提升系統處理之效率
- ✓ 採取連線限制與逾時中斷等機制，以防範分散式阻斷服務
  - 防範常見網站服務分散式阻斷服務
- ✓ 使用HTTP強制安全傳輸(Http Strict Transport Security · HSTS)協議
  - 強制網站連線必須加密防範資訊外洩

<https://www.ithome.com.tw/news/131648>



# Web API

## ◆ REST

### ◆ REST (Representational State Transfer)

◆ 常見的 REST 實作會使用  
HTTP 作為應用程式通訊協定

◆ 符合 REST 原則的服務  
稱為 RESTful Service

GET /api/TodoItems

取得所有待辦事項

GET /api/TodoItems/{識別碼}

依識別碼取得項目

POST /api/TodoItems

新增記錄

PUT /api/TodoItems/{識別碼}

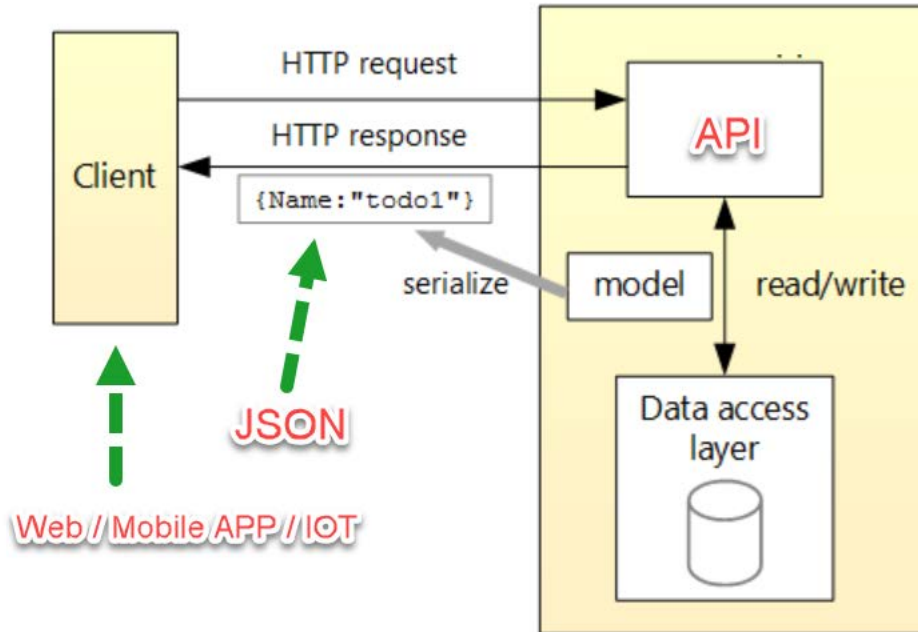
更新現有的項目

DELETE /api/TodoItems/{識別碼}

刪除項目

# Web API

## ◆ REST APIs with .NET (.NET Framework 4.5)



# Web API

## ◆ 設計原則

- ◆ 強制使用HTTPS
- ◆ 盡可能依REST採用正確的HTTP Method
- ◆ 呼叫來源的驗證及授權
- ◆ 錯誤訊息的回應內容請勿包含對 API 攻擊者可能有幫助的資訊
  - 例：401 (未經授權)，但不應出指是帳號錯誤或密碼錯誤



軟體操作示範：

**實作：Web API**

# CORS 簡介

- ◆ CORS(Cross-Origin Resource Sharing)
  - ◆ W3C 標準，讓伺服器放寬同源政策
  - ◆ 可以明確允許某些跨源要求
  - ◆ 同源政策保護瀏覽器安全性限制防止網頁程式對另一個網域提出呼叫請求
  - ◆ 防止惡意網站從另一個網站以程式碼方式發出請求，以取得敏感性資料

軟體操作示範：

# 實作：Web API CORS 設計

# 本堂教學重點

1. Web API 設計概念

2. API 資料傳輸 JSON 劫持

◆ 下堂教學重點

## 2. API 資料傳輸 JSON 劫持

# API 資料傳輸 JSON 劫持

## ◆ JSON劫持

◆ {"username":"lan","idno":"A123456789"}

◆ 攻擊者利用CSRF手段劫持到敏感信息

◆ JSON做為API主流交換資料的格式，在一般的API應用裡，若沒有針對請求來源做驗證，那麼json劫持就容易發生

◆ 防禦手法同CSRF

- 在請求中加入one time token，並且在伺服器端驗證

# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

小金下訂單

[http://www.myweb.com/order?](http://www.myweb.com/order?id=a0001&cnt=10)  
[id=a0001&cnt=10](http://www.myweb.com/order?id=a0001&cnt=10)

# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

### ◆ 簽章，sign

依雙方約定的密碼進行參數加密，  
做為簽章

abc999



# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

◆ 簽章，sign

加密(a0001+10+abc999) =  
440e9f668e41c1bb138acd4e233c2f  
c8

# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

<http://www.myweb.com/order?>  
[id=a0001&cnt=10&sign=440e9f668](#)  
[e41c1bb138acd4e233c2fc8](#)

# API 資料傳輸 JSON 劫持

- ◆ JSON 內容竄改防護
  - ◆ 伺服器端解密簽章值

解密

$$(440e9f668e41c1bb138acd4e233c2fc8) = a0001+10+abc999$$

# API 資料傳輸 JSON 劫持

◆ 請求時效防護

◆ 簽章sign加入時間戳

加密(a0001+10+abc999+2019/1/1  
13:15:33) =  
4f403a10b5041ad3ee80e0c8a37f0  
5db

# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

### ◆ 伺服器端解密簽章值

解密

(440e9f668e41c1bb138acd4e233c  
2fc8+ 2019/1/1 13:15:33) =  
a0001+10+abc999+

# API 資料傳輸 JSON 劫持

## ◆ JSON 內容竄改防護

◆ 請求時效超時 ( 例如設定超時值為20秒)

比對2019/1/1 13:15:33與目前時間  
>20秒，拒絕請求

軟體操作示範：

實作：簽章示範

# Q&A



# 下堂教學重點

- ◆ Web API 請求權限設計
- ◆ API 防範惡意請求的對策

# 問卷

<http://www.pcschoolonline.com.tw>

開課查詢 免費體驗專區 課程總覽 - 專業師 1 學員專區 - 講師專區

公告專區

我的課表

課程劃位

取消劃位

2 課程檔案下載

課程檔案下載：

學員的「上課教材」，下載檔案為壓縮檔 ([解壓縮操作步驟](#))。  
如無法觀看上課教材，請安裝 [PDF閱讀軟體](#)。

自107年1月1日起，課程錄影檔由180天改為365天(含)內無限次觀看 (上課隔日18:00起)。

上課日期	課程名稱	課程節次	教材下載	
2017/12/27 2000 ~ 2200	線上真人-ZBrush 3D動畫造型設計	18	上課教材	錄影檔 3 課堂問卷
2017/12/20 2000 ~ 2200	線上真人-ZBrush 3D動畫造型設計	17	上課教材	錄影檔
2017/12/18 2000 ~ 2200	線上真人-ZBrush 3D動畫造型設計	16	上課教材	錄影檔

問  
卷



巨匠線上真人

[www.pcschoolonline.com.tw](http://www.pcschoolonline.com.tw)