巨匠線上真人

資訊安全概論
與
網站軟體安全建構實務

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
您好!
登出
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
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
98%
54%
巨匠電腦真人課程

ZOOM 學員操作說明

5 查看選項/共同註記/筆（連連看）

2 共享螢幕（指導演練；點評作品）
老師須先停止共享螢幕
才能請學生共享螢幕

1 聊天

4 解除靜音

3 與會者/舉手

巨匠線上真人

資訊安全概論與網站軟體安全建構實務

第三堂：雲端網站安全性設計

本堂教學重點

1. 雲端檔案儲存體
2. 網站資料存取權限簽章設計

◆ 下堂教學重點

本堂教學重點

1. 雲端檔案儲存體
2. 網站資料存取權限簽章設計

◆ 下堂教學重點

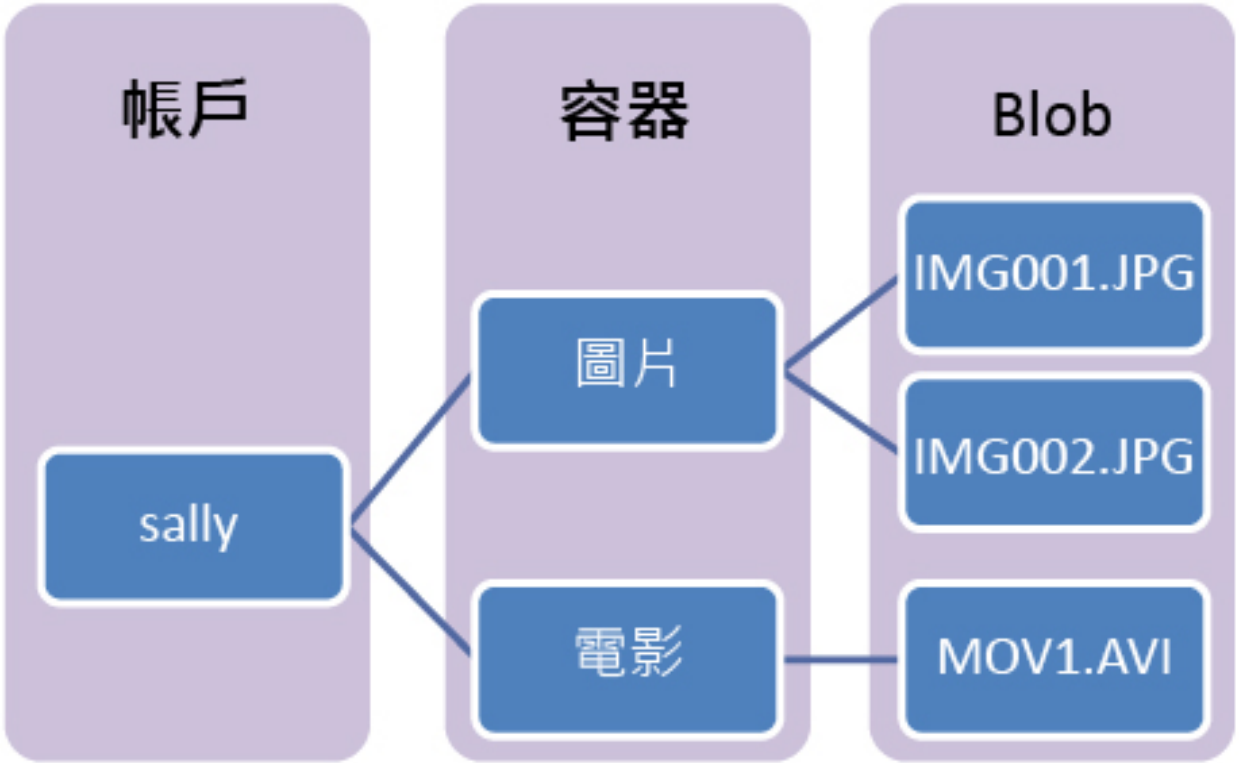
1.雲端檔案儲存體

雲端檔案儲存體

- Blob 儲存體
  - 儲存非結構化資料
  - 類似在電腦 (或平板電腦、行動裝置等) 裡儲存的檔案
  - 使用 URL、REST 介面、 Azure SDK 存取
  - 應用程式透過 HTTP/HTTPS 存取 Blob 儲存體中的物件
  - 進階儲存體使用 SSD 可得到最快的效能
- 應用情境
  - 直接提供檔案或文件輸出至瀏覽器
  - 儲存備份和還原、災害復原和封存資料
  - 串流傳輸視訊和音訊

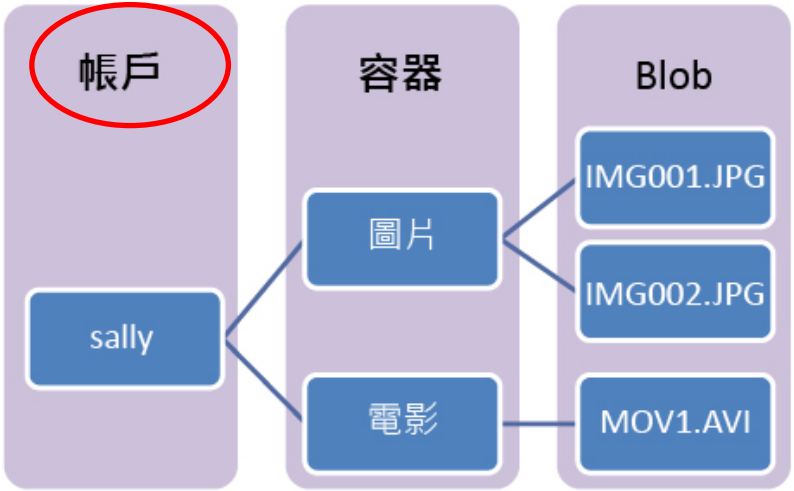
雲端檔案儲存體

- Blob 儲存體



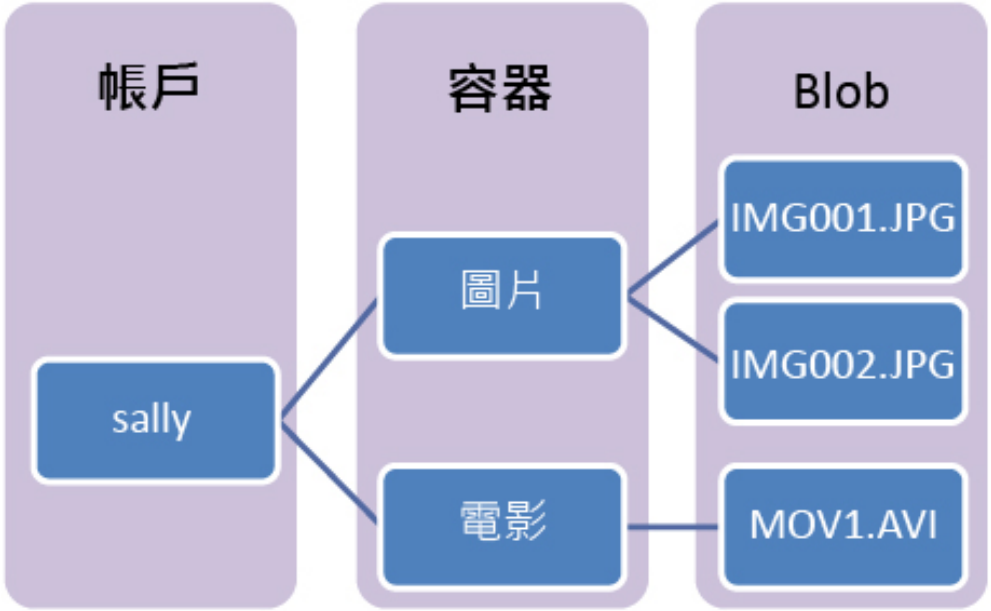
雲端檔案儲存體

- 儲存體帳戶
  - Azure 儲存體帳戶提供雲端中的唯一命名空間，用來儲存及存取 Azure 儲存體中的資料物件
  - 儲存體帳戶名稱必須介於 3 到 24 個字元的長度
  - 只能包含數字和小寫字母
  - 儲存體帳戶名稱必須在 Azure 中是獨一無二的



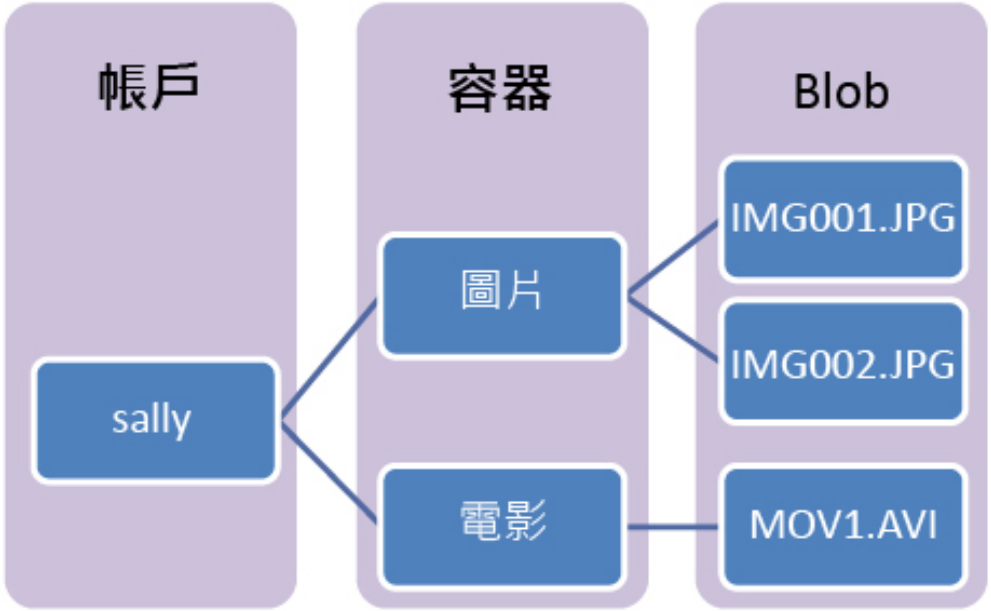
雲端檔案儲存體

- 容器
  - 類似於資料夾目錄
  - 所有 Blob 都必須放在容器中
  - 容器名稱必須是英數字小寫
  - 一個帳戶可以包含的容器不限數量
  - 容器可以儲存無限制的 Blob



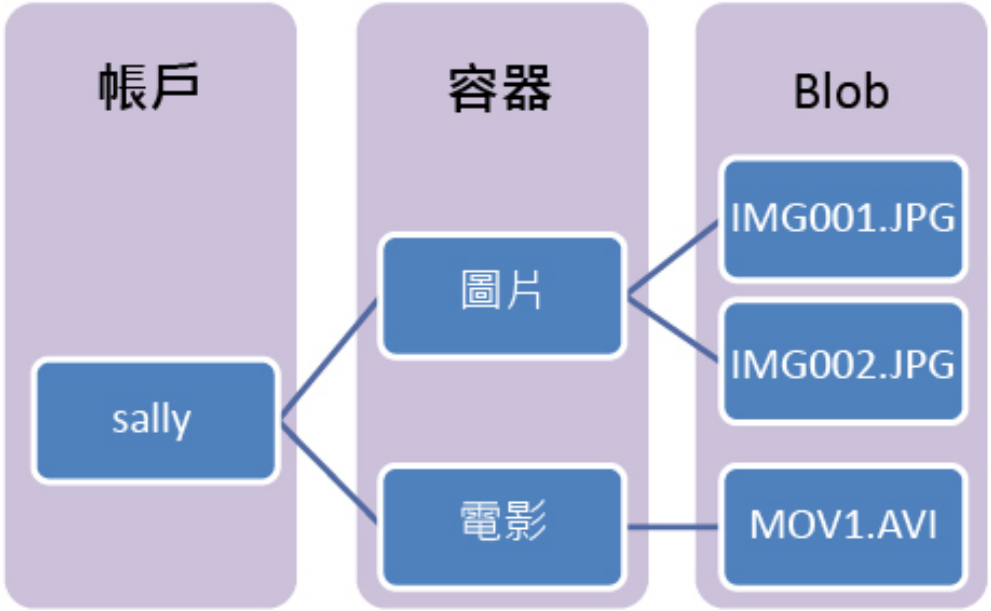
雲端檔案儲存體

- Blob
  - 任何類型和大小的檔案
  - 區塊 Blob
    - 每個區塊最大為 100 MB
    - 單一區塊 blob 可含 50,000 個區塊
    - 4.75 TB (100 MB X 50,000)
    - 資料儲存上是打散分割成不同資料區塊



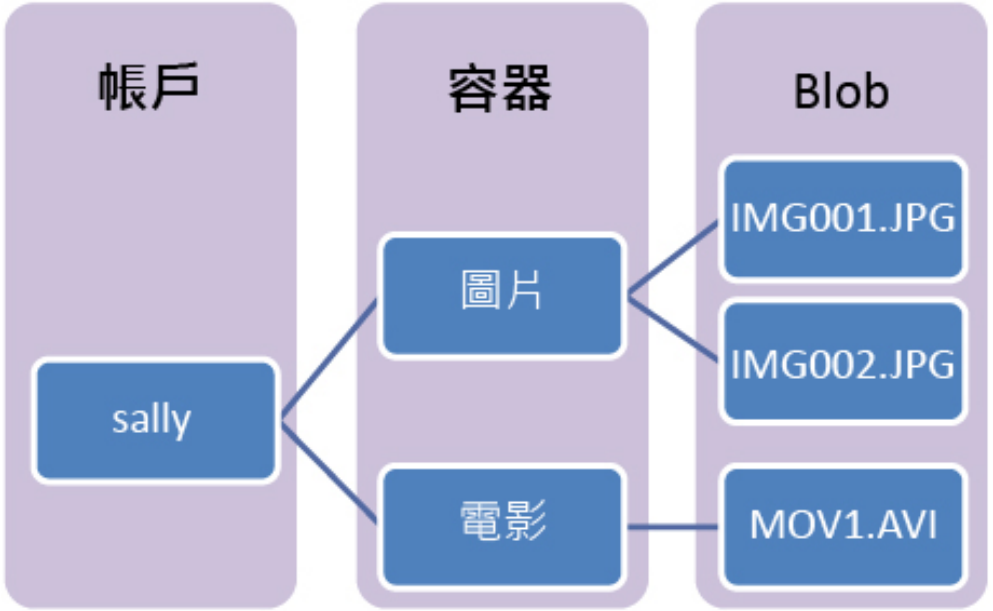
雲端檔案儲存體

- Blob
  - 附加 Blob
    - 區塊 Blob 相似，但針對附加作業最佳化
    - 單一區塊 blob 可含 50,000 個區塊
    - 每個區塊最大為 4 MB
    - 195 GB (4 MB X 50,000)
    - 資料儲存上是打散分割成不同資料區塊



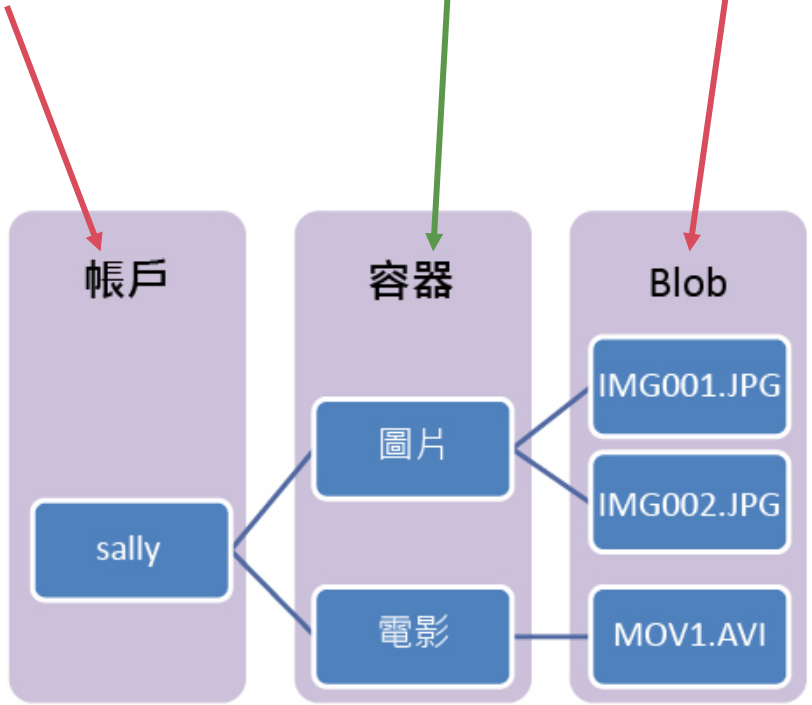
雲端檔案儲存體

- Blob
  - 分頁 Blob
    - 小可達 8 TB
    - 資料儲存上是連續性的
    - Azure 虛擬機器
      使用分頁 Blob 作為
      作業系統和資料磁碟。



雲端檔案儲存體

- https://pc532.blob.core.windows.net/media/903946-XXL.jpg



操作示範：

建立與管理儲存體帳戶

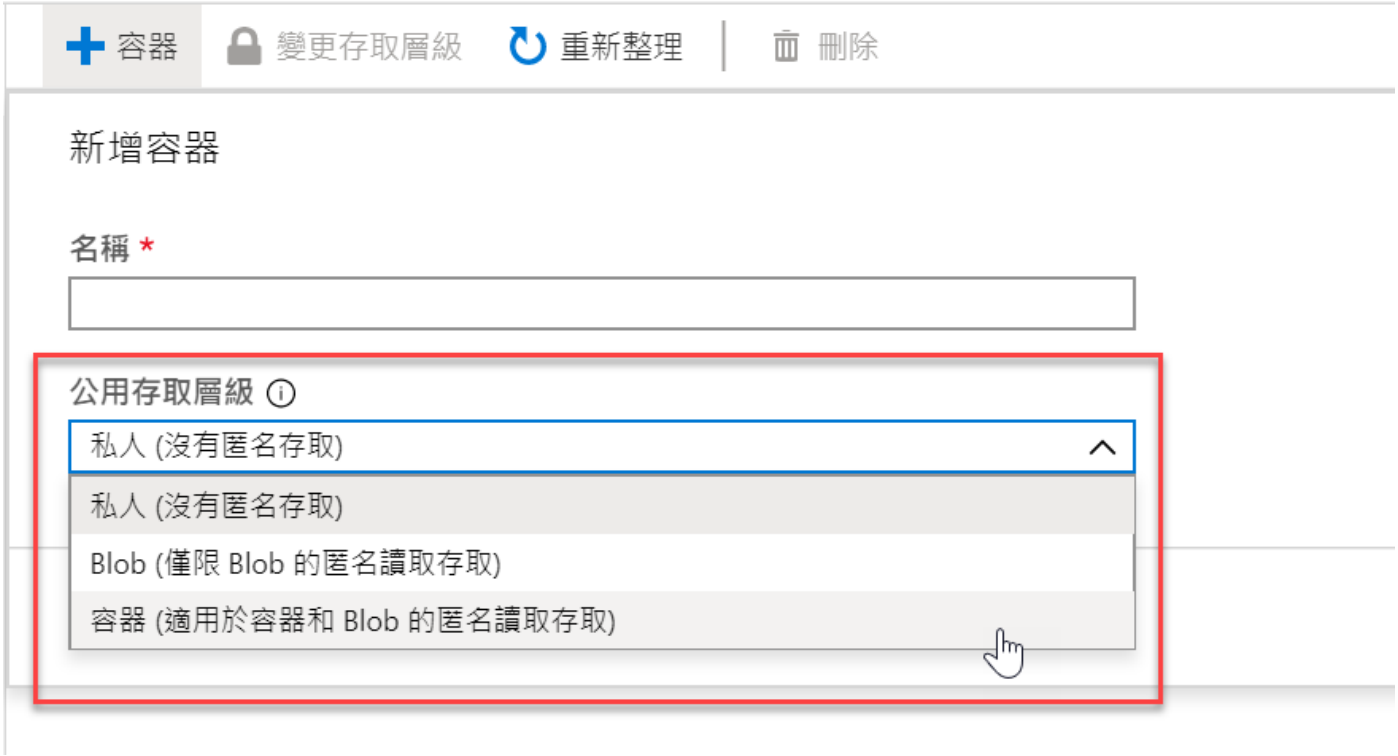
本堂教學重點

1. 雲端檔案儲存體
2. 網站資料存取權限簽章設計

- 下堂教學重點

2.網站資料存取權限簽章設計

網站資料存取權限簽章設計



網站資料存取權限簽章設計

- Azure 儲存體的所有資料都會使用儲存體服務加密（SSE）自動加密
- 使用 HTTPS 通訊協定，針對傳輸過程加密
- 使用共用存取簽章來授與 Azure 儲存體資料物件的存取權

網站資料存取權限簽章設計

- 下載 Blob (透過 Uri 方式)
  - 當不開放匿名儲存權限時，必須加入臨時簽章，才能直接下載

```
var readPolicy = new SharedAccessBlobPolicy()
{
    Permissions = SharedAccessBlobPermissions.Read,
    SharedAccessExpiryTime = DateTime.UtcNow + TimeSpan.FromMinutes(5)
};

var sasConstraints = new SharedAccessBlobPolicy();
sasConstraints.SharedAccessStartTime = DateTime.UtcNow.AddMinutes(-5);
sasConstraints.SharedAccessExpiryTime = DateTime.UtcNow.AddMinutes(10);
sasConstraints.Permissions = SharedAccessBlobPermissions.Read;

var sasBlobToken = blob.GetSharedAccessSignature(sasConstraints);

var newUri = new Uri(blob.Uri.AbsoluteUri + blob.GetSharedAccessSignature(readPolicy));
```

操作示範：

儲存體存取權限簽章

跨站請求偽造

- Cross-site request forgery - CSRF 或者 XSRF
- 攻擊目的
  - 偽造成使用者身份對目標伺服器發出正常請求

跨站請求偽造

- 攻擊手法

小富登入網銀，伺服驗證身份

跨站請求偽造

- 攻擊手法

伺服驗證身份，發給代表其身份的cookie

跨站請求偽造

- 攻擊手法

小富輸入轉帳5000到帳戶A12345
http://www.myrichbank.com/pay?account=A12345&amount=5000

跨站請求偽造

- 攻擊手法

轉帳成功後，小富沒有登出網銀，
直接瀏覽另一個 mytodaynews 網站

跨站請求偽造

- 攻擊手法

mytodaynews 網站首頁被惡意植入了一段 JavaScript

跨站請求偽造

- 攻擊手法

document.cookie
取得小富網銀未過期的cookie

跨站請求偽造

- 攻擊手法

發送了請求到網銀伺服器

熱門新聞!

跨站請求偽造

- 攻擊手法

實果!!
小富的帳戶被惡意轉出了300000
到它人帳戶A168888

跨站請求偽造

- 攻擊分析
  - 伺服器驗證 cookie 正確即會執行相關作業，伺服器並無法判斷請求是否為真正的使用者所發起
  - 即便 cookie 有做加密，只要 cookie 未到期，發送到伺服器端解密後仍然是可以通過驗證的
  - Https 並無法防止 CSRF 攻擊，Https 只能保證傳輸過程是加密的

跨站請求偽造

- 攻擊分析
  - 改用 POST 方式並無法防止 CSRF 攻擊，Javascript 等前端程式語言，仍然是可以用程式的方式發出 POST 請求的

```
$.ajax({
  type: "POST",
  url: "http://www.myrichbank.com/pay?account=A168888&amount=300000",
  data: data,
  success: success,
  dataType: dataType
});
```

跨站請求偽造

- 防禦技巧
  - 網銀頁面除了cookie之外，增加 one time 式的 token，正常頁面在發送請求時連帶送回 token，伺服器端同時驗證 token 及 cookie
  - 偽造的頁面（請求）並無法取得這個 one time 式的 token，因此無法通過伺服器端的驗證

```
>
   <div>
       轉帳帳戶：
       <input name="PayAccount" type="text" id="PayAccount" /><br />
       轉帳金額：
       <input name="PayAmount" type="text" id="PayAmount" /><br />
       <input type="submit" name="PayAction" value="轉帳" id="PayAction" />
       <input type="hidden" name="OneTimeToken" id="OneTimeToken" value="abcdef123456" />
   </div>
/form>
y>
```

Q&A

下堂教學重點

- Web API 設計概念
- API 資料傳輸 JSON 劫持

問卷

http://www.pcschoolonline.com.tw

巨匠線上真人

www.pcschoolonline.com.tw