



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

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

The screenshot shows the homepage of the Juei Computer Online Live website. The header is orange with navigation links: 巨匠電腦線上真人 (Juei Computer Online Live), 開課查詢 (Class Inquiry), 免費體驗專區 (Free Experience Area), 課程總覽 (Course Overview), 專業師資 (Professional Faculty), 學員專區 (Student Area), 講師專區 (Instructor Area), and 最新消息 (Latest News). There are also social media icons for 360, Facebook, and YouTube. A user is logged in as '您好!' with a '登出' (Logout) button. The main banner features the text '程式語言好難學?' (Programming Language is so hard to learn?), '那是因為你還沒學過Python!' (That's because you haven't learned Python!), and '(線上老師 LIVE 直播教學 · 搶先看)' (Online Teacher LIVE Broadcast Teaching · Sneak Peek). A dropdown menu is open from the '學員專區' (Student Area) link, listing various options: 點數卡產品兌換 (Points Card Product Exchange), APCS檢測專區 (APCS Detection Special Area), 公告專區 (Announcement Special Area), 我的課表 (My Class Schedule), IT真人課程劃位 (IT Live Course Seating), 電腦分校課程劃位 (Computer Branch Course Seating), 外語真人課程劃位 (Foreign Language Live Course Seating), 美語分校課程劃位 (American English Branch Course Seating), 取消劃位 (Cancel Seating), 課程檔案下載 (Course Archive Download - highlighted with an orange box and a callout bubble), 上課權益查詢 (Class Benefit Inquiry), 教學平台測試 (Teaching Platform Test), 學習諮詢 (Learning Consultation), 常見問題 (Frequently Asked Questions), 個資維護 (Personal Information Maintenance), 忘記密碼 (Forgot Password), and 登出 (Logout). The background of the banner has a blue and purple digital theme with a clock face showing 98% and 54%.

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

360 f YouTube

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

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)

巨匠電腦真人課程

ZOOM 學員操作說明

The screenshot shows the Zoom interface with several key elements highlighted and numbered:

- 5 查看選項/共同註記/筆 (連連看)**: A dropdown menu is open from the '共同註記' (Annotate) button in the top toolbar, showing options: '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' button in the toolbar is also highlighted with an orange box.
- 2 共享螢幕 (指導演練；點評作品)**: A callout box points to the '共享螢幕' (Share Screen) button in the bottom toolbar. The callout text reads: '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**: A callout box points to the '聊天' (Chat) button in the bottom toolbar.
- 3 與會者/舉手**: A callout box points to the '與會者' (Participants) button in the bottom toolbar. A secondary callout box points to the '舉手' (Raise Hand) button within the '與會者' window.
- 4 解除靜音**: A callout box points to the '解除靜音' (Unmute) button in the bottom toolbar.

The interface also shows a top bar with the URL 'www.pcschool.com.tw' and a status bar at the bottom with icons for '解除靜音', '啟動視訊', '邀請', '與會者', '共享螢幕', '聊天', and '錄影'.



巨匠線上真人

資訊安全概論與網站軟體安全建構實務

第二堂：雲端網站安全性設計與 OWASP防範對策

本堂教學重點

1. 雲端服務與雲端虛擬機器的差別
 2. 雲端網站安全性設計與OWASP防範對策
- ◆ 下堂教學重點

本堂教學重點

1. 雲端服務與雲端虛擬機器的差別
 2. 雲端網站安全性設計與OWASP防範對策
- ◆ 下堂教學重點

1.雲端服務與雲端虛擬機器的差別

雲端服務與雲端虛擬機器的差別



IaaS

Infrastructure-as-a-Service

主機

基礎結構即服務



PaaS

Platform-as-a-Service

建置

平台即服務



SaaS

Software-as-a-Service

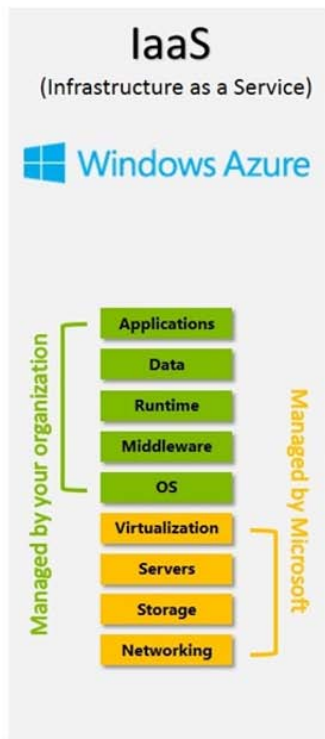
消費

軟體即服務

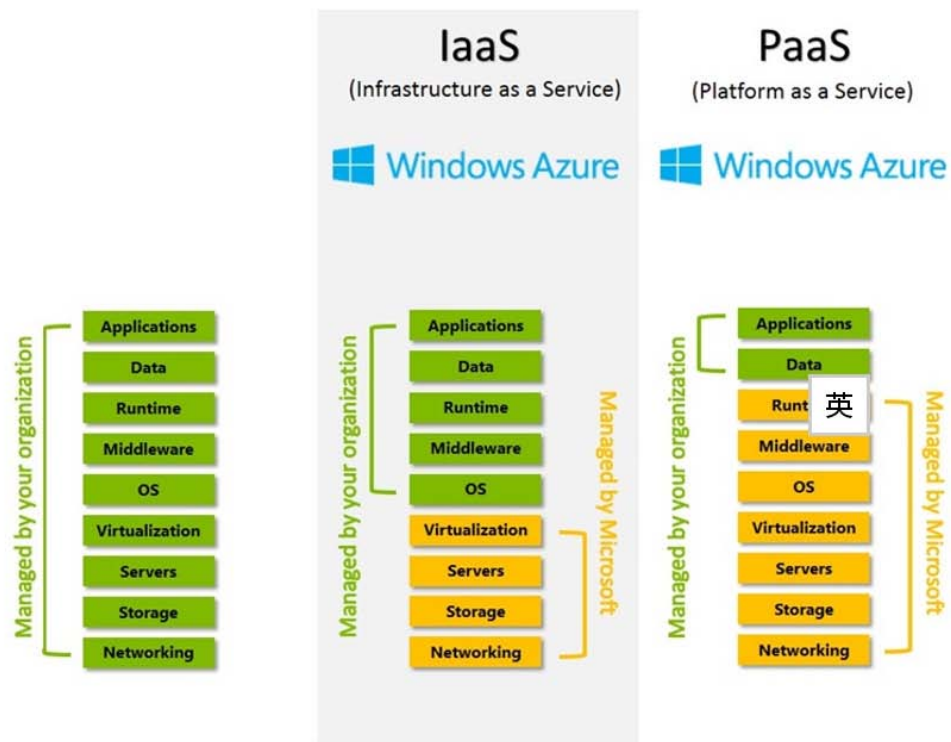
雲端服務與雲端虛擬機器的差別



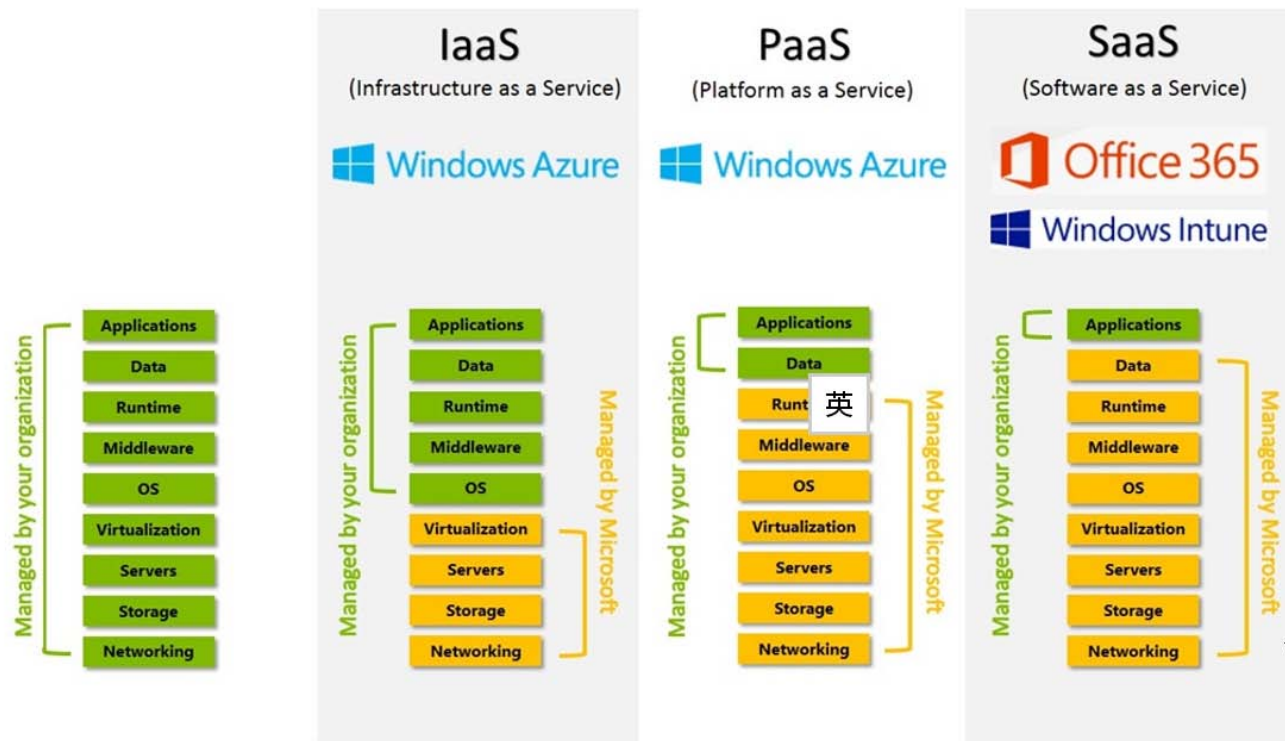
雲端服務與雲端虛擬機器的差別



雲端服務與雲端虛擬機器的差別



雲端服務與雲端虛擬機器的差別



雲端服務與雲端虛擬機器的差別

◆ 雲端虛擬機器

◆ IaaS

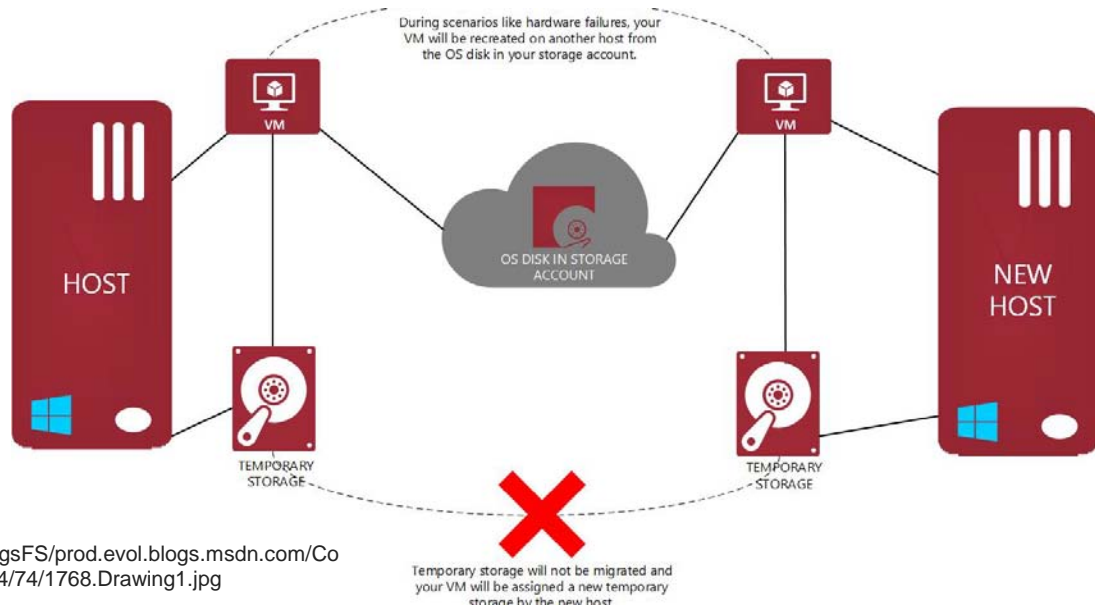
- ◆ 虛擬機器 (或 VM) 是實體電腦的軟體模擬
- ◆ Azure使用虛擬化的技術
- ◆ 對於運算環境的控制權最高
- ◆ 不需購買並維護實體硬體
- ◆ 安裝在VM上的所有軟體及維運均由使用者自行管理
- ◆ 每一訂用帳戶目前的限制是每一區域 20 個 VM
- ◆ 支援Linux、Windows Server、SQL Server、Oracle、IBM 與 SAP

雲端服務與雲端虛擬機器的差別

- ◆ 虛擬機器皆包含作業系統磁碟與本機磁碟
 - ◇ 本機磁碟儲存體為免費提供
 - ◇ 作業系統磁碟則按照磁碟的一般費率收費
- ◆ 不執行的虛擬機器仍可能有費用的產生
 - ◇ 已停止 - 收取配置核心數的費用
 - ◇ 已刪除 (解除配置) - 核心已不再配置到虛擬機器，因此不予計費

雲端服務與雲端虛擬機器的差別

- ◆ VM 可以在任何時間點移動到不同的主機(體故障等)，臨時磁碟機上的任何資料都不會被遷移



<https://msdnshared.blob.core.windows.net/media/MSDNBlogsFS/prod.evol.blogs.msdn.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/01/54/74/1768.Drawing1.jpg>

雲端服務與雲端虛擬機器的差別

- ◆ 暫存磁碟什麼情況下會造成資料遺失
 - ◆ 調整 vm 大小時
 - ◆ 關閉或重新開機 vm
 - ◆ vm 被移動到不同的主機伺服器 (由於服務修復、關閉和重新開機) 時
 - ◆ 主機被更新時
 - ◆ 主機遇到硬體故障
- ◆ 一旦遺失就無法復原資料

雲端服務與雲端虛擬機器的差別

◆ 軟體授權費用

- ◆ 自行安裝軟體於VM上，則軟體授權責任由使用者負責
- ◆ 選擇已預載的VM，則軟體授權費用包含於VM建置的費用內
- ◆ 舉例
 - 自行安裝SAP於VM上，須自行負擔SAP授權責任
 - 選擇建立SQL Server VM，則軟體授權費用已內含

雲端服務與雲端虛擬機器的差別

- ◆ 不可使用既有名稱
 - ◆ admin 、 administrator 、 guest 、 root 、 user
 - ◆ Azure會檢查名稱是否合乎規範
- ◆ 密帳必須符合複雜度原則

雲端服務與雲端虛擬機器的差別

◆ Azure App Service

- ◆ 平台即服務PaaS，Azure 會管理 OS 和應用程式run time的更新及修補
- ◆ <app_name>.azurewebsites.net 預設支援 https
- ◆ 自訂網域則必須使用自訂憑證
 - App Service 憑證
 - ▶ 直接在 Azure 中建立憑證，憑證會在 Azure Key Vault 中保護
 - 第三方憑證
 - ▶ 上傳向憑證授權單位購買的自訂 SSL 憑證

雲端服務與雲端虛擬機器的差別

◆ Azure App Service

- ◆ 預設接受所有 IP 位址的請求
- ◆ 可以設定限制存取的 IP 位址



存取限制

存取限制可讓您定義允許/拒絕規則的清單，以控制進入您應用程式的流量。規則會依優先順序評估。若：量。 [深入了解](#)

codeian.azurewebsites.net

[codeian.scm.azurewebsites.net](#)



新增規則



優先順序

名稱

來源

端點狀態



1

Allow all

Any

軟體操作示範：

實作：APP Service

雲端服務與雲端虛擬機器的差別

◆ 網站設定檔安全管理

- ◆ 資料庫連線字串

- ◆ 應用程式設定值

- ◆ 常見做法是放在config檔內，例如web.config，一旦設定檔被竊，所有資訊全部曝光

雲端服務與雲端虛擬機器的差別

◆ Azure APP Service

- ◆ Azure APP Service config (組態)，經過加密並儲存在 Azure 中，在應用程式啟動時解密，加密金鑰會定期輪替
- ◆ 由 Azure Key Vault 金鑰保存庫來管理，撰寫程式向 Azure Key Vault 服務取得所儲存的資料

軟體操作示範：

實作：APP Service網站設定檔安
全性管理

雲端服務與雲端虛擬機器的差別

- ◆ 本機端或虛擬機器的 web.config 加密
 - ◇ 透過 aspnet_regiis.exe 指令進行加解密
 - ◇ 資料庫連線資訊加密
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef "connectionStrings" "D:\My.Web\MVCDEMO"
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf "connectionStrings" "D:\My.Web\MVCDEMO"
 - ▶ D:\My.Web\MVCDEMO : 網站實體路徑

雲端服務與雲端虛擬機器的差別

- ◆ 本機端或虛擬機器的 web.config 加密
 - ◇ 透過 aspnet_regiis.exe 指令進行加解密
 - ◇ 應用程式資訊加密
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pef "appSettings" "D:\My.Web\MVCDEMO"
 - C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -pdf "appSettings" "D:\My.Web\MVCDEMO"
 - ▶ D:\My.Web\MVCDEMO : 網站實體路徑

軟體操作示範：

實作：本機網站設定檔加解密

本堂教學重點

1. 雲端服務與雲端虛擬機器的差別
2. 雲端網站安全性設計與OWASP防範對策

◆ 下堂教學重點

2.雲端網站安全性設計與OWASP 防範對策

雲端網站安全性設計與OWASP防範對策

A screenshot of a forum post. The background is a blurred image of a forum interface. Overlaid on the center is large, bold text. The top line is in yellow with a black outline, and the bottom line is in green with a black outline. Below the text, there is a light blue footer area containing the source information.

個資如此不值錢
200000筆資料只值8歐元

EZ3C.TW
國外論壇流出 1111 人力銀行 20 萬筆個人求職資料外洩，只值 8 歐元 :: 哇哇3C日誌

雲端網站安全性設計與OWASP防範對策

◆ 網站應用程式基本安全性防範重點

- ◆ 防止惡意資料的輸入
- ◆ 安全性的資料庫資料存取
- ◆ 使用者權限的管理
- ◆ Cookie 資訊的保護

永遠不要相信
客戶端傳送過來的資料

雲端網站安全性設計與OWASP防範對策

◆ OWASP

◆ Open Web Application Security Project

- <https://www.owasp.org/>

◆ OWASP TOP 10 是其中的一項計劃

- https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

◆ 提高Web應用程式的安全性

◆ Top 10 - Web應用程式安全風險前十名

- https://www.owasp.org/index.php/Top_10-2017_Top_10

雲端網站安全性設計與OWASP防範對策

◆ OWASP TOP 10 2017

- ◆ 注入攻擊 Injection
- ◆ 失效的身份認證 Broken Authentication
- ◆ 敏感資料外洩 Sensitive Data Exposure
- ◆ XML外部實體注入 XML External Entity Injection
- ◆ 失效的權限控制 Broken Access Control
- ◆ 不安全的組態設定 Security Misconfiguration
- ◆ 跨站腳本攻擊 Cross-Site Scripting (XSS)
- ◆ 不安全的反序列化漏洞 Insecure Deserialization
- ◆ 引用有已知漏洞的元件 Using Components with Known Vulnerabilities
- ◆ 不完善的記錄及監控 Insufficient Logging&Monitoring

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

- ◆ 避免將用戶端的輸入值，以字串串接方式組成SQL Command
- ◆ (.NET) 使用 Parameter 方式進行資料庫溝通
- ◆ 別再使用字串 replace 自行過濾字元

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

```
using (SqlCommand cmd = new SqlCommand())  
{  
    cmd.CommandText = "select * from Employees where EmployeeID='" + id + "'";  
}
```



id = 1

```
ry1.sql - I...L98GW\ianch (55))* ✕  
select * from Employees where EmployeeID='1'
```

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

```
using (SqlCommand cmd = new SqlCommand())  
{  
    cmd.CommandText = "select * from Employees where EmployeeID='" + id + "'";  
}
```



id = ' or 1=1

select * from Employees where EmployeeID='' or 1=1						
訊息						
EmployeeID	LastName	FirstNa...	Title	TitleOfCourtesy	BirthDate	HireDate
	Davolio	Nancy	Sales Representative	Ms.	1948-12-08 00:00:00.000	1992-05-01 00:00:00
	Fuller	Andrew	Vice President, Sales	Dr.	1952-02-19 00:00:00.000	1992-08-14 00:00:00
	Leverling	Janet	Sales Representative	Ms.	1963-08-30 00:00:00.000	1992-04-01 00:00:00
	Peacock	Margaret	Sales Representative	Mrs.	1937-09-19 00:00:00.000	1993-05-03 00:00:00

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

```
using (SqlCommand cmd = new SqlCommand())  
{  
    cmd.CommandText = "select * from Employees where EmployeeID='" + id + "'";  
}
```



id = ' or 1=1

```
select * from Employees where EmployeeID='' or 1=1
```

EmployeeID	LastName	FirstNa...	Title	TitleOfCourtesy	BirthDate	HireDate
	Davolio	Nancy	Sales Representative	Ms.	1948-12-08 00:00:00.000	1992-05-01 00:00:00
	Fuller	Andrew	Vice President, Sales	Dr.	1952-02-19 00:00:00.000	1992-08-14 00:00:00
	Leverling	Janet	Sales Representative	Ms.	1963-08-30 00:00:00.000	1992-04-01 00:00:00
	Peacock	Margaret	Sales Representative	Mrs.	1937-09-19 00:00:00.000	1993-05-03 00:00:00

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

```
using (SqlCommand cmd = new SqlCommand())
{
    cmd.CommandText = @"SELECT * FROM customers
    WHERE name = '" + name + "' AND password = '" + pwd + "'";
}
```

'OR 1=1 --

```
SELECT * FROM customers WHERE name = 'ian' AND password = '123'
SELECT * FROM customers WHERE name = '' OR 1=1-- AND password = '123'
```

雲端網站安全性設計與OWASP防範對策

◆ SQL Injection注入攻擊

```
using (SqlCommand cmd = new SqlCommand())
{
    cmd.CommandText = @"SELECT * FROM customers
    WHERE name = '" + name + "' AND password = '" + pwd + "'";
}
```

'OR 1=1 ; Drop Table customers --

SELECT * FROM customers WHERE name = 'ian' AND password = '123'

SELECT * FROM customers WHERE name = '' OR 1=1; Drop Table customers -- AND password = '123'

軟體操作示範：

實作：SQL Injection

雲端網站安全性設計與OWASP防範對策

- ◆ 失效的身份認證 Broken Authentication
 - ◆ 身分驗證憑證沒有用Hash或加密保護
 - ◆ 憑證可猜測
 - ◆ Session ID暴露在URL裡
 - ◆ Session ID沒有超時限制；或者，用戶登出後taken沒有失效
 - ◆ 成功登入後，Session ID沒有替換
 - ◆ 密碼、Session ID和其他憑證未使用加密傳輸

雲端網站安全性設計與OWASP防範對策

◆ XSS攻擊

- ◆ 跨站腳本攻擊
- ◆ 注入惡意指令程式碼到網頁
- ◆ 程式碼注入
- ◆ <https://zeroday.hitcon.org/vulnerability/ZD-2018-00550>

軟體操作示範：

實作：XSS攻擊

雲端網站安全性設計與OWASP防範對策

◆ XML External Entity Injection

- ◆ 注入攻擊

- ◆ 採XML做為資料交換管道

- ◆ 完全禁用DTD (外部實體)

- https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

雲端網站安全性設計與OWASP防範對策

◆ XML External Entity Injection

```
<?xml version="1.0" encoding="UTF-8"?>  
<stockCheck><productId>123</productId></stockCheck>  
</xml>
```

User端輸入

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE haha [ <!ENTITY id SYSTEM "file:///etc/passwd"> ]>  
<stockCheck><productId>&id;</productId></stockCheck>
```

雲端網站安全性設計與OWASP防範對策

◆ 敏感資料外洩

◇ Sensitive Data Exposure

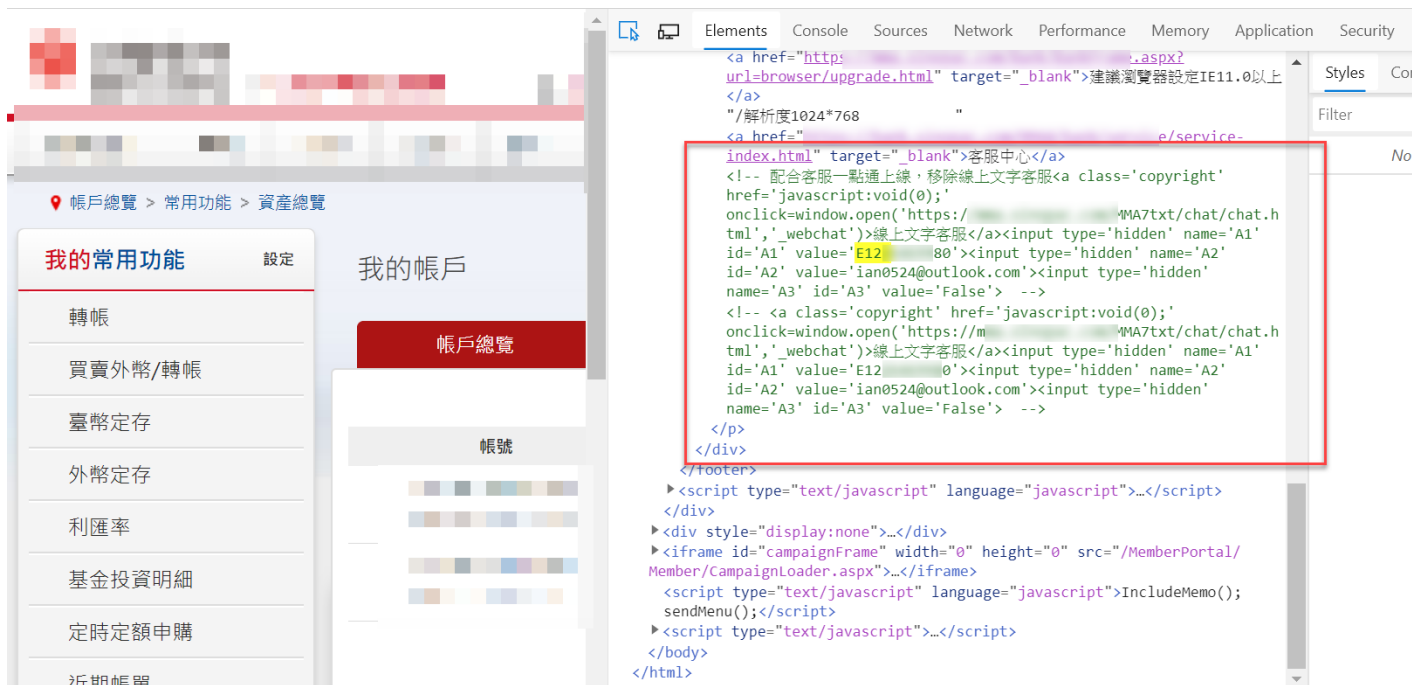
◇ 針對敏感性資料需要做額外的保護措施

- 加密
- 不要在URL帶上參數

▶ <http://abc.def.com?idno=E123456789>

雲端網站安全性設計與OWASP防範對策

◆ 敏感資料外洩



The screenshot shows a web application interface on the left and a browser's developer tools on the right. The web application displays account information, including a sidebar with "我的常用功能" (My常用功能) and a main section titled "我的帳戶" (My Account). The browser's developer tools show the source code of the page, with a red box highlighting a section of the code that contains sensitive data, such as email addresses and phone numbers, which are highlighted in yellow.

```
<a href="http://.../browser/upgrade.html" target="_blank">建議瀏覽器設定IE11.0以上</a>"/>
"/>
<a href=".../e/service-index.html" target="blank">客服中心</a>
<!-- 配合客服一點通上線，移除線上文字客服<a class='copyright'
href='javascript:void(0);'
onclick=window.open('https://.../MA7txt/chat/chat.h
tml','webchat')>線上文字客服</a><input type='hidden' name='A1'
id='A1' value='E12...80'><input type='hidden' name='A2'
id='A2' value='ian0524@outlook.com'><input type='hidden'
name='A3' id='A3' value='False'> -->
<!-- <a class='copyright' href='javascript:void(0);'
onclick=window.open('https://m.../MA7txt/chat/chat.h
tml','webchat')>線上文字客服</a><input type='hidden' name='A1'
id='A1' value='E12...0'><input type='hidden' name='A2'
id='A2' value='ian0524@outlook.com'><input type='hidden'
name='A3' id='A3' value='False'> -->
</p>
</div>
</footer>
<script type="text/javascript" language="javascript">...</script>
</div>
<div style="display:none"></div>
<iframe id="campaignFrame" width="0" height="0" src="/MemberPortal/
Member/CampaignLoader.aspx">...</iframe>
<script type="text/javascript" language="javascript">IncludeMemo();
sendMenu();</script>
<script type="text/javascript">...</script>
</body>
</html>
```


軟體操作示範：

實作：敏感資料外洩

雲端網站安全性設計與OWASP防範對策

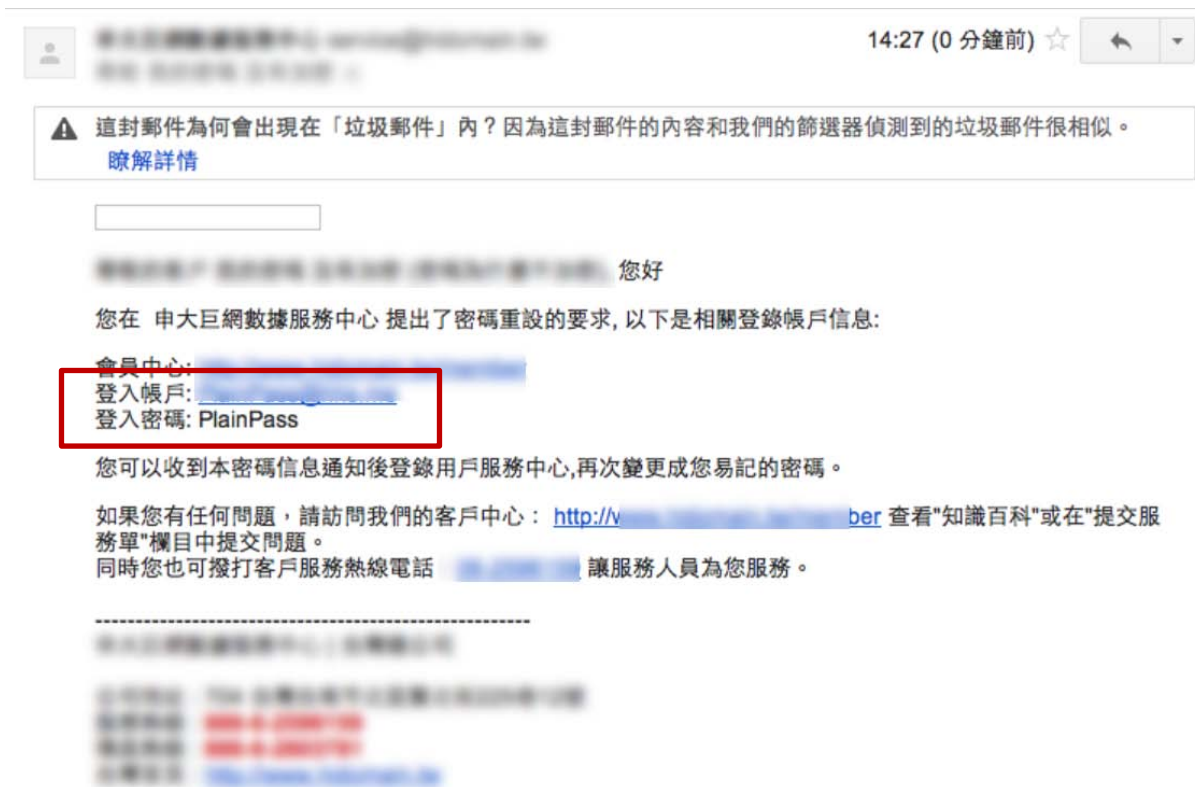
◆ 哪裡怪怪的？

賣家氣炸！半年內網購225次不取貨 婦人：吃藥後忘了

小舖查覺有異，清查之後發現劉女申請的帳號雖然名字、帳號不同，但使用的密碼卻都一樣，憤而提告。對此，持輕度身心障礙手冊的劉女坦承，自己確實有向小舖訂貨，但沒取貨是因為沒有收到簡訊通知，「有時候吃藥後，連自己在做什麼都忘了。」

雲端網站安全性設計與OWASP防範對策

◆ 哪裡怪怪的？



Q&A

下堂教學重點

- ◆ 雲端服務與雲端虛擬機器的差別
- ◆ 雲端網站安全性設計與OWASP防範對策

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



➤ 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](#)。

公告專區

我的課表

課程劃位

取消劃位

2

課程檔案下載

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)。

問
卷

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	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	



巨匠線上真人

www.pcschoolonline.com.tw