

# 網上應用系統保安

## 1. 當我的網站伺服器使用 UNIX 或微軟視窗系統時，我應採取哪種一般保安預防措施？

你應採取多項預防措施，例如應移除所有未使用的服務、指令介面、和程式語言解譯器或編譯器，並應正確安裝網站伺服器，且應依照“有需要才知道”基礎來授權使用檔案的權利，也應定期檢查系統和網絡紀錄中可疑的活動。此外，應適當地管理可登入網站伺服器的用戶帳號的數目，例如確定所有用戶選擇良好的密碼，至少利用保密插口層(SSL) / 傳輸層保安 (TLS) 來應保護網站伺服器的用戶認證，以確保其密碼不會被攻擊者竊聽。假如系統牽涉敏感或機密資料，也應考慮使用雙重認證。

應注意以下指引，以加強網站伺服器的保安：

- 根據供應商的保安指引，安全地配置網站伺服器。
- 使用適當的特權帳號來執行網站伺服器程序，避免使用例如“root”，“SYSTEM”或“Administrator”之類的完全特權帳號來執行網站伺服器程序。
- 安裝最新保安修補程式於網站伺服器軟件。
- 配置接達權使網站伺服器軟件無法修改提供給用戶的檔案，換言之，網站伺服器軟件應有只供讀取檔案的接達權。
- 當儲存或處理敏感資訊時，在網站伺服器中安裝基於主機的入侵檢測系統(HIDS)，以監控可疑活動或未授權創作/刪除/修改檔案。應主動覆檢入侵檢測系統的警告和報告，以盡早確定可能發生的保安攻擊。
- 安裝網站伺服器軟件，避免資訊外洩，例如網站伺服器軟件版本、內部IP位址、目錄結構等等。
- 關閉或移除網站伺服器軟件中不必要的組件。
- 確定在網站伺服器中的應用程式檔案，並利用接達控制保護它們。
- 當使用SSL時，備份私人密碼匙，作為伺服器核證之用，且避免未經授權的接達。

## 2. 什麼是一般網上應用系統弱點？什麼是終端用戶一般保障措施？

以下是網絡應用程式常見的漏洞：

- 跨網址程序編程 (XSS)
- 插入弱點
- 惡性檔案執行
- 危險直接物件參照(Insecure Direct Object Reference)
- 跨網址要求偽造 (CSRF)
- 資訊外洩和不適當的錯誤處理
- 有缺陷的認證和對話管理
- 不安全的加密運算儲存

- 不安全的溝通方式
- 沒有限制URL的接達權

以下是一些給終端用戶的保安訣竅:

- 不要使用公共電腦登入重要的網絡應用程式
- 不要儲存你的用戶名稱和密碼在工作站
- 記得在結束對話時登出
- 不同的網絡應用程式和伺服器使用不同的登入組和密碼
- 假如不能使用一次性密碼的話，要定期改變重要網絡應用程式的密碼
- 立即報告給服務提供者異常的行為
- 確定完整修補及更新操作系統和系統零件，例如互聯網瀏覽器
- 安裝個人防火牆及使用最新病毒識別碼來安裝抗電腦病毒軟件
- 不要從未知的來源下載軟件或插件(plug-ins)

### 3. 網上應用系統的保安訣竅是什麼?

透過完整的系統發展周期，考慮不同的保安控制:

- 收集應用程式保安要求。
- 採取最佳作業實務的標準或基準。
- 定義保安編碼標準，以消除攻擊，例如 SQL 插入攻擊、跨網站程序編程。
- 為應用程式回應進行淨化，以捕捉所有輸出、回覆代碼和錯誤代碼。
- 除非經過強大加密技術所證實，否則不要信任 HTTP 交付的標頭、客戶瀏覽器參數、cookie 程式、表格欄或隱藏參數。
- 在伺服器保存敏感的對話價值，以避免客戶端修改。
- 加密含有敏感資料的網頁和避免 caching 技術。
- 推行對話管理。
- 推行合適的終端用戶帳號和接達權管理。
- 限制後端資料庫的接達，執行 SQL 指令和 OS 指令。
- 當應用程式呼叫時，不要用真正的檔案名稱和目錄路徑回答，使用配對(mapping)作為過濾層。
- 建立一個集中模組，進行應用程式審計和報告。
- 使用最合適的認證方法，以確定和認證進入的用戶 / 系統要求。
- 建立並執行威脅模型 (threat modelling)。
- 設計及推行網絡應用程式保安架構。
- 在發展階段，執行保安風險評估，以確定要求的保安控制。
- 強制執行保安守則標準。

- 執行保安測試，例如壓力測試、系統測試、回歸測試、組件測試等。
- 執行編碼詳細覆檢。
- 在發表系統正式運作之前和任何重大系統改變之後，必須執行全面保安審計。
- 定期檢查應用程式紀錄。
- 推行版本控制和分離應用程式發展環境。
- 安裝網絡應用程式防火牆。

#### 4. 假如外判網上應用程式發展，有沒有核對清單以便核實及接受產品?

以下是幾個網上應用程式保安評估需要檢驗的範例：

##### 識別與認證

- 用戶與程序是如何認證的?
- 所推行的認證程序是否有遵守規格和機構保安政策?
- 假如認證是基於密碼的，如何處理和儲存用戶的密碼?
- 密碼處理機制是否遵守機構保安政策?
- 程式源碼中是否有任何設定於源碼中(hard-coded)的密碼或密碼匙?
- 是否要求應用程式要認證每一個對話?

##### 資料保護

- 資料保護機制是否依照機構保安政策來推行?
- 是否適當地保護所有儲存和暫存的資料?
- 是否適當地保護傳送中的所有資料?
- 假如使用加密，是如何處理加密的?
- 加密處理是否遵守整體機構保安政策?

##### 紀錄

- 審計追蹤機制是否根據規格來推行?
- 應用程式審計紀錄是否無力對抗非授權的刪除、修改或揭露?

##### 錯誤處理

- 如何處理錯誤訊息?
- 資訊外洩是否有任何機會在隨後的攻擊中被利用?
- 應用程式失敗是否導因於危險的系統狀態?

## 操作

- 是否強行執行職務分工和最低特權原則?
- 在發表最後產品之前，內建用戶名稱、測試用戶名稱和預設用戶密碼是否已經從操作系統、網站伺服器和應用程式本身中移除?
- 是否完整且清楚定義系統管理程序、修改管理程序、運作復原程序和備份程序?

必須強調這份清單並不是詳盡的，一切端視保安要求和目標網上應用程式的特性，且應該根據特殊需求，列入額外的測試例子或檢查標準。

此外，當外判任何資訊系統給第三方資訊提供者時，應放置合適的保安管理程序，以保護資訊和消弭有關資訊科技專案/服務的相關保安風險。

## 5. 什麼是一般認證方法?

認證系統中有三個基本的認證要素，即是你知道的東西、你擁有的東西及你本身即擁有的東西。要作為對抗身分竊取的增加威脅，執行高風險電子交易時，應推行雙重認證。有五個一般常見的認證方法，就是密碼和基於 PIN 的認證、基於 SMS 的認證、對稱密碼認證、公開密碼匙認證及生物特徵認證。每一種方法的詳細資料可以在電子認證網站 <<<http://www.e-authentication.gov.hk/tc/professional/methods.htm>>>中找到。

## 6. 我要如何決定電子交易和其保安要求的適當保證水平?

針對企業擁有者推行安全之電子認證系統的建議流程可在電子認證網站 <<<http://www.e-authentication.gov.hk/en/business/do.htm>>>中找到。你可找到如何決定保證水平和相對應的保安要求資訊。

## 7. 採用虛擬伺服器的一般保安風險是什麼? 什麼是降低其風險的保安措施?

虛擬科技讓一個或多個客戶操作系統(guest operating systems)運作於另一個主機操作系統之上，每一個客戶操作系統在模擬環境中運作，該環境設備齊全、獨立，且與真實的機器幾乎一樣。要是沒有適當的保護，機構將面臨虛擬化帶來的保安風險。

舉例來講，發展虛擬化的一般保安威脅是不同系統間的保安獨立會因虛擬化而導致削弱效果，在虛擬化之後，不同資訊系統間的分離仰賴於正確的內部虛擬網絡配置。不正確的配置可能會危及保安。專用虛擬機器(VM)上之基於軟件的網絡防火牆可能有助解決這個風險；另一個辦法是在VM間推行硬件防火牆，因此，硬件防火牆會管理所有VM之間的交易，然而，該方法也許會對網絡表現有明顯的影響。

確保安全的虛擬機器包含許多如同確保安全的操作系統的最佳作業實務，包括推行優質修補程式管理、端點保安措施，如抗電腦病毒措施及推行在主機和客戶操作系統之間的防火牆。

## 8. 入侵者如何透過網絡攻擊來攻擊終端用戶？

主要網絡攻擊者將終端用戶或其電腦列為目標的重要範例如下：

### 'Italian job' 網絡攻擊

2007 年 6 月，有人攻擊超過一千個網站，其中包含許多義大利政府網站，受影響的網站被植入一則簡短的 HTML “iFRAME”碼，將參觀者重新導入到另一個網站，然後惡性 JavaScript 會在其電腦中安裝按鍵紀錄工具 (keylogger) 和特洛伊木馬下載檔案 (Trojan downloader program)，以便測試和試看是否可以危及更多的電腦。

### MySpace Phish / Drive-by 攻擊

2007 年 6 月，發現數百個 MySpace 個人檔案被植入仿冒詐騙 (Phishing) 網站連結，MySpace 的用戶面臨的風險是當他們參閱任何 MySpace 個人檔案網頁時，包含惡性 JavaScript 的網頁會無聲無息地將參觀者重新導入到惡性網站，試圖濫用 Internet Explorer 的漏洞。一個常見的代理網絡 bot 是 “flux bot”，會被安裝來嘗試隱藏於經常更換的代理伺服器後面的仿冒詐騙網站。

### 跨網站程式編程病毒 (“XSS”)

在 2005 年 10 月，Samy 病毒的作者濫用在 MySpace 上的 XSS 漏洞，其可以上傳受感染的 XSS 碼到他的 MySpace 個人檔案網頁上，然後，當其他經認證的 MySpace 用戶參觀 Samy 的個人檔案時，該病毒強迫他們的網絡瀏覽器加入 Samy 為朋友，並利用惡性程式碼修改他們的個人檔案，所以當用戶參觀 Samy 或是任何受感染的用戶個人檔案時，Samy 病毒就可以繼續大量地擴散。當時，超過一百萬個 MySpace 用戶個人檔案受到感染。

### 其他攻擊

仿冒詐騙 (Phishing) 可被視為社會工程攻擊 (social engineering attack)，罪犯試圖引誘沒防備的網絡瀏覽者進入看似真實網站的詐騙網站，例如 eBay，或其他網上銀行的網站。互聯網搜尋引擎也有助網絡攻擊。在 2004 年 12 月，網絡病毒 Santy.A 濫用軟件 phpBB 佈告欄的漏洞，且並不隨機地猜測目標 IP 的位址，而是使用 Google 搜尋引擎來幫忙尋找新的無力對抗的目標，目的是要透過 phpBB 漏洞發動篡改攻擊。