

網站內容管理系統

2008 年 2 月

©香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

免責聲明：政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

目錄

摘要.....	2
I. 介紹.....	3
什麼是網站內容管理系統?.....	3
WCMS對商業上的影響與趨勢.....	4
WCMS的一般組件	4
II. 保安上的問題及其防範措施	6
III. 結論.....	8

摘要

「網站內容管理系統」(Web Content Management System, WCMS) 是一個用於網站的應用程式，促進企業內不同部門的使用者，能有效率地管理機構網站的內容。在最近幾年間，機構為了要經由網站來發布與傳達他們的資訊，網頁內容的管理技術已經愈來愈重要。如同其它以網絡為基礎的應用程式一樣，WCMS也受到了相同的資訊保安威脅。本文將會簡述一些與WCMS有關的常見安全問題，並提供一些防範的措施。

I. 介紹

什麼是網站內容管理系統?

自從dot-com在1990年末期開始興盛時，對地球上幾乎任何大或小的公司來說，網站都已經是司空見慣的事。在這些日子裡，幾乎每家企業都需要一個網站，與他們的客戶、合作夥伴，及股東等通訊，提供有關企業的即時資訊、產品與服務訊息。此外，企業網站更有增無減地進行商業活動以及訂單交易的功能。

網站內容更新的傳統方式

建構與設置網站通常不是一次性可以完成的項目。在一家企業中的不同部門，也各有不同領域的內容需要加入與更新。此外，因應現今商業的變化多端，網站的內容亦必須不斷地定期維護與更新。

從前，要作網站的維護時，上傳與更新的工作經常要IT部門的幫忙。把網頁內容更新至伺服器的普遍方法，包括使用FTP（file transfer protocol）的檔案傳輸程式，另一方法則在網頁界面中建立一個專用的上傳路徑，讓不同內容的擁有者能夠選擇適當的檔案，並透過HTTP上傳。這兩種普及方式，至今仍被經營網絡主機的公司及各中小企業（SMEs）所採用。

傳統方式的問題

傳統上，技術人員必須協助需要上網更新網站內容的編輯人員，將內容轉換成適當的網頁專用格式（即HTML），並代為更新到網頁伺服器上。這種多次反覆操作的程序，經常會造成訊息發布的延遲，內容供應者與技術人員之間也需要高度的彼此信賴，很明顯這是個欠缺效率的方法。

對傳統方式而言，管理網站的更新是另一個問題。因為有時候一個網站是由許多不同領域的內容所構成，而這些內容則必須由企業內不同的部門來輸入資料。當可以由多過一個人同時更新網站時，記錄與追蹤更新或修訂的人與網頁最新修訂版本的問題就變得嚴重。

網站內容管理的演進

最近，WCMS的設計，促使以合作模式去更新一個網頁變得更容易。WCMS是一個網站的應用程式，它使企業內不同部門的使用者，能使用一種有效率的方法，管理機構網站的內容。網頁的內容可以包含純文字、圖片，以及影音等。一個現代的WCMS系統也能包含工作流程的功能，以便於執行與批准建立、儲存、與更新網站的步驟流暢無阻。其它功能如版本（versioning）、check-in或check-out的審核等，也有助於網站更新的管理與追蹤。

WCMS對商業上的影響與趨勢

商用的WCMS產品有下列好處¹：

1. 快速的回應時間：我們可以更快速地在網頁上建立一個可用的銷售網站，因為內容擁有者能夠直接更新網頁的內容，而不必依靠相關技術人員的協助。
2. 更有效率的工作流程：WCMS的框架可簡化網站的修訂與更新的需求。利用預設且已達共識的工作流程，來自不同部門的使用者可以加入與更改網頁的內容。
3. 改進的保安功能：在WCMS的框架之下，只有經由監督人員或管理人員批准同意下的內容才可以發布。這也減少了資料發布時可能發生的人為疏忽。此外，大多數的WCMS系統也提供有關發布活動的審計追蹤，這都有助於維持使用者的責任性。
4. 其它的好處則包含改良了的版本追蹤、與翻譯伺服器（translation server）整合、和經由共用的網頁設計與被控制的範本，使網頁的外觀能夠達到一致性。

最近幾年，網站內容的管理技術已經變得愈來愈重要²，在市場上已可以找到商業的及公開原始碼的WCMS產品。

WCMS的一般組件

許多WCMS系統是由Java與PHP之類的程式語言所編寫，且運行在網頁伺服器上。除了網頁伺服器外，WCMS也許還包含了一些額外的組件，如工作流程引擎、搜尋引擎、及電子郵件的整合模組等。

網站的內容通常是儲存在資料貯藏裝置或資料庫如MySQL（公開原始碼）或者Oracle（商業軟件）當中。網站內容也含有純文字與圖片資料以供發布。來自一些被受管理的網站內較舊版本之網頁，也能夠儲存在資料庫中。

¹ <http://www.edocmagazine.com/print.asp?ID=30578>

² <http://mediaproducts.gartner.com/reprints/fatwire/144978.html>

一般而言，設計完成的網頁並不會直接上傳到相關伺服器上。反之，使用者必須在離線狀態下保存好這些網頁的相關資料，直到它們被批准發布。一旦被批准完成後，檔案的傳輸程式便會自動執行，且上傳與連結在生產網頁伺服器裡的有關網頁。

WCMS在本質上是個由後端資料庫所支援的網頁應用程式，還有其它功能如搜尋引擎及與翻譯引擎（translation engine）整合。WCMS也受到跟網上應用系統相同的一般保安威脅，例如跨網址程式編程攻擊（cross-site scripting）、植入式弱點（injection flaws）及惡意程式的執行等。

為了說明使用者的責任，使用者在接達WCMS之前通常必須通過認證。在某些情況下，使用者必須透過一個叫做反向代理伺服器（reverse proxy server）的中介伺服器來作出認證，以代替直接連結WCMS伺服器的方法。此外，對於內容上的職務分工，可把使用者劃分為兩個群組 — 內容編輯人員與內容管理人員。只有內容管理人員擁有決定最終發布與否的權力。至於技術人員所扮演的角色，則是去建立網頁的模板，並且保持其網頁設計風格與一般觀感的一致性。

一般而言，傳送至網頁伺服器的資料與內容都是公開的資訊。假設必須把敏感的資料儲存在WCMS的伺服器上，則應該執行適當的加密以及認證措施。

II. 保安上的問題及其防範措施

如先前所述，WCMS是基於現存網絡技術而建立的應用系統。就像其它網上應用程式般，WCMS也受制於相同的保安威脅，以及在運作程序上的保安漏洞。本節將會討論一些普遍的保安問題，以及如何減低它們所帶來的損害。

保安上的問題

因為WCMS是一種軟件應用程式，所以它就像其它程式一樣容易受到程式錯誤（bugs）的侵襲。而事實上，WCMS的保安漏洞也曾被發現。舉例說，一個被稱為「absolute path traversal vulnerability」的保安漏洞，在2006年就已經在公開源始碼的產品「OpenCms」中被發現。此項保安漏洞讓已認證的遠端使用者能夠隨心所欲地下載檔案³。

另一個保安問題則是在於接達WCMS時所需保護的認證憑證。許多WCMS產品之設計首要任務都只是設法去解決網站本身內容管理方面的問題，而非建立一套安全的產品。有些WCMS產品並沒有在登入與密碼管理上提供足夠的保護機制。且這些密碼（包含了管理員的密碼）都可能以純文本格式被傳送於網絡上。

同樣地，作為發布/上傳程序的一部份，WCMS也有可能使用像FTP這樣的檔案傳輸協定，把WCMS的資料儲存伺服器內的檔案傳輸到網頁伺服器上。使用FTP時，認證憑證與密碼都是以純文本格式在網絡上傳送，所以它並不是一個安全的協定。此外，由於資料發布是一種自動化的程序，FTP的認證憑證可能是已經寫死在某些設定檔內。通常像這樣寫死的登錄密碼是不會經常改動。因此，任何對這些密碼的洩漏，都可能會造成讓他人非法接達這些網頁內容的後果。

若WCMS包含了其它的模組，這種獨特的子系統，也許在WCMS上擁有它們自身的程式錯誤與保安漏洞。舉例說，若WCMS擁有一個電子郵件模組，WCMS就有可能受到跟電子郵件伺服器面對的一些普遍威脅一樣，如仿冒郵件等。總體而言，WCMS的後端資料庫伺服器也有可能存在保安漏洞。

防範措施

有幾項預防措施應該要事先完成，以減低前文所述的保安威脅：

³ <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2006-393>

1. 對於所有的網頁伺服器應用軟件，應該保持執行最佳作業實務，時常更新修補程式。任何關於WCMS產品保安漏洞的警戒或者警示，都應該要立即處理，特別是在WCMS可以直接與互聯網接達的時候。修補程式管理程序也要更新額外的WCMS模組，包括：電子郵件的子系統、後端資料庫的伺服器，以及JAVA的運行環境等。
2. 應該要制定一套嚴格的密碼政策。這當中應該包含密碼的最少長度、分派給每位員工的初始密碼、限制的文字與格式、以及有限的密碼生命週期等。
3. 透過互聯網來傳送的登入動作與密碼，都應該要使用SSL/TLS來保護，使攻擊者不能透過網絡來作偷窺的動作。一般而言，應該要對管理員的頁面作更進一步的控制，使其在互聯網上不會被公開接達。
4. 當由WCMS發布網頁內容到生產網頁伺服器上，像是FTP這種傳輸檔案的程式都應該要被SSH所取代，以利用加密過的資料來保護傳送的渠道。有些SSH的實施也包含了一項特點，那就是控制那些IP被允許連接到目標伺服器。
5. 為了加強資訊保安，許多WCMS都有內建的接達控制，將使用者分為編輯人員及管理人員的角色。而且對這些角色以及所對應的接達權限，都應該清晰地定義與定期審視。
6. 一個好的WCMS應該維持著審計追蹤的機制，並記錄所有經過認可的編輯和批准活動。應該根據它們的有用程度保留這些審計追蹤至一段時間，而且應確保它們的安全，僅允許已授權的人讀取而不能更改。

III. 結論

雖然一個良好的WCMS能夠幫助企業更容易掌握他們的網頁內容，以應付今時今日變化多端的商業環境，但若有不當的內容被發布在網站上時，終端用戶就應該察覺到其對企業可能帶來的保安影響。建議終端用戶如下：

1. 確實知道要發布的是什麼內容。只有經過批准的內容才可以放入相關的發布程序中。
2. 每個使用者的身份（使用者的ID）應該只能同時代表著一個人。不應准許分享或群組共用的ID。
3. 交給服務供應商作保養與維護支援的密碼，如懷疑或証實已被入侵時，則應即時更改該密碼。應該重視密碼的管理作業實務，例如強制實施嚴格的密碼，以及定期更換密碼等。
4. 爲了預防任何嘗試非法接達系統的活動，應該啟動自動保護機制，例如當電腦在預設時間內沒有運作時，需要密碼的屏幕保護程式便應啟動。
5. 當一個編輯與更新群組的成員停止對機構或者群組提供服務時，他在WCMS的使用者帳戶與接達的權力，都應該要盡快終止。
6. 應該定期替使用者電腦的軟件，包括網頁瀏覽器、JAVA的運行環境等更新所有軟件修補程式。