

WEB 2.0 與其保安措施

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. 何謂 WEB 2.0?.....	3
II. WEB 2.0 的潛在保安威脅和考慮.....	4
高度參與文化帶來的威脅	4
有關 AJAX 的保安威脅	4
有關網站頻道 (WEB FEEDS) 的保安威脅	5
數據私隱和知識產權	5
對於互聯網資源的影響	5
III. 預防措施.....	6
對資訊科技從業者的保護	6
對終端用戶的保護	7
IV. 結論	9

摘要

Web 2.0 近來已經變成一個引人注目而又包羅萬有的名詞，用來形容不只是文字和非靜態的資訊發布網站。在 Web 2.0 的世界中，網頁變成人們創造和分享自己個人網上內容的平台，這些網上內容大多以網誌 (Blog)、影像或是照片的形式表示。許多網站也使用簡易資訊聚合 (Really Simple Syndication, RSS)，以供瀏覽者作為收集個人感興趣的新聞標題之彙總工具。為了使該平台更加方便使用和普及，人們被鼓勵經常瀏覽和發布那些網頁上的內容。如 MySpace 等受歡迎的社交網絡，或是如 YouTube 般的影像分享網站，皆是使用 Web 2.0 科技的主要例子。

然而，凡事有利也有弊。Web 2.0 帶來許多好處，例如使互聯網的內容更加豐富以及改善用家的體驗。與此同時也帶來了一些新的網上保安及攻擊方法的問題。本文討論 Web 2.0 所產生的潛在威脅，並且建議相關對策。

I. 何謂WEB 2.0?

Web 2.0 並沒有一個明確的定義。對許多人而言，這個名詞指的是特別的網上應用系統技術，以及集思廣益地利用互聯網去提供整合性互聯網服務給用戶，例如網誌(Weblogs) 和Wikis之類的網站。Web 2.0 大量依賴用戶的自發性充當發行人(user-as-publisher) 的互動模式運作，以及允許一群用戶推行他們所創造的內容。許多企業漸漸使用此技術來作為最佳的員工合作和溝通工具。O'Reilly列出了七個原則，以幫助分辨Web 2.0 應用系統的主要功能¹。近幾年逐漸出現許多Web 2.0 服務和網站，如 YouTube (<http://www.youtube.com>)、 Facebook (<http://www.facebook.com>)、 MySpace (<http://www.myspace.com/>) 等等。

¹ <http://www.oreilly.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html>

II. WEB 2.0 的潛在保安威脅和考慮

凡事都有正反兩面，Web 2.0 科技帶來了許多好處，例如內容豐富的網絡世界和改善用戶體驗，同時也產生了新的保安考慮和攻擊方法。因為 Web 2.0 應用系統的其中一樣特點，便是鼓勵更多用戶參與其中，使個人用戶或客戶面對保安威脅與漏洞的機率也提高了。以下是 Web 2.0 所帶來的常見保安威脅。

高度參與文化帶來的威脅

Web 2.0 讓人們能夠在各式各樣的合作平台上創造和主導內容，就像網誌和Wikis一樣。但是，基於互動模式的運作下，惡意濫用這些平台的可能性確實存在。這些平台可作為連結欺詐網站、惡性程式碼與其它類似間諜軟件（spyware）等保安威脅的發送點。攻擊者通常會利用個別開發者的社群和網站寄放內容之間的隱含信任關係，來損害個別用戶或是網站，舉例而言，一個存放在YouTube網站上的虛假影片檔，可能帶有Zlob特洛伊木馬，這類檔案影響無數的用戶²。因為網頁內容更新流程變得更加分散，所以確認發行者的真實性和可信賴程度，將會是主要的考慮。

另一個潛在威脅是企業資訊外洩。當員工透過網誌編寫和分享資訊或意見時，機構在控制何種資訊可以發布和是否可正式公布的問題上，將會變得更加困難。企業和顧客的敏感資料將可能被洩漏。此外，攻擊者可能會獲得有關企業的資料，並對機構進行社會工程攻擊（social engineering attack）。

有關AJAX的保安威脅

為了提供更豐富的用戶體驗，許多 Web 2.0 網站已經使用簡易的用戶界面編碼，例如非同步 JavaScript 和 XML（Asynchronous JavaScript and XML, AJAX）。在傳統的客戶/伺服器系統模式，主要的作業需求大多在伺服器端管理和處理。AJAX 則允許大部份的作業需求在客戶端處理。當探測和試驗應用系統的保安漏洞時，將會給予惡意用戶更多機會去修改客戶端的任何應用系統編碼。

因為 AJAX 可以跟許多網上服務聯繫，兩者之間的連接也藉此啟動，帶來額外的攻擊方法，即惡意用戶可隨意添加具敵意的內容。例如，AJAX 可用來擴大跨網址程式編程（XSS）攻擊的可能性，即惡意用戶試圖將病毒碼置入合法網站，從而誤導使用者和竊

² http://www.theregister.co.uk/2007/06/20/youtube_security/

取他們的資料。這不只讓攻擊者能夠竊取保密資訊，也讓他們可將惡性程式碼置入主機。

JavaScript 入侵攻擊已被提供保安機制的供應商列為新的網站漏洞類別。這類漏洞特別影響採納 Web 2.0 AJAX 的網絡應用系統³。透過這個漏洞，一個未經授權的用戶可以讀取包含在 JavaScript 中的保密資料。假如 JavaScript 是用於數據傳送模式，尤其是正在處理敏感和保密的資料時，應用系統便有可能受到攻擊。

有關網站頻道 (WEB FEEDS) 的保安威脅

在非集中式和內容分散的 Web 2.0 特性中，網站資訊透過如 RSS 和 Atom 等輕量企業協同組織規約 (lightweight syndication protocols) 散佈到其它網站。網站頻道讓用戶及網頁不需透過瀏覽該網站，便可以取得所需的內容標題和內文。要認證頻道項目之發行者的真實性，還未有標準的機制。如此一來，惡意攻擊者便可使用網站頻道將 JavaScript 置入 RSS，以便攻擊客戶端的瀏覽器。攻擊者所需做的是把手稿程式置入標準的 RSS 或是 Atom 中，例如 RSS 的標題、連結或描述式 XML 標籤。當終端用戶瀏覽這個特定的網站，並且透過 RSS 頻道下載網頁時，惡性程式碼便會被執行。

數據私隱和知識產權

另一個值得注意的論點是關於用戶的私隱和保護資料的權利。在早期的 Web 2.0 應用系統上，版權只是很寬鬆地執行。例如，亞馬遜網站 (Amazon) 宣稱對所有在該網站發表的文章之擁有權，但是在缺乏強制執行情況下，用戶也許可以在別處重複發表相同的文章。然而，當了解到數據控制可能是主要的競爭優勢，企業將會更努力地控制數據的接達與分佈。

對於互聯網資源的影響

AJAX 的廣泛使用也可能會影響網絡。使用 AJAX 科技可導致客戶端和伺服器之間頻繁 (非用戶啟動) 或持續的數據交換，任何在數據交換過程中的額外耽擱或數據損失，都可能對用戶產生影響。雖然 AJAX (和 AJAX 開發者) 會逐步改進來適應互聯網 (例如處理耽擱或背後的損失)，但是，與目前互聯網傳遞數據的品質比較，用戶也可能會要求更一致性和更可靠的網絡表現。現今，任何一致性網絡表現的需求通常符合互聯網規約 QoS 機制，但是在互聯網推行 QoS 會較在私人內部網絡上推行更加具挑戰性。未來也許會出現其他有趣的及引人關注的解決方案。

³ <http://www.securityfocus.com/news/11456>

III. 預防措施

之前提及的保安考慮，值得進一步討論必要的預防措施。以下將列舉一些預防措施。

對資訊科技從業者的保護

透過設計的保安措施

根據 Gartner 的說法，在系統開發周期（SDLC）整合最佳保安作業實務和工具時，不良的應用系統開發和缺乏監督將是 Web 2.0 開發者要面對的兩個最大保安議題。在 Web 2.0 衆多創新服務的潮流下，Web 2.0 應用系統的保安審計水準，也許跟傳統上以客戶為主的應用系統與服務有不同之處。

如同其它應用系統，保安考慮應被納入系統開發周期內的所有階段，尤其是推行適當的認證控制、輸入資料確認、和誤差處理控制等等。這些重要的控制和確認程序可以避免未經授權入侵的威脅。為了進一步確保推行適當的保護措施，在開發任何新的應用系統或是推出新程式之前，應該執行保安風險評估。

透過控制的保安措施

如前所述，Web 2.0 是著重以客戶為中心的應用系統。假如沒有實行適當的控制措施，系統便會面臨很大的威脅。為了建立互動和安全的 Web 2.0 應用系統，配搭適當控制的保安架構會是很重要的要素。這個架構的一些構成要素包括：

1. 在可信任架構中執行有效的對話管理機制，以確保認證和授權。
2. 在不同的階層中，於伺服器的兩端執行數據確認，以限制或預防植入隱蔽程式碼或是任何形式的攻擊。
3. 採用可信任的商業邏輯伺服器執行所有後端服務的作業需求。

透過開放式的保安措施

開放程式軟件或是 API 是在開放形式下開發的，它們通常都有較強的保安意識，因此，這類軟件通常有較多的內置保安措施。機構應採用已審核過的保安規約與業界標準，而不是使用私有的方法去推行保安措施。假如使用開放程式軟件或是 API，則應查核及確保該軟件的所有使用牌照是否有效，而且應及時修補這些解決方案已發表的漏洞。

關於 Web 2.0 的公司管治（Governance）

雖然目前 Web 2.0 服務大多存放於公共服務，即機構之外，管理部門仍需注意 Web 2.0 可能會影響到公司內部人員的風險，因這些公司內部人員擁有使用 Web 2.0 服務的權力。公司管理部門應訂立可以保護公司或是客戶敏感資料之政策，並確保這類資訊不會外洩在類似網誌的開放網站上。另外，應舉行定期保安認知培訓，以確保員工知道公司資訊科技保安政策，並加強有關這類新科技帶來之風險的保安意識。

爲了避免這些網站頻道所帶來的風險，只可信任從聲譽良好的來源所提供的資料頻道。對於提供網站頻道的應用系統開發者而言，應執行預防措施，例如將必要的 HTML 標籤列入白名單（white-listing）。此舉可降低網站頻道上 XSS 攻擊的可能性。

以下是資訊科技從業人員應該考慮的額外最佳作業實務：

1. 儘管 Wikis 可涵蓋較寬廣和更快速改進的標題，但是 Wikis 並沒有辦法防止錯誤的消息和匿名作者的出現，這些錯誤消息和匿名作者有可能對於已發表的消息進行惡意或是非授權的修改。當配置 Wikis 這類的應用系統時，應強制執行編輯控制，即應該限制只可更新合法和授權區域。也應執行適當的認證和接達控制，以確保內容的完整性。
2. 當使用網誌來傳達公司遠景，或用於其它促銷用途時，必須避免敏感或私人資料外洩，並應執行監控和過濾所有網誌內容。另外，應告知所有網誌用戶可接受的網誌使用政策。
3. 如同其它應用系統，Web 2.0 程式應通過完整的漏洞測試，以確認漏洞及發現其它弱點，這些漏洞包括惡意指令插入攻擊（command injection）、跨網址程式編程攻擊（cross-site scripting）和緩衝區滿溢攻擊（buffer overflow）。在推出應用系統之前，必須修正所有問題以及減低保安威脅。此外，應定期執行保安評估。

對終端用戶的保護

對於終端用戶而言，應遵守相關保安規例和政策，不應信任從可疑來源而來的網站頻道。爲了平衡保安功能，可限制JavaScript在瀏覽器上的使用，以避免惡性程式碼攻擊⁴。此外，也應採用抗電腦病毒產品供應商所建議的最新保安修補程式。

當編寫和發表網誌時，應該要保護個人資料和有關其它個人或機構的機密資料。舉例說，在沒有正當理由的情況下，不應透露電郵地址、手機號碼或是個人照片等個人資料。個人資料私隱專員公署也建議年輕人在網上發表文章時，應考慮將個人資訊發表在公共領域的風險。這樣便可以保護自己的資訊免受濫用或是用作非法活動的潛在危險⁵。如

⁴ http://www.cert.org/tech_tips/malicious_code_FAQ.html

⁵ http://www.pcpd.org.hk/english/infocentre/press_20070829.html

要在互聯網上揭露他人資料時，年輕人也應尊重其他人的私隱。

IV. 結論

Web 2.0 為網頁和互聯網帶來了嶄新的發展方向，然而，我們也需要考慮新的保安風險，尤其是攻擊者也許會將注意力從伺服器端轉移到客戶端，而客戶端通常強大的保安措施。

許多早期 Web 1.0 學到的保安經驗，可以應用到 Web 2.0 上。儘管 Web 2.0 日益增加的功能使保安風險也增加了，但應用在 Web 1.0 上的基本保安原則也可應用在 Web 2.0 上。

我們不應忽視和忽略應用系統的基本保安原則。在開發 Web 2.0 的初期，保安措施便應建置於 Web 2.0 應用系統內。在應用系統推出之前，應配置保安流程和控管監督在其中，也應實施周期性和持續性的保安風險評估，以確認和修補漏洞。管理部門、應用程式開發者和終端用戶皆須共同合作去迎接 Web 2.0 所帶來的挑戰。