OWASP 公布十大網頁應用程式的安全威脅

原文出處：THE H SECURITY (CERT 譯)
http://www.h-online.com/security/news/item/OWASP-top-ten-of-web-application-security-risks-released-1887663.html

開放網路安全研究計畫 OWASP 公布了它的十大最危險的網頁應用程式安全威脅。從 2010 年以來，這個組織認為，XSS 和 CSRF 攻擊有下降的趨勢，而個人簽證的破解和 session 管理過程則上升到第二名。同時，感染程式碼則重返排行榜的第一名。

OWASP 十大資安危險報告是在十年前首次發佈，而且受到網頁開發者和資安專家的高度重視。這份報告每三年發佈一次，且它的關注重心從以前的潛在漏洞方面轉移到一般資安威脅上。這份最新的報告從上百間公司中的數千個應用程式收集了超過 50 萬個漏洞。

OWASP 將危險的加密儲存和不足的傳輸層保護兩種分類合併為「敏感性資料外洩」，它指的是一般性資料外洩的資安問題。同樣的，2010 年報告中的「錯誤的有限 URL 連結」也被擴展為更具一般性的分類，也是更具功能性的連結控制，因為可以有很多種方式，並不只局限於 URL，去連結到一個現代網頁程式的功能層面。

一種全新的分類是有關管理者去使用一個已知的有漏洞的元件，像是程式庫、開發架構和開發樣板。在三年前的報告中，這是被分類在「資安錯誤管理」中，但是 OWASP 表示這種形式的問題已經日趨嚴重到必須新設一個分類出來了。

OWASP 公布十大網頁應用程式的安全威脅：

1. 程式碼感染（1）
2. 個人認證破解和 session 管理（3）
3. 跨網站攻擊程式（2）
4. 危險的直接性物件（4）
5. 資安錯誤管理（6）
6. 敏感性資料外洩（7/9）
7. 遺失的功能層面連結控制（8）
8. 跨網站偽造回應（5）
9. 使用已知危險元件（-）
10. 未經認證的間接流量和轉送流量（10）