

# OWASP Top 10

OWASP Top 10 – 2007 年版	OWASP Top 10 – 2010年版
A2 – Injection Flaws 注入弱點	↑ A1 – Injection 注入弱點風險
A1 – Cross Site Scripting (XSS) 跨站腳本攻擊	↓ A2 – Cross Site Scripting (XSS) 跨站腳本攻擊
A7 – Broken Authentication and Session Management 身分驗證缺陷與連線階段管理	↑ A3 – Broken Authentication and Session Management 身分驗證缺陷與連線階段管理
A4 – Insecure Direct Object Reference 不安全的直接物件參考	= A4 – Insecure Direct Object References 不安全的直接物件參考
A5 – Cross Site Request Forgery (CSRF) 跨站請求偽造	= A5 – Cross Site Request Forgery (CSRF) 跨站請求偽造
<2004 版 A10 – Insecure Configuration Management> 不安全的系統組態管理	+ A6 – Security Misconfiguration (新增) 錯誤或不安全的系統組態
A10 – Failure to Restrict URL Access 網址存取控制失當	↑ A7 – Failure to Restrict URL Access 網址存取控制失當
不在2007年版中	+ A8 – Unvalidated Redirects and Forwards (新增) 未驗證的轉址與轉送
A8 – Insecure Cryptographic Storage 不安全的加密儲存方式	↓ A9 – Insecure Cryptographic Storage 不安全的加密儲存方式
A9 – Insecure Communications 不安全的通訊方式	↓ A10 – Insufficient Transport Layer Protection 傳輸層保護不足
A3 – Malicious File Execution	- 不在2010年版，但仍然重要勿忽視
A6 – Information Leakage and Improper Error Handling	- 不在2010年版，但仍然重要勿忽視





資源回收筒



DAEMON Tools Lite



desktop.ini



FileCruiser



SAP Logon



資源回收筒



desktop.ini

伺服器管理員

檔案(F) 執行(A) 檢視(V) 說明(H)

伺服器管理員 (TTUXA02)

角色

功能

診斷

設定

存放

伺服器管理員 (TTUXA02)

取得這台伺服器的狀態概觀、執行上層管理工作，以及新增或移除伺服器角色與功能。

伺服器摘要

伺服器摘要說明

電腦資訊

變更系統內容

檢視網路連線

設定遠端桌面

設定伺服器管理員遠端管理

安全性資訊

移至 Windows 防火牆

設定更新

檢查新的角色

執行安全性設定指導

設定 IE ESC

角色摘要

角色摘要說明

上次重新整理時間: 今天 下午 01:20 設定重新整理

