Weak Server Side Controls

- 常見問題：
  - Injection
  - XSS
  - Broken Authentication and Session Management

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