附件 3－附錄 1 政府 Web 網站委外安全注意事項與安全檢核表

1. Web 應用程式的網路攻擊層出不窮

各機關目前委外開發之 Web 應用程式，在功能面與內容部分，大多能滿足民眾需求，惟在委外開發、購買及維護這類的應用程式方面，對於資安方面要求非常有限；近日有關 Web 應用程式的網路攻擊層出不窮，破壞技術與日俱增，影響日益嚴重；此外，個人資料保護法通過後，個人資料洩漏涉及的損害賠償責任很重，各機關透過網站公布的資訊常與個人資料相關，其資安控制措施如不加強，未來將面臨巨大挑戰。

2. 對 Web 應用程式安全漏洞的了解不足

鑑於網路技術發展日新月異，各機關資安工作的負擔日益沉重，在人力有限的情形下，對於 Web 應用程式安全漏洞的了解與相關的防範技術能力可能有所不足，因此特就 OWASP(Open Web Application Security Project - OWASP)所提供之開放原始碼計畫，各地分會製作出免費、公正、開放來源文獻之工具與標準，提供各機關參考。

3. 常見最嚴重的 Web 應用程式十大漏洞與安全對策

OWASP 公布常見最嚴重的十大漏洞與風險，請詳見 https://owasp.org/Top10/zh_TW/ 說明

OWASP 十大漏洞都是我們常見會發生的設定或設計上的錯誤，其中有許多必須由程式開發者與網站管理者共同研擬對策才能避免，因此兩者從程式開發階段就必須緊密的合作。

4. 風險管理

有些風險並非程式漏洞所造成的，例如「阻絕服務攻擊」是屬於一種網路

攻擊行為，與應用程式安全與否無關，但對於提供網路服務確實是一項系統的風險。而「政府資訊作業委外安全參考指引」內容系依照 CNS27001 標準在整體安全風險的管理上著墨，故「政府資訊作業委外安全檢核表」著重於管理面的檢核，適用於各類委外服務。

但是所有在網路上提供便民服務的資訊系統，均會面對來自網際網路的各種風險，屬於系統發展類的軟體開發或系統整合案，無論系統大小或機密等級高低，招標過程大同小異，委外作業所要管理的風險差異不大，故難以依照系統之機密(防護)等級區分。

5. web **應用程式安全檢核**

為便於機關掌握 Web 應用程式安全檢核重點，篩選出具實務意義的重要控制措施項目共 75 項，依據系統安全等級區分「普」、「中」及「高」3 個等級，列舉適用的控制措施項目，方便各機關在辦理 web 應用程式委外開發時，依據系統的安全強度，要求廠商(或第三方)執行不同程度的檢核，控制措施詳細內容請參閱「Web 應用系統安全參考指引」，該指引亦針對各控制措施以市面上常見之程式語言 ASP.NET、PHP 及 Java 提供範例。檢核內容詳見表 1「Web 應用程式安全檢核表」。

表1　Web 應用程式安全檢核表

Web 應用程式安全檢核表						
控制措施	類別	實作項目	適用分級			是否符合
			普	中	高	
存取	帳號管理	使用者的會談階段，設定該帳號在合理的時間(至多 30 分鐘)內未活動即自動失效	◎	◎	◎	

控制		使用者的會談階段在登出後失效	◎	◎	◎	
		管理者介面限制存取來源或不允許遠端存取	◎	◎	◎	
	最小權限	對使用者/角色，僅賦予所需要的最低權限		◎	◎	
		軟體程序(process)及伺服器服務，以一般使用者權限執行，不以系統管理員或最高權限		◎	◎	
	遠端存取	採用伺服端的集中過濾機制檢查使用者授權	◎	◎	◎	
稽核與可歸責性	稽核事件	針對身分鑑別失敗、存取資源失敗、重要行為、重要資料異動、功能錯誤及管理者行為進行日誌記錄	◎	◎	◎	
		應稽核資訊系統管理者帳號所執行之各項功能	◎	◎	◎	
	稽核紀錄內容	日誌紀錄包含以下項目 1.識別使用者之ID(不可為個資類型)。2.經系統校時後的時間戳記。3.執行的功能或存取的資源。4.事件類型或等級(priority)。5.事件描述	◎	◎	◎	
		採用單一的日誌紀錄機制，確保輸出格式的一致性	◎	◎	◎	
	稽核儲存容量	依據稽核紀錄儲存需求，配置稽核紀錄所需之儲存容量	◎	◎	◎	
	稽核處理失效之回應	資訊系統應在稽核處理失效(如儲存容量不足)之情況下，採取適當之行動，例如：關閉資訊系統、覆寫最舊的稽核紀錄或停止產生稽核紀錄等。	◎	◎	◎	

		當機關規定需要即時通報的稽核失效事件發生時，資訊系統應在機關規定之時效內，對機關特定之人員、角色提出告警(適用於高等級)			◎	
	時戳	資訊系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對映到世界協調時間(UTC)或格林威治標準時間(GMT)	◎	◎	◎	
		系統內部時鐘應具備定期同步機制	◎	◎	◎	
	稽核資訊之保護	對日誌紀錄進行適當保護及備份，避免未經授權存取	◎	◎	◎	
		定期備份稽核紀錄到與原稽核系統不同之實體系統 (如 Log 伺服器)	◎	◎	◎	
		重要系統資料或紀錄留存雜湊值以確保完整性			◎	
營運持續計畫	資訊系統備份	重要資料定時同步至備份或備援環境，並加以保護限制存取	◎	◎	◎	
	資訊系統備援	採用「高可用性」(High Availability)架構(分散式或叢集伺服器架構)			◎	
識別與鑑別	內部使用者之識別與鑑別	採用多重因素身分鑑別(兩種以上驗證類型)			◎	
		資訊系統在建立連線前，應識別允許存取之特定來源(如 IP)			◎	
	身分鑑別管理	確實規範使用者密碼強度(密碼長度 12 個字元以上、包含英文大小寫、數字，以及特殊字元)	◎	◎	◎	
		使用者必須定期更換密碼，且至少不可以與前 3 次使用過之密碼相同	◎	◎	◎	

		具備帳號鎖定機制，帳號登入進行身分鑑別失敗達 5 次後，至少 15 分鐘內不允許該帳號及來源 IP 繼續嘗試登入	◎	◎	◎	
		身分鑑別相關資訊不以明文傳輸	◎	◎	◎	
		採用圖形驗證碼(CAPTCHA)機制於身分鑑別及重要交易行為，以防範自動化程式之嘗試		◎	◎	
		密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性令牌(Token)，檢查傳回令牌有效性後，才允許使用者進行重設密碼動作		◎	◎	
	鑑別資訊回饋	資訊系統應遮蔽在鑑別過程中之資訊(如密碼)，以防止未授權之使用者可能之窺探/使用	◎	◎	◎	
	加密模組鑑別	密碼添加亂數(Salt)進行雜湊函式(HASH Function)處理後，分別儲存亂數及雜湊後密碼		◎	◎	
系統與服務獲得	安全系統發展生命週期需求階段	針對系統安全需求，以檢核表方式進行確認	◎	◎	◎	
	安全系統發展生命週期設計階段	應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估		◎	◎	
		將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正		◎	◎	
	安全系統發展生命週期開發階段	具有防範 SQL 命令注入攻擊(SQL Injection)之措施	◎	◎	◎	
		具有防範跨站腳本攻擊(XSS, Cross-Site Scripting)之措施	◎	◎	◎	
		具有防範「跨站請求偽造」(Cross-Site Request Forgery, CSRF)攻擊之措施	◎	◎	◎	

		發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細的錯誤訊息	◎	◎	◎	
		所有功能皆進行錯誤及例外處理，並確保將資源正確釋放	◎	◎	◎	
		具備系統嚴重錯誤之通知機制(例如電子郵件或簡訊)			◎	
	安全系統發展生命週期測試階段	執行「弱點掃描」安全檢測	◎	◎	◎	
		執行「滲透測試」安全檢測			◎	
	安全系統發展生命週期部署與維運階段	作業平台定期更新並關閉不必要服務及埠口(Port)	◎	◎	◎	
		針對系統依賴的外部元件或軟體，注意其安全漏洞通告，定期評估更新	◎	◎	◎	
		系統依賴的外部元件或軟體，不使用預設或空的密碼	◎	◎	◎	
	安全系統發展生命週期委外階段	資訊系統開發若委外服務應將系統發展生命週期各階段依安全等級將安全需求納入委外合約	◎	◎	◎	
	獲得程序	開發、測試以及正式作業環境應作區隔		◎	◎	
	資訊系統文件	應儲存與管理系統發展生命週期之相關文件	◎	◎	◎	
系統與通訊保護	傳輸之機密性與完整性	機敏資料傳輸時，採用加密機制		◎	◎	
		使用公開、國際機構驗證且未遭破解的演算法			◎	
	資料儲存之安全	參數設定或系統設定存放處，限制存取或進行適當保護			◎	
		機敏資料儲存時，採用加密機制			◎	
系統	資訊系統監控	發現資訊系統有被入侵跡象時，應通報機關特定人員	◎	◎	◎	

與資訊完整性		監控資訊系統，以偵測攻擊和未授權之連線，並識別資訊系統之未授權使用		◎	◎	
		資訊系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時針對該事件進行分析			◎	
	軟體及資訊完整性	於伺服器端以正規表示式(Regular Expression)方式，檢查使用者輸入資料合法性		◎	◎	

資料來源： 本計畫整理