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			適	用分	級	是		
制	<i>y</i> = -1	ウルエロ				否		
措	類別	實作項目	普	中	高	符		
施			1	'	. •	合		
<i>t</i>	帳號管理	使用者的會談階段,設定該帳號在合理	0	0	0			
存		的時間(至多30分鐘)內未活動即自動						
取		失效						

控		使用者的會談階段在登出後失效	0	0	0	
制		管理者介面限制存取來源或不允許遠端	0	0	0	
		存取				
	最小權限	對使用者/角色,僅賦予所需要的最低		0	0	
		權限				
		軟體程序(process)及伺服器服務,以一			0	
		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	0	0	0	
		授權				
	稽核事件	針對身分鑑別失敗、存取資源失敗、重	0	0	0	
		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	0	0	0	
		項功能				
	稽核紀錄內	日誌紀錄包含以下項目 1.識別使用者之	0	0	0	
稽	容	ID(不可為個資類型)。2.經系統校時後				
核		的時間戳記。3.執行的功能或存取的資				
與		源。4.事件類型或等級(priority)。5.事				
可		件描述				
歸		採用單一的日誌紀錄機制,確保輸出格	0	0	0	
責性		式的一致性				
江	稽核儲存容	依據稽核紀錄儲存需求,配置稽核紀錄	0	0	0	
	量	所需之儲存容量				
	稽核處理失	資訊系統應在稽核處理失效(如儲存容	0	0	0	
	效之回應	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			0	
		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	0	0	0	
		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	0	0	0	
	稽核資訊之	對日誌紀錄進行適當保護及備份,避免	0		0	
	保護	未經授權存取				
		定期備份稽核紀錄到與原稽核系統不同	0	0	0	
		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			0	
		完整性				
營	資訊系統備	重要資料定時同步至備份或備援環境,	0	0	0	
運	份	並加以保護限制存取				
持	資訊系統備	採用「高可用性」(High Availability)			0	
續	援	架構(分散式或叢集伺服器架構)				
計						
畫						
	內部使用者	採用多重因素身分鑑別(兩種以上驗證			0	
	之識別與鑑	類型)				
識	別	資訊系統在建立連線前,應識別允許存			0	
別		取之特定來源(如 IP)				
與	身分鑑別管	確實規範使用者密碼強度(密碼長度 12	0	0	0	
鑑	理	個字元以上、包含英文大小寫、數字,				
別		以及特殊字元)				
		使用者必須定期更換密碼,且至少不可	0	0	0	
		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	0	0	0	
		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	0	0	0	
		採用圖形驗證碼(CAPTCHA)機制於身		0	0	
		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		0	0	
		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	資訊系統應遮蔽在鑑別過程中之資訊	0	0	0	
	饋	(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	密碼添加亂數(Salt)進行雜湊函式		0	0	
	別	(HASH Function)處理後,分別儲存亂				
		數及雜湊後密碼				
	安全系統發	針對系統安全需求,以檢核表方式進行	0	0	0	
	展生命週期	確認				
	需求階段					
系	安全系統發	應根據系統功能與要求,識別可能影響		0	0	
統	展生命週期	系統之威脅,進行風險分析與評估				
與	設計階段	將風險評估結果回饋需求階段的檢核項		0	0	
服		目,並提出安全需求修正				
務	安全系統發	具有防範 SQL 命令注入攻擊(SQL	0	0	0	
獲	展生命週期	Injection)之措施				
得	開發階段	具有防範跨站腳本攻擊(XSS, Cross-Site	0	0	0	
		Scripting)之措施				
		具有防範「跨站請求偽造」(Cross-Site	0	0	0	
		Request Forgery, CSRF)攻擊之措施				

 餐生錯誤時,使用者頁面僅顯示簡短錯 ② ③ ③ ③ ④ 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 安全系統發展生命週期部別談階段 安全系統發展生命週期部別談階段 安全系統發展生命週期所不必要服務及原生命週期所不必要服務及原生命週期所不必要服務及原生命週期所不必要服務及原生命週期所不必要服務及原生命週期所不必要服務及度的密碼。 安全系統發度度生命週期所不必要服務及度或全的密碼。 安全系統發度度生命週期方式件或軟體,在使用預算的不使或空的密碼。 安全系統發度度生命週期度的分析。 安全系統發度度生命週期度的方式。 政立室的密码。 資訊系統文度的經過數學的學問數學的學問數學的學問數學的學問數學的學問數學的學問的學問,不使用預算的學的學的學的學的學的學的學的學的學的學的學的學的學的學的學的學的學的學的學		T		1		ı	
所有功能皆進行錯誤及例外處理,並確 ◎ ◎ ◎ ◎ ◎ □ □ □ □ □ □ □ □ □ □ □ □ □ □			發生錯誤時,使用者頁面僅顯示簡短錯	0	0	0	
			誤訊息及代碼,不包含詳細的錯誤訊息				
具備系統嚴重錯誤之通知機制(例如電 字郵件或簡訊) 安全系統發 執行「弱點掃描」安全檢測			所有功能皆進行錯誤及例外處理,並確	0	0	0	
子郵件或簡訊) 安全系統發 執行「弱點掃描」安全檢測 執行「滲透測試」安全檢測 測試階段 安全系統發 作業平台定期更新並關閉不必要服務及 ◎ ◎ ◎ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □			保將資源正確釋放				
安全系統發 展生命週期 測試階段			具備系統嚴重錯誤之通知機制(例如電			0	
展生命週期 測試階段 安全系統發 展生命週期 部子のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、いいいは、ないは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、大学・のでは、いいは、いいは、いいは、いいは、いいは、ないは、ないは、ないは、いいは、いい			子郵件或簡訊)				
測試階段 安全系統發 展生命週期 部署與維運 特旦(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 機生命週期各階段依安全等級將安全需求 委外階段 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 文件 係 傳輸之機密 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 裁進行適當保護 機敏資料儲存時,採用加密機制 ⑥ □		安全系統發	執行「弱點掃描」安全檢測	0	0	0	
測試階段 安全系統發 作業平台定期更新並關閉不必要服務及 ◎ ◎ ◎ ◎ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		展生命週期	執行「滲透測試」安全檢測			0	
展生命週期 部署與維運 階段 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,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 相發、測試以及正式作業環境應作區隔 資訊系統文 傳輸之機密 機繳資料傳輸時,採用加密機制 通 資料儲存之 安全 裁數資料儲存時,採用加密機制		測試階段					
部署與維運 階段		安全系統發	作業平台定期更新並關閉不必要服務及	0	0	0	
 階段 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 ② ② ③ 設或空的密碼 安全系統發展生命週期各階段依安全等級將安全需求委外階段 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 ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ②		展生命週期	埠口(Port)				
系統依賴的外部元件或軟體,不使用預 ② ② ③ ② ② ② ② ② ② ② ② ③ ③ ③ ③ ③ ② ② ② ② ③ ② ③ ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ② ②		部署與維運	針對系統依賴的外部元件或軟體,注意	0	0	0	
設或空的密碼 安全系統發 資訊系統開發若委外服務應將系統發展 ◎ ◎ ◎ ◎ ◎ 《 《 《 《 《 《 》 》 《 》 》 《 《 》 》 《 》 《		階段	其安全漏洞通告,定期評估更新				
安全系統發 廣訊系統開發若委外服務應將系統發展 生命週期 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 ① ② ② (系統依賴的外部元件或軟體,不使用預	0	0	0	
展生命週期 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 ② ② (設或空的密碼				
委外階段 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 〇 資訊系統文件 應儲存與管理系統發展生命週期之相關 〇 系傳輸之機密性與完整性與完整性與完整性與完整性與完整性與完整性與完整性的與實質法 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 〇 機般資料儲存時,採用加密機制 〇		安全系統發	資訊系統開發若委外服務應將系統發展	0	0	0	
獲得程序 開發、測試以及正式作業環境應作區隔		展生命週期	生命週期各階段依安全等級將安全需求				
資訊系統文 應儲存與管理系統發展生命週期之相關 ◎ ◎ ◎ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○		委外階段	納入委外合約				
件 文件 系 傳輸之機密 機敏資料傳輸時,採用加密機制 ⑥ 統 性與完整性 使用公開、國際機構驗證且未遭破解的 演算法 ⑥ 通 資料儲存之 參數設定或系統設定存放處,限制存取 或進行適當保護 ⑥ 保 機敏資料儲存時,採用加密機制 ⑥		獲得程序	開發、測試以及正式作業環境應作區隔		0	0	
 (傳輸之機密		資訊系統文	應儲存與管理系統發展生命週期之相關			0	
 統性與完整性 使用公開、國際機構驗證且未遭破解的 演算法 通 資料儲存之 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 ◎ 		件	文件				
與 演算法 演算法	系	傳輸之機密	機敏資料傳輸時,採用加密機制		0	0	
與 演算法 通 資料儲存之 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 機 機敏資料儲存時,採用加密機制	統	性與完整性	使用公開、國際機構驗證且未遭破解的			0	
部 安全 或進行適當保護 機敏資料儲存時,採用加密機制 ◎	與		演算法				
訊 安全 或進行適當保護 機敏資料儲存時,採用加密機制 ◎	通	資料儲存之	參數設定或系統設定存放處,限制存取			0	
護	訊	安全	或進行適當保護				
護	保		機敏資料儲存時,採用加密機制			0	
系 資訊系統監 發現資訊系統有被入侵跡象時,應通報 ○ ○ ○	頀						
	系	資訊系統監	發現資訊系統有被入侵跡象時,應通報	(0	0	
統 控 機關特定人員	統	控	機關特定人員				

與		監控資訊系統,以偵測攻擊和未授權之	0	0	
資		連線,並識別資訊系統之未授權使用			
訊		資訊系統應採用自動化工具監控進出之			
完		通信流量,並於發現不尋常或未授權之			
整		活動時針對該事件進行分析			
性	軟體及資訊	於伺服器端以正規表示式(Regular	0		
	完整性	Expression)方式,檢查使用者輸入資料			
		合法性			

資料來源: 本計畫整理