零售業《能力標準說明》能力單元

「網站監測及測試技術」職能範疇

名稱	執行安全測試
編號	107250L5
應用範圍	在網站測試中，對網站進行安全體系測試、應用及傳輸安全測試，以保證網站的正常運行。
級別	5
學分	6（僅供參考）
能力	表現要求 1. 瞭解安全測試的要求 • 明白安全測試的要求，如部署與基礎結構、輸入驗證、身份驗證、授權、配置管理、敏感性資料、會話管理、加密、參數操作、異常管理等 2. 掌握安全體系測試 • 進行基礎結構測試，如網路是否提供了安全的通信、內部的防火牆、遠端應用程式伺服器、目標環境的信任級別 • 評估應用程式是否易受SQL注入、XSS等攻擊 • 檢定是否區分公共訪問和受限訪問、是否明確服務帳戶要求、如何驗證調用者身份、如何驗證資料庫的身份、是否強制試用帳戶管理措施 • 制訂是否支援遠端系統管理、是否保證配置存儲的安全、是否隔離管理員特權 • 設置是否存儲機密資訊、如何存儲敏感性資料、是否在網路中傳遞敏感性資料、是否記錄敏感性資料 • 進行異常管理，如是否使用結構化的異常處理、是否向用戶端公開了太多的資訊 • 審核和分析日誌記錄，如是否明確記錄了要審核的活動、分析註冊與登入的活動 • 檢查伺服器端的腳本漏洞 3. 展示專業能力 • 確保網站安全測試，不會影響相關網站的功能及性能 • 確保網站安全測試，符合相關法例的要求
評核指引	此能力單元的綜合成效要求為： • 能夠掌握網站安全體系測試的知識 • 能夠運用網站安全體系及傳輸安全測試的方法
備註	