網站資訊安全技術報告

指導教授：陳鍾誠

學生：資工四 110910560 羅德耕

一、常見的網站資訊安全威脅

- 跨站腳本攻擊 (XSS): 攻擊者在網站中注入惡意腳本，當用戶訪問時，此腳本會在用戶瀏覽器中執行，導致用戶資料泄露。
- SQL 注入: 攻擊者通過在網站輸入欄位中提供惡意 SQL 語句，宜設取得資料庫的資料。
- 跨站請求僞逮 (CSRF): 讓用戶在未授權的情況下，執行變更密碼或金融交易等操作。
- 分散式阻斷服務攻擊 (DDoS): 攻擊者起用大量請求，使網站資源而府，以阻斷服務提供。

二、網站資訊安全技術與防護措施

- 內容安全政策 (CSP): 安全裁置規定可製作的源，限制網頁載入非信任內容，以防止 XSS 攻擊。
- 輸入驗證與參數化查詢: 對用戶輸入進行驗證，將查詢與用戶資料分離，防止 SQL 注入攻擊。
- 密碼化請求與繁例化: 加入唯一的請求認證碼，保證 CSRF 攻擊不能成功。
- DDoS 防禦: 安裝防火牆和流量監控，使用 CDN 來分散請求，增強抗攻擊能力。

三、資訊安全技術的實施與挑戰

- 新舊威脅和設備細節: 因物聯網 (IoT) 設備增加，網站處理的訊息量也增加，專業的安全設備在實現中角色重要。
- 人工智能和混合攻擊: AI 可能被攻擊者添加帶有惡意的模型，帶來新型威脅。
- 安全總覽和維護: 持續進行安全評估和更新安全策略，才能保持長期安全。

四、資料出處

- 國家資通安全研究院技術報告：linkFortinet
- 安全報告：linkTrend Micro
- 主題訊息：link
- 主流研究文章：arxiv.org
- 由ChatGPT協助整理