一、指導老師：王德譽

二、組　員：王昱佑（11227098）、林楷博（11227111）、陳逸賢（11227079）

三、系統環境：

軟體：

- 系統與部署：AlmaLinux、Kali Linux、KVM、Tailscale。
- 網站與資料庫：Nginx、PHP-FPM、MariaDB。
- 攻防工具：ModSecurity、OWASP CRS、Fail2ban、Hydra。
- 日誌與監控：Promtail、Loki、Grafana。

硬體：承載虛擬環境電腦、操作與展示用電腦。

通訊設備/協定：HTTP、SSH

四、系統功能與特色：

(一)功能

1. 資安攻防情境實作

(1) 提供 Stored XSS 情境，展示惡意內容儲存後對網頁造成的影響。

(2) 提供多組 SQL Injection 案例，觀察不同輸入如何改變資料查詢結果。

(3) 透過密碼字典攻擊測試，展示 Fail2ban 的來源封鎖與解除封鎖功能。

2. 日誌查詢與事件判讀

(1) 查閱事件時間、來源、規則及處理狀態，理解各項紀錄的用途。

(2) 切換 Web 防禦模式，對照操作結果與日誌，辨識偵測及阻擋的差異。

(3) 結合 SQL 查詢紀錄、圖表資料，練習追蹤及核對事件。

(二)特色

本專題以攻防實作作為資安學習入口，適合資安入門至具基礎操作能力的使用者。系統透過具體情境、模式切換及結果觀察，協助使用者理解漏洞效果與防禦處理，並將日誌判讀融入操作流程。

使用者可從頁面反應出發，查找對應紀錄，再核對規則命中、查詢結果及封鎖狀態，理解系統如何處理事件。透過操作、觀察與查證，逐步建立日誌閱讀及以證據解釋攻防結果的能力。