應用程式資訊安全防護

課程綱要

PART 1｜威脅與攻擊

- 進階持續威脅攻擊竊取機密資料
- 分散式阻斷服務攻擊癱瘓網路運作
- 物聯網設備資安弱點威脅升高
- 網路與經濟罪，犯影響電子商務與金融運作
- 資訊供應商持續遭駭破壞供應鏈安全

PART 2｜安全應用程式

- 說明OWASP資訊安全規範
- 說明OWASP資訊攻擊的防範方式
- 不同應用系統如何規劃OWASP

PART 3｜鑑別與授權

- 驗證與授權的架構與意義
- 網站系統如何進行驗證模式與授權架構
- IoT物連網服務如進行驗證與授權

PART 4｜加密技術

- 驗證與授權的架構與意義
- 網站系統如何進行驗證模式與授權架構
- IoT物連網服務如進行驗證與授權

PART 5｜Session 管理說明

- Session使用重點與方式說明
- 網站應用系統Session配合的Cookie如何應用
- Cookie安全性注意事項

PART 6｜安全編碼

- SQL Injection防範
- XSS如何防範
- 資訊加密與雙重驗證規則

PART 7｜Open API安全設計

- 說明RESTful API如何進行API KEY驗證
- 實作如何傳遞Token以及其種類差異
- LINE Bot實作說明

PART 8｜安全與維護

- 系統如何部署與策略設計
- 硬體與機房管制措施
- 災難防護作業