Subject 校外研習分享-「資安鑑識課程-系列 I 初級課程：網站應用程式安全與資安風險分析」

圖資處資訊服務組 / 毛政仁 謝宗諭

毛政仁研習心得

應用程式安全是一個廣泛的主題，範圍涵蓋網頁、行動應用程式和應用程式開發介面(API)的軟體漏洞。這些漏洞可能出現於使用者的驗證或授權流程、程式碼和組態的完整性，以及成熟的政策與程序之中。應用程式漏洞可能成為重大資安外洩事件的引信。應用程式安全是資安外圍防禦的重要一環。

在本次課程中，講師以案例網站常見事件為起頭，說明對應的防禦機制，並且以駭客角度來審視什麼樣的網站容易成為目標，與個人業務相關性極大，因此受益良多，課程中有以實際操作方式教導駭客如何攻擊、破解方式等等，知悉了許多平常不會注意到的小細節與防護方式。除了要定期對已知漏洞進行第一時間防護，且要定期進行弱點掃描，檢查程式及系統的版本。落實平常的每一細節，才可將端點資安風險降到最低。

最後老師講到提到跨網站指令碼(Cross-site scripting，通常簡稱為XSS)以及SQL攻擊(SQL injection)，簡稱隱碼攻擊，皆屬於是發生於應用程式之資料庫層的安全漏洞。由於程式設計不良或缺失導致，如何設計出優良無缺陷的程式，此為身為資訊服務組人員最重要的課題，亦是今後努力的目標。

謝宗諭研習心得

隨著網路與行動裝置不斷發展進步，網站安全維護已不再像以前一般只要保護好自己的網站就好，在程式工程師及網頁設計師開發web-based網路應用程式時，需要避免因撰寫程式時產生的bug讓使用者在不經意的情況下觸發，導致網站或整體資安營運出現問題。

在本次課程中，講師以案例網站常見事件為起頭，說明對應的防禦機制，並且以駭客角度來審視什麼樣的網站容易成為目標，推薦常用的分析工具。由於部分工具可入侵網站尋找弱點，講師特別強調分析工具能做好事，但同時也會帶來對應風險，尤其入侵網站部分絕對不能隨意找尋網路上的對象，必須要以自己的測試網站來實行。

目前大部分的網路應用程式皆與網站服務有關，尤其是有對外服務的網站更具有高風險。如果網站在沒有任何防護的情況下連接上網路，駭客最快可在35秒便完成入侵，不僅可盜取網站資料，還能讓該網站成為跳板攻擊其他網站。在駭客思維中，沒有百分之百安全的網站架構，因此程式工程師要執行嚴密的上線前測試，針對目前的已知漏洞進行第一時間防護，並且要定期進行弱點掃描，檢查程式及系統的版本。

最後講師以OWASP TOP 10 (2017年版)總結課程，OWASP (Open Web Application Security Project)為指標性機構，收集各種網頁安全漏洞，推動世界軟體的安全性，歸納出容易攻擊的弱點並彙整為十大資安問題及防範措施。藉由了解網站風險排名，可檢視本校網站是否能防範最可能發生的攻擊，進而保護資料安全。