聽了有關資訊安全的演講後，讓我了解資訊安全的三個核心:機密性、完整性和可用性稱為C.I.A.，機密性指的是訊息不能被其他不應該獲得的人所取得，提供用戶資料的保密，完整性是儲存資訊的過程中，資料不會被未授權的篡改，可用性是讓一個系統是一個可隨時工作的狀態。除了這些之外我也了解了authentication、authorization和accounting稱作(AAA)、第一個意思是透過什麼方式來證明自己真的是被宣稱的人，第二個是透過something you know , something you have, something you are來給你對應的權限，最後Accounting 是記錄使用者做了什麼事情，因為這次的演講我才能真正了解這幾三個詞的意思。再來是探討了資安的風險在哪裡，還沒聽演講時只覺得如果我的帳號密碼外洩了才會有資安風險，但是這次聽完才發現要有 資產、威脅、漏洞這三個一起才會造成資安風險，資產通常會面臨不同種類的威脅，如果有了漏洞就可能會造成威脅，會有資安風險就是因為有漏洞。但是有了風險也需要考量到造成的影響是否大或小，如果影響大那我們一定得去處理，如果小的話我們就不用急著要去做處理，所以風險的公式是“機率去乘上影響”，當發生的機率小但是造成的影響大以及發生的機率大但是造成的影響小等等例子。而在資訊安全的機率表示著攻擊難度的高低、弱點是否常見、弱點容不容易被發現等等，影響則是代表考量弱點對機密性、一致性、可用性等的影響。最後是OWASP Top 10 的A01權限控制失敗、A02 加密機制失效、A03 注入式攻擊、A04不安全設計、A05 安全設定缺陷、A06危險或過舊的原件、A07認證及驗證機制失效、A08軟體及資料完整性失效、A09資安紀錄及監控失效和A10伺服器請求偽造(SSRF)，其中我有特別去注意注入式攻擊因為很常聽到SQL Injection，當一個網站有帳號密碼必須輸入時，攻擊者可能會先輸入user/user，當系統回傳一個密碼錯誤代表攻擊者能知道有user這個帳號，所以攻擊者可能會在密碼輸入’||’1，因為or後面是1讓整個條件變為真，所以攻擊者可以繞過密碼認證，成功登入目標的帳號。因此要防範這種問題可以使用正規表達式過濾輸入值將單引號換成雙影號避免以上的方法可以進入系統。聽完這次的演講我覺得資訊安全這一塊也挺有趣的，之前其實就對網路攻防戰很有興趣，而且剛好就是在資訊安全這個領域，這次剛好也補充到一些很基本得小知識。