新北市政府教育局
資通系統之資安議題

講師：葉益禎

中華民國111年11月22日

課程大綱

序號	大綱
一	近期資安事件及實例分析
二	資安法對於資通系統之要求
三	如何撰寫安全的資通系統
四	問題與討論

近期資安事件及實例分析

長沙銀行系統漏洞被利用 罪犯開設4萬異常賬戶賺16萬

北京新浪網 (2022-02-16 16:58)

2019年2月間，被告人尚某等人將內含公民身份證號碼、姓名、手機號碼等信息內容及串碼、一個固定銀行卡號、Fiddler應用程序軟體提供給被告人司某、劉某，利用Fiddler應用程序軟體能夠攔截由長沙銀行伺服器向長沙銀行APP發送的數據校驗結果、加掛銀行卡信息、審核狀態信息並加以修改的技術功能，使以相關公民身份提出的開設長沙銀行線上II類銀行賬戶(以下簡稱II類戶)的申請在缺少「視頻審核的業務流水號」、「證件上傳成功」、「生成的視頻流水號」等驗證環節的情況下能夠通過電子渠道開設長沙銀行II類戶，所開設的長沙銀行II類戶雖不能正常使用但可用以作為綁定賬戶開立具有辦理限額消費和繳費、限額向非綁定賬戶轉出資金等功能的他行III類戶。其中被告人劉某以此方法開設了80個長沙銀行II類賬戶，獲取錢款人民幣160元。

Safari爆重大漏洞，帳號密碼、照片恐外洩

2022.01.18 風傳媒

隨著網路普及率愈來愈高，資安問題成為網路安全隱患。近來蘋果iOS 15、iPadOS 15的瀏覽器Safari被爆出現重大漏洞，使用者帳密等個人資訊恐遭駭客盜取，**不管是iPhone、Mac的用戶都受到影響，而在蘋果官方更新前，僅有1方法可以自保！**

Safari瀏覽器爆重大漏洞，快取消「這設定」自救

瀏覽器指紋辨識服務業者「FingerprintJS」發布文章表示，蘋果iOS 15、iPadOS 15的瀏覽器Safari出現程式錯誤，導致使用者的即時上網資訊遭到洩露，而這項程式錯誤發生在「IndexedDB」資料庫工具，也就是用於客戶端存儲的瀏覽器。

Log4j重大安全漏洞

CVE-2021-44228

一個被全世界廣泛使用的軟體「Log4j」出現重大安全漏洞，資安公司Tenable警告是這十年以來最嚴重的單一漏洞，駭客可能藉此直接進入網頁伺服器存取資料，甚至遠端遙控伺服器。微軟則表示，追蹤到中國、伊朗、北韓、土耳其等國家政府支持的駭客團體，試圖透過這個漏洞發動攻擊。

由於Log4j是一個基於Java程式語言設計的軟體，因此所有以Java為基礎的App和伺服器都有可能因為這個漏洞而遭遇駭客攻擊。目前確認容易被鎖定的公司包括蘋果、亞馬遜、推特、百度、騰訊、特斯拉、IBM等知名企業。

SQL Server重大安全漏洞

南韓資安業者AhnLab本周警告，最近有一波Cobalt Strike攻擊行動鎖定的是尚未修補的SQL Server安全漏洞，或者是透過暴力破解與字典攻擊以取得SQL Server的存取憑證。

Cobalt Strike為一款商業化的滲透測試軟體，通常作為模擬入侵攻擊的紅隊演練之用，駭客則經常濫用它來滲透目標對象，進而安裝勒索軟體，或是潛伏於組織中竊取資訊，該軟體預設的惡意程式酬載稱為Beacon，亦肩負與C&C伺服器通訊的責任。

AhnLab說明，駭客先掃描1433傳輸埠，以辨識那些開放的SQL Server，再進行暴力破解或字典攻擊，取得憑證後再安裝Lemon Duck等挖礦工具，同時植入Cobalt Strike作為伺服器的後門，以便永久存在於受害者組織內並進行橫向移動。 CVE-2021-36798

Windows作業系統零時差漏洞

- 微軟旗下的作業系統Windows近期爆出最新的零時差漏洞，只要駭客取得擁有部分登入全的用戶帳號，就可以透過這個漏洞將自己升級為電腦管理員，進而在短時間內掌控目標電腦。而這個漏洞涵蓋所有版本的Windwos作業系統，其中也包含現行熱門的Windwos 11、Windows 10與Windows Server 2022
- 資安人員Abdelhamid Naceri先前發現微軟作業系統中存在有Windows Installer的權限擴張漏洞「CVE-2021-41379」，經過研究後認為，透過CVE-2021-41379可以更新的方式，讓有心人士取得電腦的最高管理權限。Abdelhamid Naceri在發現後就依照慣例提交給微軟，而微軟也在11月9日發布相關修補程式，但後來Abdelhamid Naceri研究後，發現微軟所發布的CVE-2021-41379漏洞修補程式並沒有妥善修補
- Abdelhamid Naceri所發布的軟體，可以繞過9日微軟發布的更新，依循同樣的漏洞對電腦展開攻擊。國外媒體實際測試的情況下，也證實只需要幾秒鐘的時間，就可以將手上僅有訪問權限的使用者帳號，提升至擁有系統管理員權限的管理者帳號。

資料來源：2021年11月27日周刊王

出帳管理系統的漏洞，竟成為駭客入侵的管道，並藉此發動勒索軟體攻擊

駭客鎖定的攻擊目標，不光只是針對組織常見的商用軟體、作業系統下手，也有可能朝企業財務管理軟體而來。例如，資安業者Huntress發現一起美國工程公司遭到勒索軟體攻擊的事故，而駭客入侵該公司的管道，就是BQE出帳系統的SQL注入漏洞CVE-2021-42258。

BQE是專門開發企業財務管理系統的澳洲軟體公司，號稱有超過40萬客戶使用他們的產品。而這項SQL漏洞存在於名為BillQuick Web Suite當中，該公司獲報後，於10月7日發布22.0.9.1版予以修補。

對於這個漏洞帶來的影響，Huntress指出，一旦攻擊者利用這項SQL注入漏洞，不只可以存取BillQuick伺服器的資料，還能在Windows伺服器上執行惡意指令。而且，要觸發這項漏洞的難度並不高，研究人員表示，他們只在該系統的登入頁面上輸入單引號，就會出現SQL資料庫的錯誤訊息，進而發現這項漏洞。

2022.03.01

Newtalk新聞

2022/03/03 星期四

新聞 | 觀點 | 讀者投書 | 討論區 | 影音 | 熱門議題 - 0303全台大停電

總覽 | 政治 | 國際 | 中國 | 社會 | 財經 | 環保 | 專欄 | 選舉 | 體育

議題 | 娛樂 | 網紅 | 電競 | 遊戲 | 旅遊 | 科技 | 生活 | 創夢 | 新奇

三星手機爆資安漏洞！Galaxy系列機種皆遭殃

位於以色列第二大城市的特拉維夫大學(Tel Aviv University)研究發現，三星Galaxy系列手機的資安問題是ARM Trustzone系統中的密鑰存儲方式出現問題。多款Galaxy系列手機皆受到影響，包括Galaxy S8、Galaxy S10、Galaxy S20等等機型，至少1億部Galaxy手機都有資安漏洞，用戶需要小心。

Trustzone是一種將敏感資訊與主要操作系統利用硬體隔開，保護私人、敏感的加密資訊。而三星手機中的Trustzone與安卓系統是同時運作的，要執行安全任務或加密功能時必須與主要操作程序分開。惡意駭客攻擊可能會利用分開操作程序的漏洞，竊取手機用戶的敏感資訊。

2021-05-12

【臺灣資安大會直擊】資安人員在臺灣資安大會首度揭露Slack新漏洞，一旦駭客濫用可發動SSRF攻擊

用戶端提供應用系統的使用者來源、存取的目的應用程式伺服器位置資訊，有可能在提供服務的網站應用程式沒有做好防備的情況下，成為攻擊者可濫用的弱點。在2021臺灣資安大會上，IBM軟體工程師陳孝勇首度揭露的協作平臺Slack漏洞，就與這類資訊的處理有關

在企業對外提供網頁應用程式的時候，使用者電腦的瀏覽器或是應用程式API，通常要發出請求，經由代理伺服器（Proxy）引導，連線到實際的應用程式伺服器，才能存取相關服務，但在過程中用戶端發出的連線資訊，也可能被攻擊者濫用。在2021年的臺灣資安大會上，IBM軟體工程師陳孝勇首度揭露在協作平臺Slack發現的漏洞（目前尚未取得CVE編號），攻擊者可藉由這項防護上的瑕疵，進而發動伺服器端請求偽造（SSRF）攻擊。這項漏洞經陳孝勇通報後，Slack已經完成相關修補，並即將在漏洞懸賞平臺HackerOne上公布。

真實案例分析-案例一(1/11)

- 說明
  - ✓ 在某一受測網站上發現PHP Remote File Include弱點後，除了利用該弱點取得受測網站部分的控制權外，還連帶入侵到另一個相關的網站

- Remote PHP File Include
  - ✓ 因未正確設定php.ini中的allow_url_fopen(4.0.3)或allow_url_include(5.2.0)選項，導致可以操作網站載入遠端主機的PHP程式並執行

真實案例分析-案例一(2/11)

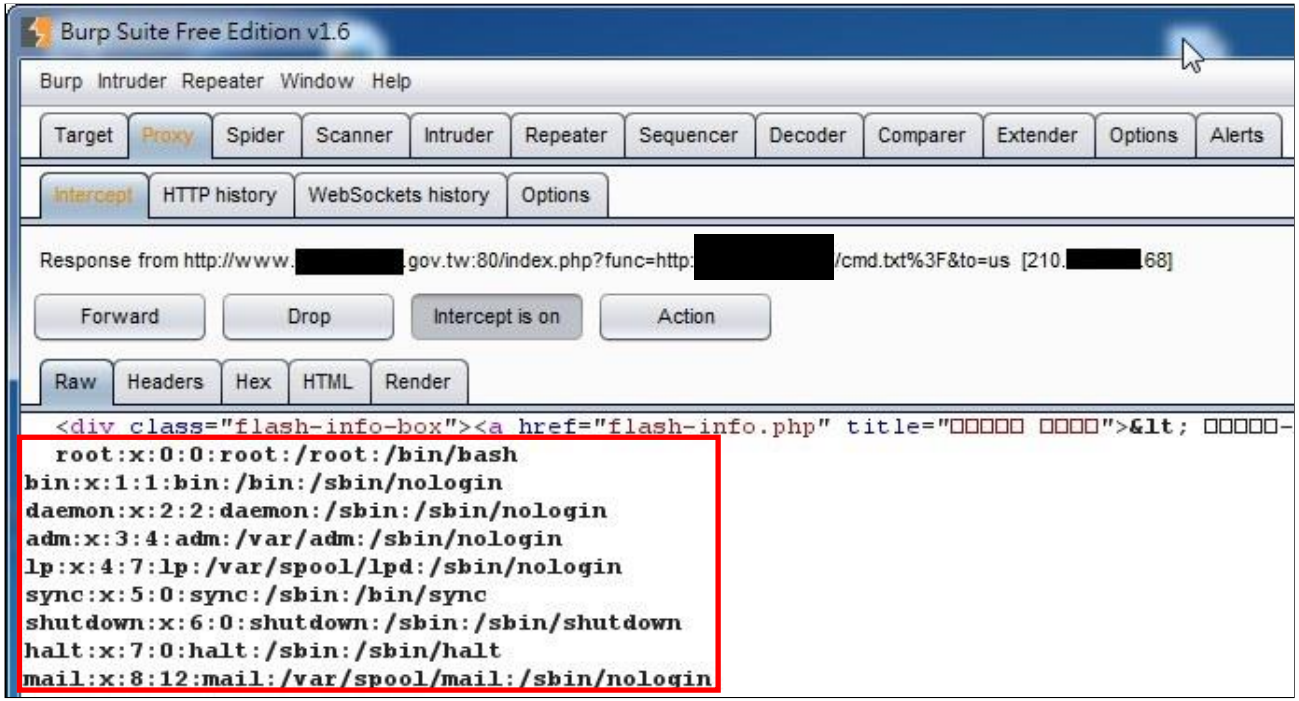
- 收集手上的資訊擴大戰果

真實案例分析-案例一(3/11)

- PHP 好像可以執行系統命令？要不試試？

真實案例分析-案例一(4/11)

- 似乎有發現了



真實案例分析-案例一(5/11)

- 可以收工了?

真實案例分析-案例一(6/11)

- 利用 wget 命令取得遠端主機上的後門程式(WEB Shell)，此時該程式為文字檔格式

  - 再利用 mv 命令將 txt 改成 php

真實案例分析-案例一(7/11)

- The END ?

真實案例分析-案例一(8/11)

- 繼續擴大戰果

真實案例分析-案例一(9/11)

- 使用後門的功能連線至資料庫

真實案例分析-案例一(10/11)

- 查詢看看可以看到甚麼?

真實案例分析-案例一(11/11)

- 成功的開闢新的戰場

真實案例分析-案例二(1/9)

- 說明
  - ✓在某管理系統的網站中，發現利用系統管理者的帳號，搭配DirBuster所找到的測試頁面，居然可以在不知道系統管理者帳號的密碼下，直接修改系統管理者帳號的密碼並登入網站!

真實案例分析-案例二(2/9)

- 對需要登入的網站執行黑箱測試
- 網站上有操作手冊，其中有寫出管理帳號

真實案例分析-案例二(3/9)

- 使用DirBuster發現測試頁面，連結中的參數好像有點熟悉....

真實案例分析-案例二(4/9)

- 連結中的參數值改成另一位使用者的帳號後，居然可以直接看到該使用者的資料

真實案例分析-案例二(5/9)

- 進入維護功能後，發現修改密碼的頁面，是用URL中特定參數的值來決定使用者帳號

真實案例分析-案例二(6/9)

- 如果將該參數的值改成管理者的帳號？

真實案例分析-案例二(7/9)

- 成功了!!

真實案例分析-案例二(8/9)

- 接著使用管理者帳號登入網站

真實案例分析-案例二(9/9)

- 就可以做任何事了!!

真實案例分析-案例三(1/6)

- 說明
  - 在某管理系統的網站中，只要修改網站回應中特定的參數值，便可以取得該系統的全部操作權限！

真實案例分析-案例三(2/6)

- 登入使用者的帳號後，發現目前能操作的功能很少，代表該帳號的權限並不高...

真實案例分析-案例三(3/6)

- 瀏覽該頁面的HTML原始碼，有所發現??

真實案例分析-案例三(4/6)

- 觀察登入過程中的HTTP請求，此為送出的登入請求，並無特別之處...

真實案例分析-案例三(5/6)

- 控制閥值難不成.....做在前端？

真實案例分析-案例三(6/6)

- 成功使用一般使用者帳號取得管理權限

資安法對於資通系統之要求

資通系統定義及資安法相關要求

- 資通安全管理法第三條
  - 資通系統：指用以蒐集、控制、傳輸、儲存、流通、刪除資訊或對資訊為其他處理、使用或分享之系統。
- 資安法對資通系統相關要求
  - 資通系統委外開發維護
    - 資通安全管理法施行系統第四條
  - 資通安全防護需求等級分級
    - 資通安全責任等級分及辦法附表九
  - 資通安全防護基準
    - 資通安全責任等級分及辦法附表十

資通安全管理法施行細則第四條要求

- 考量委外項目之性質、資通安全需求，選任適當之受託者，並監督其資通安全維護

受託方

① 受託者應具備完善之資通安全管理措施或通過協力廠商驗證

② 受託者應配置之資安專業人員(數量、資格、證照、經驗)

③ 受託者得否複委託，及進行複委託應注之事項

④ 受託業務涉及國家機密者，相關執行人員應接受適任性查核

委外之後

① 客製化開發者，應提供該資通系統之安全性檢測證明

② 非自行開發者，並應標示內容與其來源及提供授權證明

③ 受託者知悉資通安全事件時，應立即通知委託機關及採行之補救措施

④ 委託結束後，應確認受託者持有之資料之返還或刪除

⑤ 受託者應採取之其他資通安全相關維護措施

⑥ 委託機關應以稽核或適當方式確認受託者之執行情形

40

資通系統防護需求等級分級評定標準(附表九)

系統安全等級	機密性	完整性	可用性	法律遵循性
普	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生有限之影響	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生有限之影響	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生有限之影響	其他資通系統設置或運作於法令有相關規範之情形
中	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生嚴重之影響	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生嚴重之影響	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生嚴重之影響	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關或其所屬人員受行政罰、懲戒或懲處
高	發生資通安全事件致資通系統受影響時，可能造成未經授權之資訊揭露，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響	發生資通安全事件致資通系統受影響時，可能造成資訊錯誤或遭竄改等情事，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響	發生資通安全事件致資通系統受影響時，可能造成對資訊、資通系統之存取或使用之中斷，對機關之營運、資產或信譽等方面將產生非常嚴重或災難性之影響	如未確實遵循資通系統設置或運作涉及之資通安全相關法令，可能使資通系統受影響而導致資通安全事件，或影響他人合法權益或機關執行業務之公正性及正當性，並使機關所屬人員負刑事責任

資通系統防護基準要求(附表十)(1/22)

控制措施		等級	建議執行措施
存取控制			
帳號管理	建立帳號管理機制，包含帳號之申請、開通、建立、修改、啟用、停用及刪除之程序。	普	**系統功能要求：** 具備帳號管理對應功能，申請、建立、修改、啟用、停用及刪除。 宜保留稽核軌跡與申請資料交叉檢核機制。
	已逾期之臨時或緊急帳號應刪除或禁用。	中	**系統功能要求：** 系統具備標示臨時或緊急帳號及預定停用日期，屆期停用。 宜保留稽核軌跡紀錄臨時或緊急帳號設定與停用日期。
	資通系統閒置帳號應禁用。	中	**系統功能要求：** 系統自動停用3個月未登入之使用者帳號並保留稽核軌跡紀錄閒置帳號及停用日期。
	應定期審核資訊系統帳號之申請、建立、修改、啟用、停用及刪除動作。	中	**系統功能要求：** 系統提供帳號審查功能。

資通系統防護基準要求(附表十)(2/22)

控制措施		等級	建議執行措施
帳號管理	機關應定義各系統之閒置時間或可使用期限與資通系統之使用情況及條件。	高	**系統功能要求：** 系統應明確定義系統閒置時間或可使用期限及其他系統使用條件。
	逾越機關所定預期閒置時間或可使用期限時，系統應自動將使用者登出。	高	**系統功能要求：** 系統在前述定義的條件成立時應自動將使用者登出。
	應依機關規定之情況及條件，使用資通系統。	高	**系統功能要求：** 系統應具備檢查使用者是否有違反合理使用情況及條件之狀況，應保留違反之稽核軌跡、不執行違反規定之操作，並依程序或定義之違規處理原則執行。
	監控資通系統帳號，如發現帳號違常使用時回報管理者。	高	**系統功能要求：** 系統有定義監控帳號異常條件設定，如違反合理使用或達異常登入條件功能，並可設定違常使用之處理及通知對象。

資通系統防護基準要求(附表十)(3/22)

控制措施		等級	建議執行措施
最小權限	採用最小權限原則，只允許使用者(或代表使用者行為的程序)依據機關任務和業務功能，完成指派任務所需之授權存取。	中	**系統功能要求：** 應用系統依據業務功能設計功能授權管理功能，使用者僅可存取授權功能。 系統保存使用者權限設定與變更稽核軌跡紀錄。
遠端存取	對於每一種允許之遠端存取類型，都應先取得授權，建立使用限制、組態需求、連線需求及文件化。	普	**系統功能要求：** 應用系統遠端作業，以TLS連線利用瀏覽器作業。非公開資訊使用者需先登入系統，並僅存取授權功能。 應用系統若有與外機關系統或資料介接，應有明確連線與組態文件，連線過程應加密。
	使用者之權限檢查作業應於伺服器端完成。	普	**系統功能要求：** 使用系統功能權限檢查應於伺服器端完成。

資通系統防護基準要求(附表十)(4/22)

控制措施		等級	建議執行措施
遠端存取	應監控遠端存取機關內部網段或資通系統後臺之連線。	普	**系統功能要求：** 系統提供使用者登入、操作系統功能及個人資料處理軌跡紀錄。 系統應監控外機關系統或資料介接作業，保留連線作業稽核軌跡。
	使用者之權限檢查作業應於伺服器端完成。	普	**系統功能要求：** 使用系統功能權限檢查應於伺服器端完成。
	應採加密機制。	普	**系統功能要求：** 系統之資料交換過程應有加密機制，如使用TLS加密方式連線或透過VPN等加密通道執行資料交換。 系統儲存高敏感度之資料（如業務敏感或個人隱私等）應採加密機制。
	資通系統遠端存取之來源應為機關已預先定義及管理之存取控制點。	中	**系統功能要求：** 系統限制使用者方可登入後臺管理系統中。 系統應外機關系統或資料介接作業，應限定存取鑑別方式並確保通道安全。

資通系統防護基準要求(附表十)(5/22)

控制措施		等級	建議執行措施
事件日誌與可歸責性			
記錄事件	訂定日誌之記錄時間週期及留存政策，並保留日誌至少六個月。	普	**系統功能要求：** 應用系統相關日誌(包括作業系統、資料庫及應用系統等)至少留存6個月。
	資通系統應記錄特定事件之功能，並決定應記錄之特定資通系統事件。	普	**系統功能要求：** 應至少記錄使用者帳號、來源IP、登入(登出)時間、登入成功或失敗，至少保留重要個人資料之新增、修改或刪除紀錄。
	應稽核資通系統管理者帳號所執行之各項功能。	普	**系統功能要求：** 應用系統應保留系統管理者在執行各項作業之稽核紀錄。
	應定期審查機關所保留資通系統產生之日誌。	中	**系統功能要求：** 系統應整理日誌紀錄產出資料或報表，以供應用系統負責人每季進行審查。

資通系統防護基準要求(附表十)(6/22)

控制措施		等級	建議執行措施
日誌紀錄內容	資通系統產生之日誌應包含事件類型、發生時間、發生位置及任何與事件相關之使用者身分識別等資訊，並採用單一日誌機制，確保輸出格式之一致性，並應依資通安全政策及法規要求納入其他相關資訊。	中	**系統功能要求：** 系統保有之日誌紀錄之清冊應明訂各紀錄保留之欄位，並設計單一保存機制，除保存外宜具備輸出機制，輸出格式應依SOC或相關規定辦理。
日誌儲存容量	依據日誌儲存需求，配置所需之儲存容量。	普	**系統功能要求：** 估計所需之儲存容量，並納入儲存容量需求規劃，並具備儲存空間不足時將超過保存期限之日期匯出，依業務需要執行刪除或安全封存。

資通系統防護基準要求(附表十)(7/22)

控制措施		等級	建議執行措施
日誌處理失效之回應	資通系統於日誌處理失效時應採取適當之行動。	普	**系統功能要求：** 系統應定期檢核日誌存容量空間，並確保日誌紀錄寫入失效時之處理程序，避免應用系統中斷。
	機關規定需要即時通報之日誌失效事件發生時，資通系統應於機關規定之時效內，對特定人員提出警告。	高	**系統功能要求：** 日誌失效之通報對象及通報時效，並提出相關機制。
時戳及校時	資通系統應使用系統內部時鐘產生稽核紀錄所需時戳，並可以對應到世界協調時間(UTC)或格林威治標準時間(GMT)。	普	**系統功能要求：** 應用系統稽核紀錄所需時戳(timestamp)以伺服主機系統時鐘為準。
	系統內部時鐘應定期與基準時間源進行同步。	中	**系統功能要求：** 無設定NTP校時之設備應定期校時。伺服主機設定內部NTP校時。

資通系統防護基準要求(附表十)(8/22)

控制措施		等級	建議執行措施
日誌資訊之保護	對日誌之存取管理，僅限於有權限之使用者。	普	**系統功能要求：** 系統應設計保護日誌紀錄不受變更（修改或刪除）的機制，優先以雜湊驗證，或採用其他機制以保護稽核紀錄完整性。
	應運用雜湊或其他適當方式之完整性確保機制。	中	**系統功能要求：** 日誌失效之通報對象及通報時效，並提出相關機制。
	定期備份日誌至原系統外之其他實體系統。	高	**系統功能要求：** 日誌失效之通報對象及通報時效，並提出相關機制。

資通系統防護基準要求(附表十)(9/22)

控制措施		等級	建議執行措施
營運持續計畫			
系統備份	訂定系統可容忍資料損失之時間要求。	普	**系統功能要求：** 分析表登錄最長可接受的中斷時間(MTD)、目標回復時間（RTO）、目標回復時間點（RPO）及回復所需資源等相關營運衝擊分析資料。
	執行系統源碼與資料備份。	普	**系統功能要求：** 依據RPO訂定備份政策實作源碼與資料備份。
	應定期測試備份資訊，以驗證備份媒體之可靠性及資訊之完整性。	中	**系統功能要求：** 上線應用系統每年至少執行1次災害復原演練或營運持續演練。演練時以備份還原並檢查資料與程式的完整性。
	應將備份還原，作為營運持續計畫測試之一部分。	高	**系統功能要求：** 訂定營運持續計畫演練時應納入備份還原測試項目。

資通系統防護基準要求(附表十)(10/22)

控制措施		等級	建議執行措施
系統備份	應在與運作系統不同地點之獨立設施或防火櫃中，儲存重要資通系統軟體與其他安全相關資訊之備份。	高	**系統功能要求：** 資料與程式有採異地備份儲存。
系統備援	訂定資通系統從中斷後至重新恢復服務之可容忍時間要求。	中	**系統功能要求：** 於營運衝擊分析表登錄最長可接受的中斷時間(MTD)、目標回復時間（RTO）、目標回復時間點（RPO）及回復所需資源等相關資料。
	原服務中斷時，於可容忍時間內，由備援設備或其他方式取代並提供服務。	中	**系統功能要求：** 設計之備援機制，可支持於最長可接受的中斷時間(MTD)時間內完成應用系統回復正常運作目標。

資通系統防護基準要求(附表十)(11/22)

控制措施		等級	建議執行措施
識別與鑑別			
使用者之識別與鑑別	資通系統應具備唯一識別及鑑別機關使用者(或代表機關使用者行為之程序)之功能，禁止使用共用帳號。	普	**系統功能要求：** 應用系統各使用者需具備唯一識別，區分機關使用者與非機關使用者。機關用戶得指定機關用戶管理者代表操作，但不得共用。
	對帳號之網路或本機存取採取多重認證技術。	高	**系統功能要求：** 對應用系統之存取採取多重認證技術。
身分驗證管理	使用預設密碼登入系統時，應於登入後要求立即變更。	普	**系統功能要求：** 應用系統於使用者首次登錄後要求立即變更密碼。
	身分驗證相關資訊不以明文傳輸。	普	身份驗證資訊如通行碼，不以明文傳輸。(不論為首次預設密碼或使用者忘記密碼)

資通系統防護基準要求(附表十)(12/22)

控制措施		等級	建議執行措施
身分驗證管理	具備帳戶鎖定機制，帳號登入進行身分驗證失敗達五次後，至少十五分鐘內不允許該帳號繼續嘗試登入或使用機關自建之失敗驗證機制。	普	**系統功能要求：** 帳號登入失敗5次即鎖定。鎖定後至少十五分鐘內不允許該帳號繼續嘗試登入，自動或由管理者解除鎖定。
	使用密碼進行驗證時，應強制最低密碼複雜度；強制密碼最短及最長之效期限制。	中	**系統功能要求：** 應用系統宜增加驗證碼、多重身份認證或其他限制自動化程式之登入或密碼更換嘗試控制。
	密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記。	中	**系統功能要求：** 密碼重設機制對使用者重新身分確認後，發送一次性及具有時效性符記（token）之機制。
鑑別資訊回饋	資通系統應遮蔽鑑別過程中之資訊。	普	**系統功能要求：** 應用系統輸入密碼欄位應遮蔽顯示。

資通系統防護基準要求(附表十)(13/22)

控制措施		等級	建議執行措施
加密模組鑑別	資通系統如以密碼進行鑑別時，該密碼應加密或經雜湊處理後儲存。	中	**系統功能要求：** 密碼資訊宜採用不可逆雜湊處理方式儲存。 可遠端存取系統宜應採用隨機鹽雜湊（Salted Hash）方式儲存。
非內部使用者之識別與鑑別	資通系統應識別及鑑別非機關使用者(或代表機關使用者行為之程序)。	普	**系統功能要求：** 應用系統針應可明確區別非機關使用者及機關使用者。

資通系統防護基準要求(附表十)(14/22)

控制措施		等級	建議執行措施
系統與服務獲得			
系統發展生命週期需求階段	針對系統安全需求（含機密性、可用性、完整性），進行確認。	普	**系統功能要求：** 應用系統應依資通系統防護需求分級原則分級要求實施防護基準控制，及其他資安要求。
系統發展生命週期設計階段	應根據系統功能與要求，識別可能影響系統之威脅，進行風險分析與評估。	中	**系統功能要求：** 識別可能影響系統之威脅，進行風險分析與評估並保留過程文件。
	將風險評估結果回饋需求階段的檢核項目，並提出安全需求修正。	中	**系統功能要求：** 因應上述所分析之風險增列或變更資安需求紀錄。

資通系統防護基準要求(附表十)(15/22)

控制措施		等級	建議執行措施
系統發展生命週期開發階段	應針對安全需求實作必要控制措施。	普	**系統功能要求：** 依據應用系統安全需求控制措施，明列各項控制方法及資通系統技術規格。
	應注意避免軟體常見漏洞及實作必要控制措施。	普	**系統功能要求：** 實作控制措施, 避免常見漏洞，如： Web 應用系統，避免OWASP Top 10 web application Security Risks。 行動APP或行動裝置使用，避免OWASP Top 10 Mobile Security Risks。 應用系統介面，避免OWASP Top10 API Security Risks。 IOT設備使用，避免 OWASP Top 10 IoT Security Risks。

資通系統防護基準要求(附表十)(16/22)

控制措施		等級	建議執行措施
系統發展生命週期開發階段	發生錯誤時，使用者頁面僅顯示簡短錯誤訊息及代碼，不包含詳細之錯誤訊息。	普	**系統功能要求：** 訂定錯誤訊息規則代碼及顯示錯誤訊息，避免包含詳細之系統錯誤訊息。
	執行「源碼掃描」安全檢測。	高	**系統功能要求：** 應用系統首次上線前或重大變更上線前應通過「源碼掃描」安全檢測。
	系統應具備發生嚴重錯誤時之通知機制。	高	**系統功能要求：** 系統應具備發生嚴重錯誤時之通知機制。
系統發展生命週期測試階段	執行「弱點掃描」安全檢測。	普	**系統功能要求：** 系統定期執行弱點掃描安全檢測，並依限完成補強。

資通系統防護基準要求(附表十)(17/22)

控制措施		等級	建議執行措施
系統發展生命週期測試階段	執行「滲透測試」安全檢測。	高	**系統功能要求：** 應用系統應定期執行滲透測試，並依測試結果完成改善通過複測。
系統發展生命週期部署與維運階段	在部署環境中應針對相關資安威脅，進行更新與修補，並關閉不必要服務與埠口。	普	**系統功能要求：** 伺服器主機定期安裝伺服主機安全性更新，並依據部內資安規範關閉不必要之服務與埠口。
	資通系統不使用預設密碼。	普	**系統功能要求：** 應用系統及其使用之工具軟體不使用預設密碼。
	於系統發展生命週期之維運階段，應執行版本控制與變更管理。	中	**系統功能要求：** 執行應用系統程式版本與變更管理機制。

資通系統防護基準要求(附表十)(18/22)

控制措施		等級	建議執行措施
系統發展生命週期委外階段	資通系統開發如委外辦理，應將系統發展生命週期各階段依等級將安全需求(含機密性、可用性、完整性)納入委外契約。	普	**系統功能要求：** 應用系統委外招標文件資安要求。
獲得程序	開發、測試以及正式作業環境應為區隔。	中	**系統功能要求：** 開發、測試及正式環境應區隔。
資訊系統文件	應儲存與管理系統發展生命週期之相關文件。	普	**系統功能要求：** 應用系統委外招標文件明列發展生命週期交付項目。
系統與通訊保護			
傳輸之機密性與完整性	資通系統應採用加密機制，以防止未授權之資訊揭露或偵測資訊之變更。但傳輸過程中有替代之實體保護措施者，不在此限。	高	**系統功能要求：** 資通系統應有電子資料傳輸清冊，明列各傳輸管算及其加密保護機制。

資通系統防護基準要求(附表十)(19/22)

控制措施		等級	建議執行措施
傳輸之機密性與完整性	使用公開、國際機構驗證且未遭破解之演算法。	高	**系統功能要求：** 各加密機制說明採用之演算法，必需為公開、國際機構驗證且未遭破解之演算法。
	支援演算法最大長度金鑰。	高	**系統功能要求：** 各加密機制採用之演算法，使用可支援之最大長度金鑰。
	加密金鑰或憑證應定期更換。	高	**系統功能要求：** 各加密機制說明採用之金鑰變更週期定義及實作定期更換機制。
	伺服器端之金鑰保管應訂定管理規範及實施應有之安全防護措施。	高	**系統功能要求：** 應訂定伺服器端之金鑰管理規範。

資通系統防護基準要求(附表十)(20/22)

控制措施		等級	建議執行措施
資料儲存之安全	資通系統重要組態設定檔案及其他具保護需求之資訊應加密或以其他適當方式儲存。	高	**系統功能要求：** 應有需保護之機敏或高完整性要求資料清單，包含資料項目、資料內容、敏感程度、儲存位置、加密控制演算法、金鑰長度、金鑰或其他保護管理機制。
系統與資訊完整性			
漏洞修復	系統之漏洞修復應測試有效性及潛在影響，並定期更新。	普	**系統功能要求：** 應用系統配合系統修補（patch）、弱掃、滲透測試或原碼檢測修復前應先測試評估是否影響系統運作。
	定期確認資通系統相關漏洞修復之狀態。	中	**系統功能要求：** 各項檢測與修補應記錄執行日期，修復事項，並追蹤修補狀態，確認修補完成。
資通系統監控	發現資訊系統有被入侵跡象時，應通報機關特定人員。	普	**系統功能要求：** 伺服主機採用各項防護（如防火牆、WAF、IPS及HIPS），如有異常狀態監控系統會通知相關負責人員。

資通系統防護基準要求(附表十)(21/22)

控制措施		等級	建議執行措施
資通系統監控	監控資通系統，以偵測攻擊和未授權之連線，並識別資通系統之未授權使用。	中	**系統功能要求：** 應用系統應設定異常通報人員清單，針對多次登入失敗、異常使用狀況應通知使用者及通報人員
	資通系統應採用自動化工具監控進出之通信流量，並於發現不尋常或未授權之活動時，針對該事件進行分析。	高	**系統功能要求：** 應實作自動化工具監控進出之通信流量，定義不尋常或未授權之活動，並於發生時發出通知，進行分析判斷。
軟體及資訊完整性	使用完整性驗證工具以偵測未授權變更特定軟體及資訊。	中	**系統功能要求：** 重要資料宜考量應用HIPS進行防護，不可任意變更檔案，或實施其他可驗證完整性之控制。
	使用者輸入資料合法性檢查應置放於應用系統伺服器端。	中	**系統功能要求：** 應用系統輸入資料驗證均於伺服器進行處理。

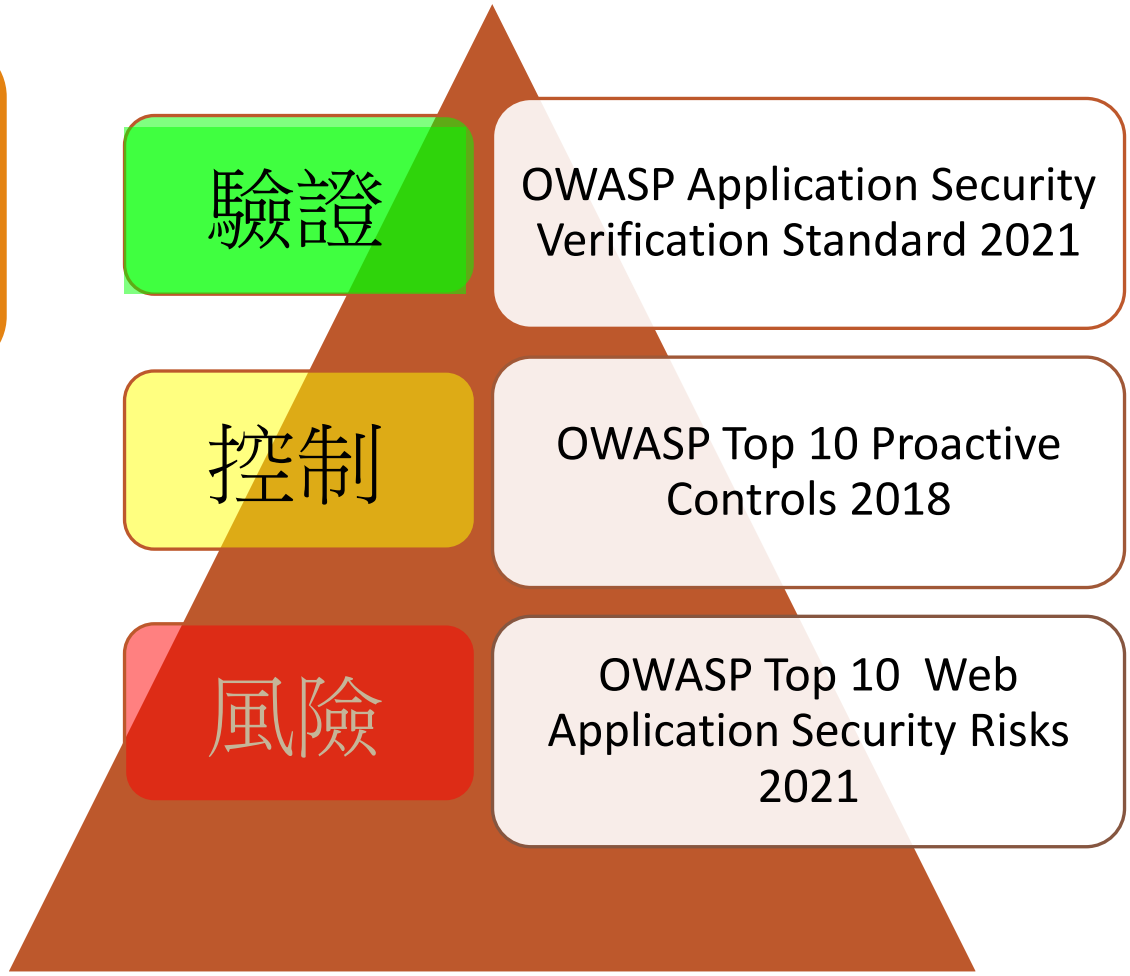
資通系統防護基準要求(附表十)(22/22)

控制措施		等級	建議執行措施
軟體及資訊完整性	當發現違反完整性時，資通系統應實施機關指定之安全保護措施。	中	**系統功能要求：** 如發生資安事件時，必須通報機關，提出緊急應變處置，並配合機關做後續處理。
	應定期執行軟體與資訊完整性檢查。	中	**系統功能要求：** 定期檢查應用系統程式及資料完整性，並保留檢核紀錄。

如何撰寫安全的資通系統

系統開發安全參考建議

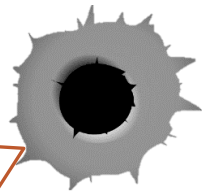
PCI_DSS v3-2-1
(6.5.1 through 6.5.10)



OWASP十大網頁應用安全風險與主動控制

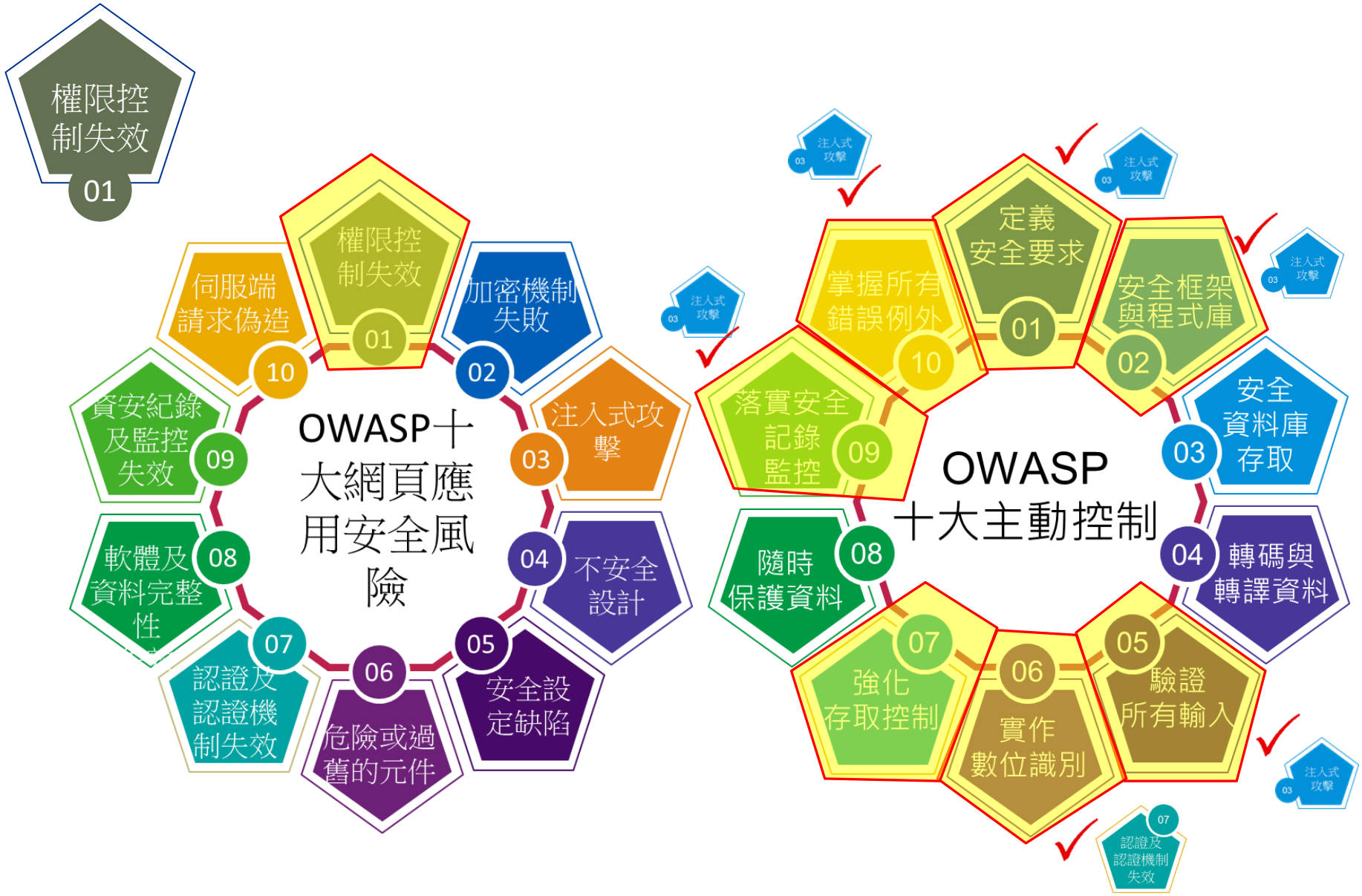
權限控制失效
01

由於缺乏自動化的檢測和應用程序開發人員缺乏有效的功能測試，因而存取控制缺陷很常見。
存取控制檢測通常不適用於自動化的靜態或動態測試。手動測試是檢測訪存取制缺失或失效的最佳方法，包括：HTTP方法（如：GET和PUT）、控制器、直接對象引用等。



對存取控制的利用是滲透測試人員的一項核心技能。SAST工具和DAST 工具可以檢測到存取控制的缺失，但不能驗證其功能是否正常。存取控制可透過手動方式檢測，或在某些特定框架下透過自動化檢測存取控制缺失。

技術影響是攻擊者可以冒充用户、管理員或擁有特權的用户，或者**創建、存取、更新或刪除任何記錄**。
業務影響取決於應用程序和資料的保護需求。


權限控制失效
01
OWASP十大網頁應用安全風險
權限控制失效
01
加密機制失敗
02
注入式攻擊
03
不安全設計
04
安全設定缺陷
05
危險或過舊的元件
06
認證及認證機制失效
07
軟體及資料完整性
08
資安紀錄及監控失效
09
伺服端請求偽造
10
OWASP
十大主動控制
定義安全要求
01
安全框架與程式庫
02
安全資料庫存取
03
轉碼與轉譯資料
04
驗證所有輸入
05
實作數位識別
06
強化存取控制
07
隨時保護資料
08
落實安全記錄監控
09
掌握所有錯誤例外
10
注入式攻擊
03
認證及認證機制失效
07

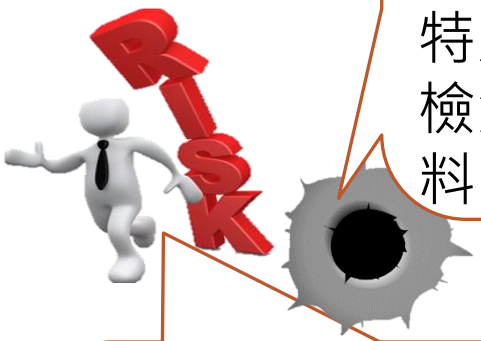
授權(存取控管)是針對特定資源發出存取請求，判斷該請求是否應該被核准或是拒絕。

- 強制所有的存取都需經過權限控制
- 預設不授權
- 最小權限原則
- 避免程式碼中寫死權限控制
- 避免不好的程式碼習慣
- 記錄所有存取控制事件
- 伺服器端的信任資料要以權限控制為導向

加密機制失敗

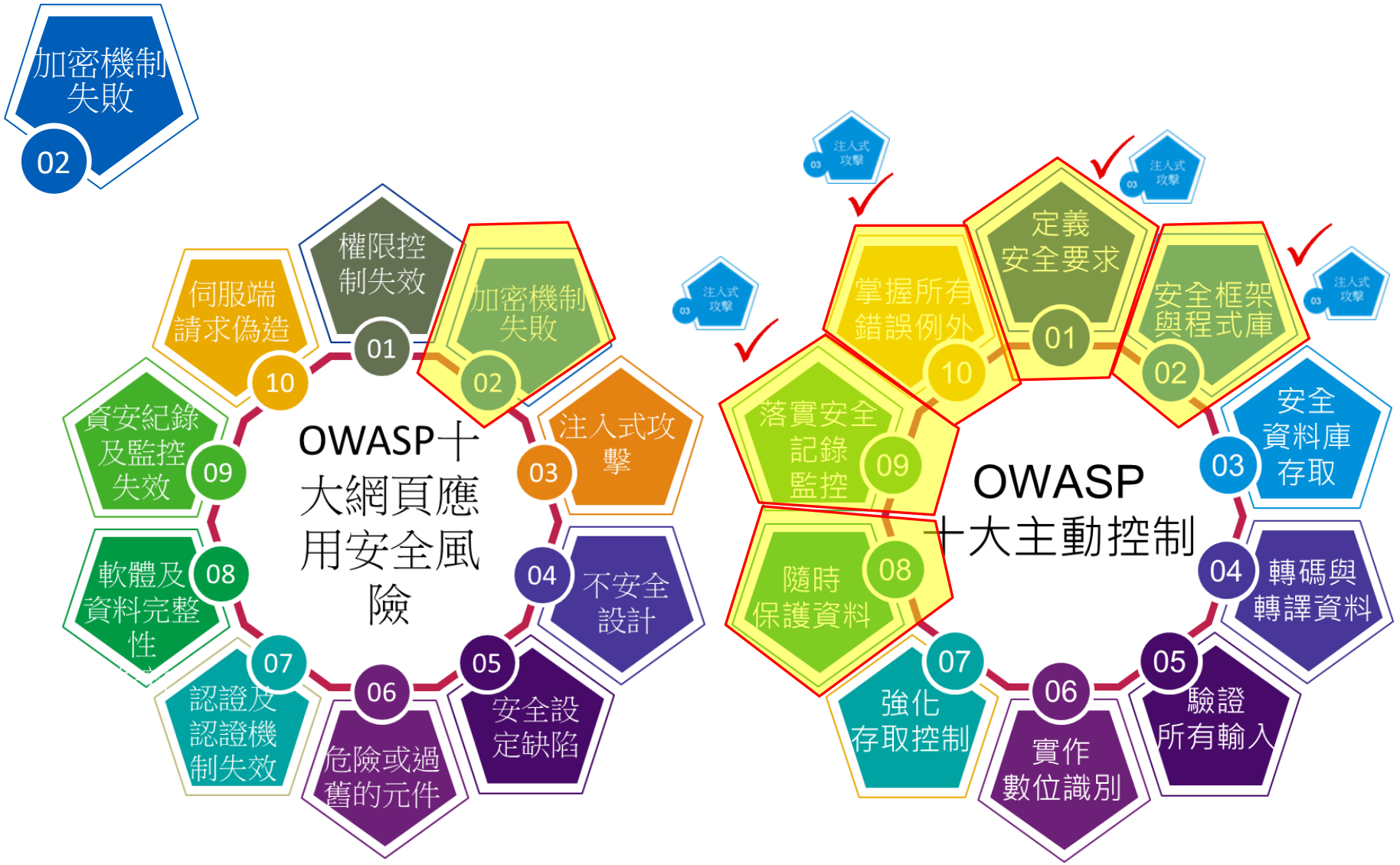
02

在最近幾年，這是最常見的、最具影響力的攻擊。這個領域**最常見的漏洞是不對敏感資訊進行加密**。在資料加密過程中，常見的問題是不安全的密鑰生成和管理以及使用弱加密算法、弱協議和弱密碼。特別是使用弱的雜湊算法來保護密碼。在伺服器端，檢測傳輸過程中的資料弱點很容易，但檢測儲存資料的弱點確非常困難。



攻擊者**不是直接攻擊密碼**，而是**在傳輸過程中**或從用户端，例如：瀏覽器，**竊取密鑰、發起中間人攻擊，或從伺服器端竊取明文資訊**。這通常需要手動攻擊。藉由使用GPU，密碼資料庫能用暴力破解。

这些資訊包括**很多個人敏感信息(PII)**，例如：醫療記錄、認證憑證、個人隱私、信用卡資訊等。這些資訊**受到相關法律和條例保護**，例如：歐盟(GDPR)和地方隱私保護法律。


加密機制失敗
02
OWASP十大網頁應用安全風險
01 權限控制失效
02 加密機制失敗
03 注入式攻擊
04 不安全設計
05 安全設定缺陷
06 危險或過舊的元件
07 認證及認證機制失效
08 軟體及資料完整性
09 資安紀錄及監控失效
10 伺服端請求偽造
OWASP
十大主動控制
01 定義安全要求
02 安全框架與程式庫
03 安全資料庫存取
04 轉碼與轉譯資料
05 驗證所有輸入
06 實作數位識別
07 強化存取控制
08 隨時保護資料
09 落實安全記錄監控
10 掌握所有錯誤例外
注入式攻擊

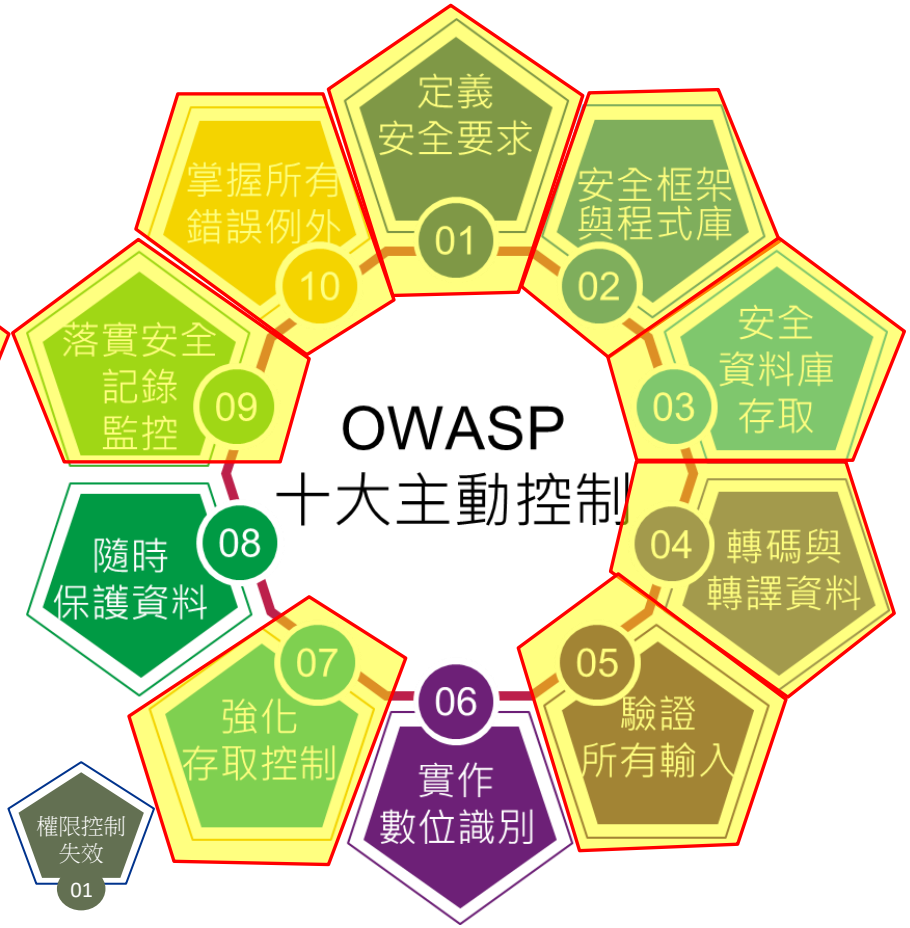
注入漏洞十分普遍，**尤其是在年代遙遠的原始碼中**。注入漏洞通常能在**SQL**、**LDAP**、**XPath**或是**NoSQL查詢語句**、**OS指令**、**XML解譯器**、**SMTP檔頭**、**正規表示法(Regular Expression)**及**ORM查詢語句**中找到。

幾乎任何數據員都能成為注入載體，包括**環境變數**、所有類型的用戶、參數、外部及內部Web服務。總之，**當攻擊者可以向解譯器傳送惡意數據時，注入的漏洞就可能會產生**。

注入會導致資料遺失、破壞、未授權揭露、無法稽核資料存取及拒絕服務等問題。
注入有時**甚至會導致伺服器完全被接管**的狀況。
對於業務上的影響則須視遭注入漏洞波及的應用系統與資料而定。

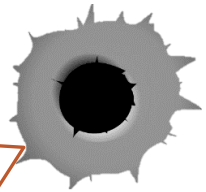

03
注入式攻擊


OWASP十大網頁應用安全風險
01
權限控制失效
02
加密機制失敗
03
注入式攻擊
04
不安全設計
05
安全設定缺陷
06
危險或過舊的元件
07
認證及認證機制失效
08
軟體及資料完整性
09
資安紀錄及監控失效
10
伺服端請求偽造


OWASP
十大主動控制
01
定義安全要求
02
安全框架與程式庫
03
安全資料庫存取
04
轉碼與轉譯資料
05
驗證所有輸入
06
實作數位識別
07
強化存取控制
08
隨時保護資料
09
落實安全記錄監控
10
掌握所有錯誤例外
權限控制失效
01

04 不安全設計

〔2021新增〕



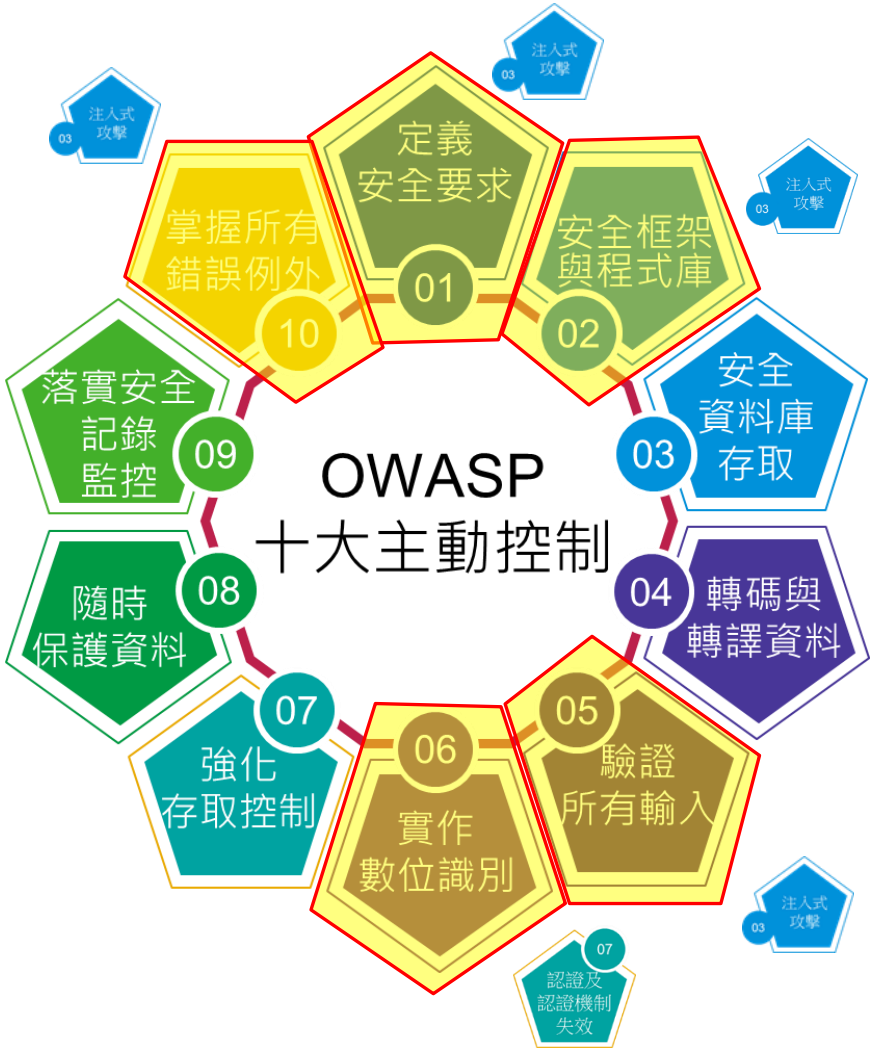
不安全設計**是 2021 年列表中新增的一項**，而不安全設計是一個廣泛的類別呈現許多不同的弱點，代表為「缺乏或無效的控制設計」。
有心人士其能造成損害的漏洞上不當利用或是攻擊。

攻擊者可以透過威脅模型挑戰並入侵系統，**使系統受到超載的流量、偽造的訂單、超量要求存取等造成系統癱瘓及虛假的訊息**被接收、執行，進而造成虧損。

例如：攻擊者亦可以透過設計漏洞安插機器人，進行不當手段的搶購商品(演唱會門票、限量商品等) 使其餘人**無法公平的競爭，造成民怨**等後續影響。

04 不安全設計

〔2021新增〕

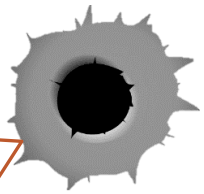


05

安全設定缺陷

安全設定錯誤可能發生在一個應用程序相關的任何層面，包括網路服務、平台、Web伺服器、應用伺服器、資料庫、框架、自定義代碼和預設安裝的虛擬機、容器和儲存。自動掃描器可用於檢測錯誤的安全配置、預設帳户的使用或配置、不必要的服務、遺留選項等。

通常，**攻擊者能夠通過未修復的漏洞**、存取預設帳户、不再使用的頁面、未受保護的文件和目錄等**來取得隊系統的未授權的存取或了解**。



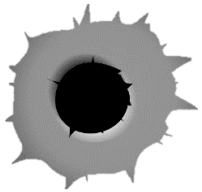
這些漏洞使攻擊者能經常存取一些未授權的系統數據或功能。有時，這些漏洞導致系統的完全攻破。
業務影響取決於您的應用程序和資料的保護需求。


05
安全設定
OWASP十大網頁應用安全風險
01
權限控制失效
02
加密機制失敗
03
注入式攻擊
04
不安全設計
05
安全設定缺陷
06
危險或過舊的元件
07
認證及認證機制失效
08
軟體及資料完整性
09
資安紀錄及監控失效
10
伺服端請求偽造
OWASP
十大主動控制
01
定義安全要求
02
安全框架與程式庫
03
安全資料庫存取
04
轉碼與轉譯資料
05
驗證所有輸入
06
實作數位識別
07
強化存取控制
08
隨時保護資料
09
落實安全記錄監控
10
掌握所有錯誤例外
注入
01

06

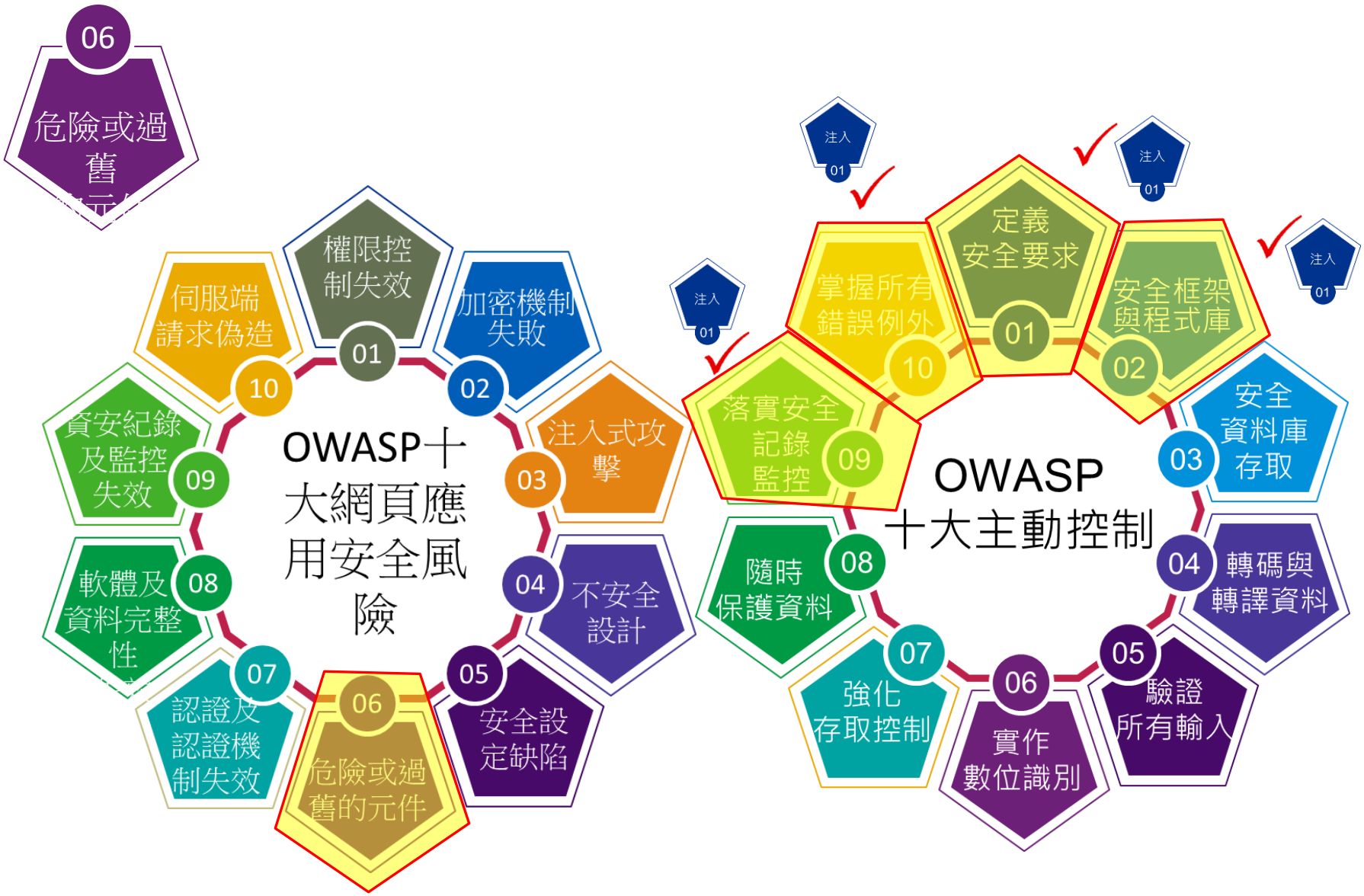
危險或過舊

這種安全漏洞普遍存在。基於組件開發的模式使得多數開發團隊根本**不了解其應用或API中使用的組件**，更談不上即時更新這些組件了。
如Retire.js之類的掃描器可以幫助發現此類漏洞，但這類漏洞是否可以被利用還需花費額外的時間去研究。



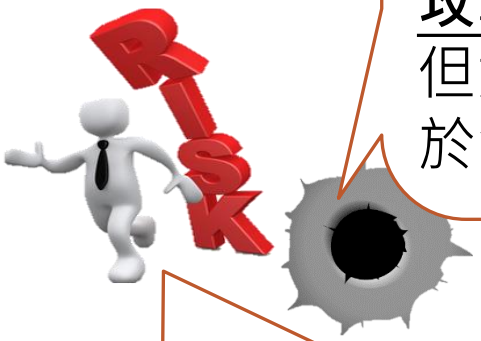
對**一些漏洞很容易找到其利用程序**，但**對其它的漏洞則需要定制開發**。

雖然對於一些**已知的漏洞其影響很小，但目前很多嚴重的安全事件都是利用組件中的已知漏洞**。根據你所要保護的資產，此類風險等級可能會很高。


06
危險或過舊
OWASP十大網頁應用安全風險
01 權限控制失效
02 加密機制失敗
03 注入式攻擊
04 不安全設計
05 安全設定缺陷
06 危險或過舊的元件
07 認證及認證機制失效
08 軟體及資料完整性
09 資安紀錄及監控失效
10 伺服端請求偽造
OWASP十大主動控制
01 定義安全要求
02 安全框架與程式庫
03 安全資料庫存取
04 轉碼與轉譯資料
05 驗證所有輸入
06 實作數位識別
07 強化存取控制
08 隨時保護資料
09 落實安全記錄監控
10 掌握所有錯誤例外
注入 01
注入 01
注入 01

07 認證及認證機制失效

大多數身份和存取管理系统的設計和實作，普遍存在身份認證失效問題。**會話管理是身份驗證和存取控制的基礎，它存在於所有有狀態應用程序中。攻擊者可以使用手動工具來檢驗失效的身份驗證**，但通常會著重於密碼轉存、字典攻擊，或者在類似於釣鱼或社會工程攻擊之後，發現失效的身份認證。



攻擊者可以獲得數百萬的**有效帳號和密碼组合**，包括憑證內容、預設的管理者帳號、自動的暴力破解和字典攻擊工具，以及高級的GPU破解工具。其中**會話管理攻擊很容易被理解，尤其是没有過期的會話密鑰**。

攻擊者只需要存取幾個帳號，或者**取得管理員帳號就可以破壞我們的系統**。根據應用程序領域的不同，**可能會導致洗錢、社會安全詐欺以及帳號身份盜用、洩漏法律高度保護的敏感信息**。

07 認證及認證機制失效

07 認證及認證機制失效

06 實作數位識別

- 安全防護建置的建議

08 軟體及資料完整性

〔2021新增〕

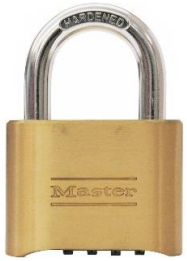
軟體及資料**完整性失效是由於缺乏資料完整性驗證**過程而使用篡改或損壞的資料做出某些決定的狀況。

物件或資料經編碼或序列化到一個對攻擊者可讀寫之結構中將導致不安全的反序列化。另一種形式則是應用程式依賴來自於不受信任來源，典藏庫及內容遞送網路之外掛，函式庫或模組。**不安全的持續性整合/部署(CI/CD)流程則會造成潛在的未經授權存取，惡意程式碼或系統破壞**。

最近一次值得注意的是對**SolarWinds Orion**的攻擊。該軟體開發商**擁有安全組建和更新完整性流程**。儘管如此，**這些流程仍被破壞並在幾個月時間中向 18,000 多個組織送出高度針對性的惡意更新**，其中大約 100 個組織受影響。

軟體及資料完整性 08

〔2021新增〕



可用以下舉措解決軟體及資料完整性失效問題：

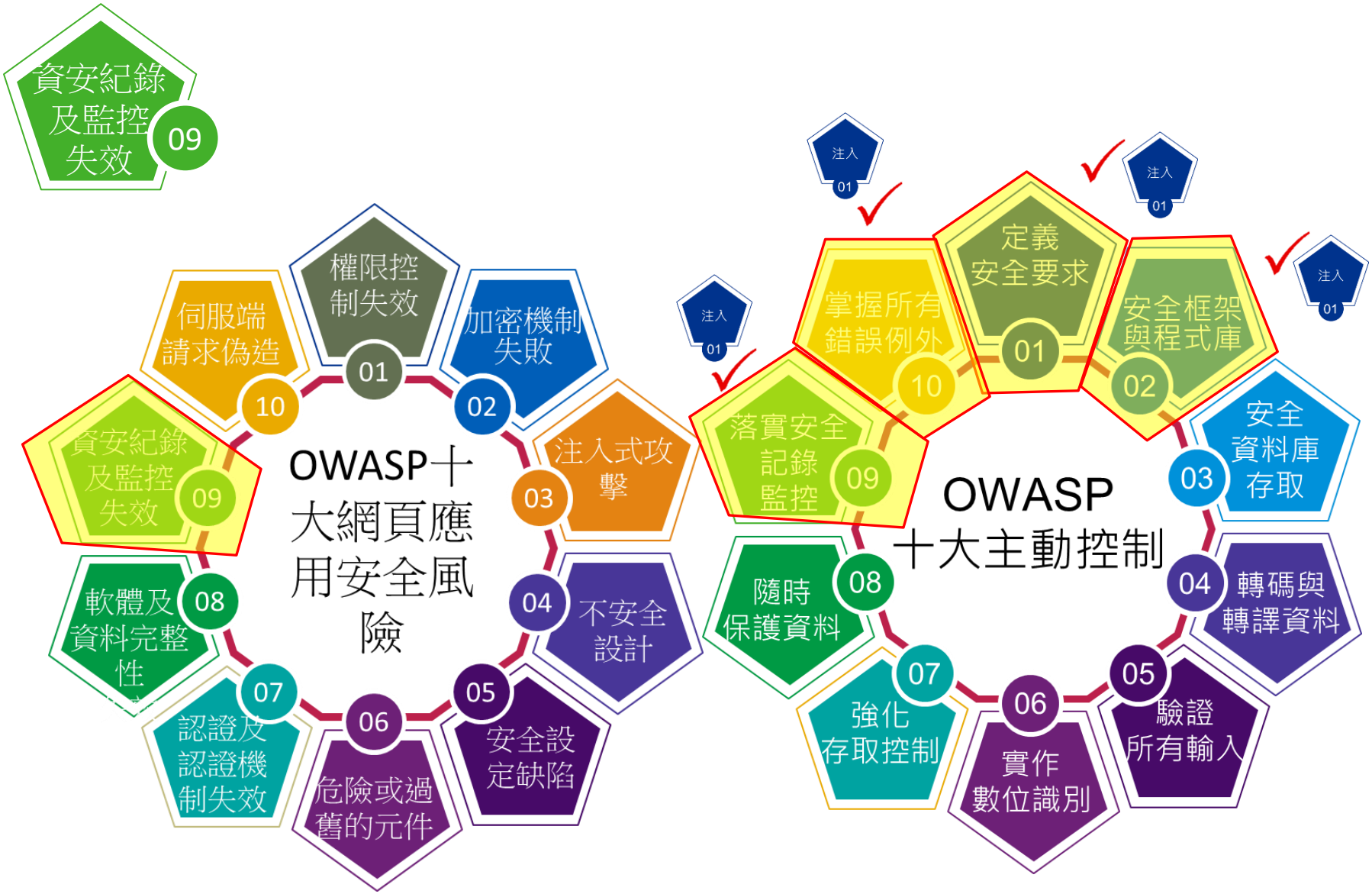
1. **確保**不受信任之客戶端**不會收到未簽署或加密之序列化資料**並**利用完整性檢查或數位簽章來偵測竄改或重放攻擊**。
2. **利用數位簽章**或類似機制確保軟體或資料來自預期之提供者
3. 確保函式庫及從屬套件，例如npm或Maven，是從受信任的典藏庫取得。
4. 使用軟體供應鏈安全工具(例如OWASP Dependency Check 或 OWASP CycloneDX)**確保元件沒有已知弱點**。
5. **適當地設定持續性整合/部署(CI/CD)流程**的組態及存取控制以確保程式碼在組建及部署流程中的完整性。

資安紀錄及監控失效 09

根據行業調查的結果，此問題被列入了Top 10中的第九項。
判斷你是否有足够監控的一個策略是在滲透測試後檢查日誌。測試者的活動應被充分的記錄下來，能够反映出他們造成了什麼樣的影響。

對不足的日誌記錄及監控的利用幾乎是每一個重大安全事件的溫床。
攻擊者依靠監控的不足和響應的不即時來達成他們的目標而不被知曉。

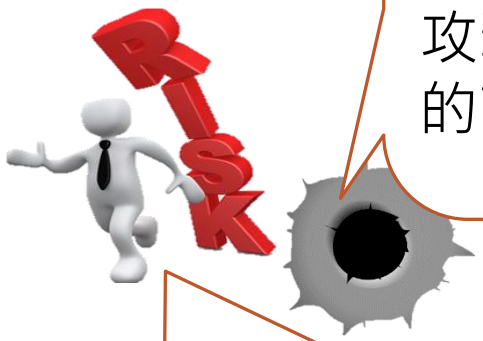
多數成功的攻擊往往從漏洞探測開始。允許這種探測會將攻擊成功的可能性提高到近100%
據統計，在2016年確定一起資料洩漏事件平均需要花191天時間，這麼長時間裡損害早已發生。


資安紀錄及監控失效
09
OWASP十大網頁應用安全風險
權限控制失效
01
加密機制失敗
02
注入式攻擊
03
不安全設計
04
安全設定缺陷
05
危險或過舊的元件
06
認證及認證機制失效
07
軟體及資料完整性
08
伺服端請求偽造
10
資安紀錄及監控失效
09
OWASP
十大主動控制
注入
01
掌握所有錯誤例外
10
定義安全要求
01
安全框架與程式庫
02
安全資料庫存取
03
轉碼與轉譯資料
04
驗證所有輸入
05
實作數位識別
06
強化存取控制
07
隨時保護資料
08
落實安全記錄監控
09

伺服端請求偽造 10

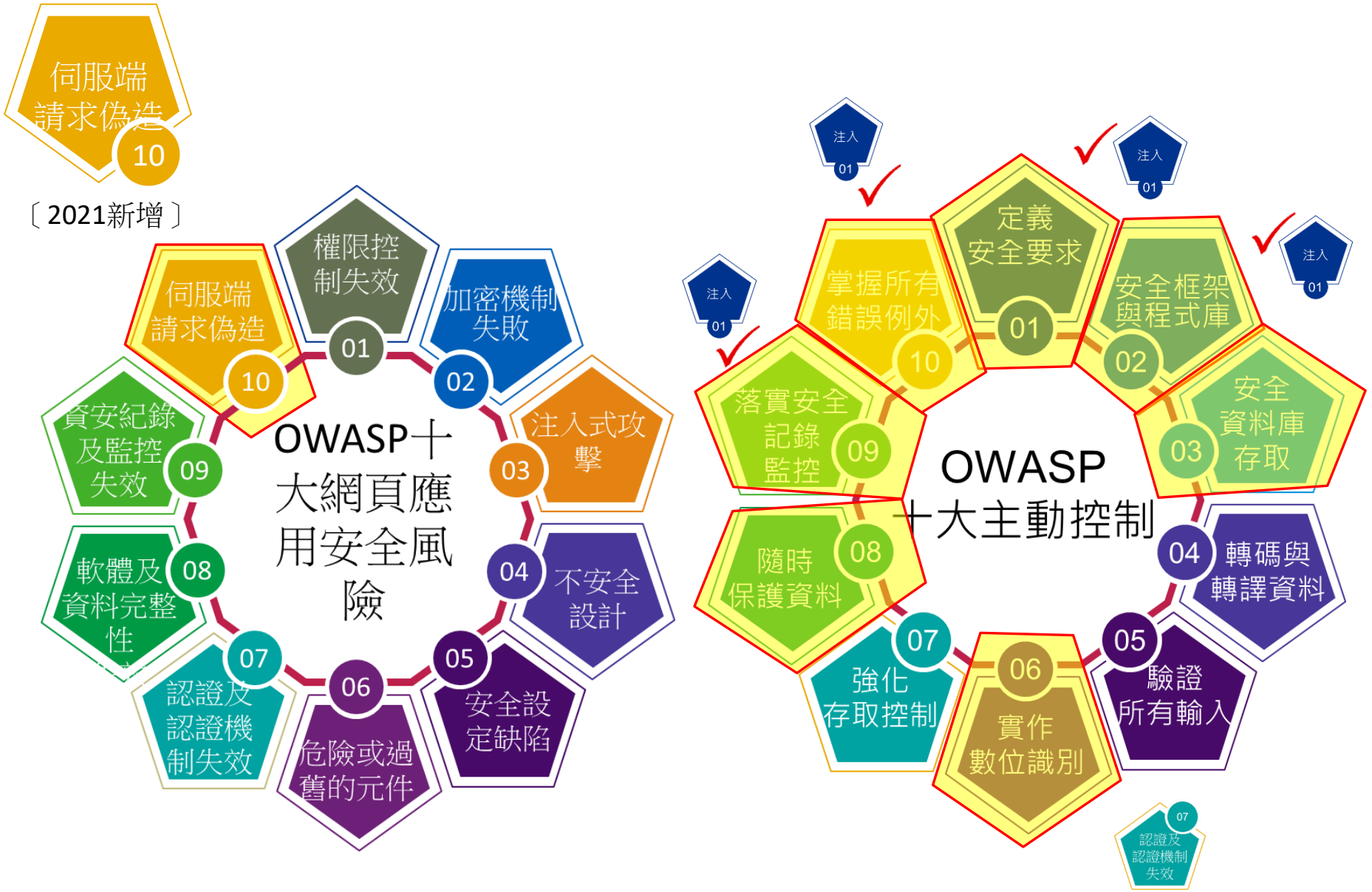
〔2021新增〕

當網頁應用程式正在取得遠端資源，卻**未驗證由使用者提供的網址，此時就會發生偽造伺服端請求**。即便有防火牆、VPN或其他網路ACL保護的情況下，攻擊者仍得以強迫網頁應用程式發送一個經過捏造的請求給一個非預期的目的端。



現今的網頁應用程式提供終端使用者便利的特色，取得網址愈常見。因此，偽造伺服端請求的發生率是在增加當中的。而且，**因為雲端服務和雲端結構的複雜性，偽造伺服端請求的嚴重性將會愈來愈嚴峻**。

隨著許多第三方 Open API 的流行與廣泛於企業內使用 (例如：Google API、Facebook API、AWS API 等等)，只要程式碼一不注意，**駭客可以使用伺服器請求偽 SSRF，穿透內網 (Intranet) 達成攻擊**。


伺服端請求偽造
10
〔2021新增〕
OWASP十大網頁應用安全風險
01 權限控制失效
02 加密機制失敗
03 注入式攻擊
04 不安全設計
05 安全設定缺陷
06 危險或過舊的元件
07 認證及認證機制失效
08 軟體及資料完整性
09 資安紀錄及監控失效
10 伺服端請求偽造
OWASP十大主動控制
01 定義安全要求
02 安全框架與程式庫
03 安全資料庫存取
04 轉碼與轉譯資料
05 驗證所有輸入
06 實作數位識別
07 強化存取控制
08 隨時保護資料
09 落實安全記錄監控
10 掌握所有錯誤例外
注入
01
07 認證及認證機制失效

問題與討論