《資訊安全實務》

試題評析	第一題：為記憶題型，可參考課程內容與重點書目。 第二題：可由課程XSS攻擊與防禦切入。 第三題：可由課程Google Hacking內容切入。 第四題：可由權限管理之 DAC、MAC 與 RBAC 思考。
考點命中	第一題：《高點資通安全總複習講義》第一回，張又中編撰，頁 1-4、46-50。 第二題：《高點資通安全總複習講義》第一回，張又中編撰，頁 1-25、28-29。 第三題：《高點資訊管理與資通安全講義》第三回，張又中編撰，頁 3-34。

一、證據蒐集是數位鑑識過程中重要的一環，請舉出五種網路犯罪證據蒐集的管道，及十種可能找出潛在犯罪證據的情資類型。（30 分）

【擬答】

(一)網路犯罪證據蒐集管道如下表所示：

網路犯罪證據蒐集管道	舉例
網站 Web Site	如 Yahoo! Kimo、PChome、Amazon……。
電子郵件 e-Mail	如 Gmail、Yahoo! Mail、Hotmail……。
新聞群組 Newsgroup	如 PTT(BBS)、論壇討論區、自由評論網……。
即時通訊 Instant Message	如 LINE、Facebook Messenger……。
社交網路服務 Social Network Service, SNS	如 Facebook、Google+、Instagram……。

(二)可能找出潛在犯罪證據的情資類型如下表所示：

網路犯罪	潛在犯罪證據的情資類型。
網路色情	於網路張貼的色情文字、圖片與影片。
網路駭客	遭受網路駭客攻擊行為的影響結果。
網路黑道	透過網路建立的社群與互動。
網路偽造文書	偽造、變造的他人電子簽章或簽寫證明標示。
網路妨害名譽	於網路發表或傳述侮辱、妨害他人之言詞。
網路妨害秘密	利用 P2P 或是其他網路管道散佈他人之隱私。
網路教唆犯罪	於網路社群討論或教唆之情事。
網路詐欺取財	買賣雙方於網路的溝通過程。
網物恐嚇勒索	利用網路傳遞讓特定人或公眾傳送恐嚇勒索之訊息。
網路侵犯著作權	未經著作人授權而使用的文章、歌曲、照片……。

二、網頁隱藏式惡意連結又稱之為「網頁掛馬」，係攻擊者利用瀏覽器或系統漏洞來植入惡意程式或木馬。請說明此攻擊手法的過程，並舉出兩種可防範此種攻擊的方法。（30 分）

【擬答】

(一)以儲存型 XSS 為例，攻擊者將輸入的資料儲存在伺服器端，具有很強的穩定性。例如：擊者發表一篇內含惡意程式碼的文章，閱讀該文章的受害者，都會在其瀏覽器執行該惡意程式碼。以討論區為例，在 Message 欄位寫入：

<script>alert("XSS Testing")</script>

即可將惡意程式碼寫入頁面中，並儲存至後端資料庫。

(二)於伺服器端可用下述方法防範：

1.HttpOnly

由 Microsoft 提出，最早於 IE 6 實做，逐漸成為一個標準，主流瀏覽器如 IE、Firefox、Chrome 皆支援。瀏覽器禁止頁面的 JavaScript 造訪具 HttpOnly 屬性的 Cookie。

PHP 5 語法：setcookie(“myCookie”, “test”, NULL, NULL, NULL, NULL, TRUE);

2.輸入過濾

針對使用者輸入內容進行驗證，包括對 URL、查詢關鍵字、POST 資料等，僅接受指定長度範圍內採用適當格式、預期字元的內容，其他一律過濾。

三、Google Hacking 是駭客利用 Google 搜尋引擎找出網頁或網站的安全漏洞，再利用所得到的資訊入侵電腦網路的一種駭客攻擊方法，請說明導致 Google Hacking 的原因以及避免 Google Hacking 攻擊的方法。(25 分)

【擬答】

Google Hacking 為利用搜尋引擎的進階搜尋字串，找到企業網站的關鍵資訊，如網站伺服器檔案、帳號、密碼、管理介面等資料。由於 Google 搜尋出的網頁已超過 80 億筆，各式各樣的資料都有機會被找到，因此可用其發動攻擊。

發生 Google Hacking 的原因在於網頁的程式撰寫出現問題或權限管控不佳，讓駭客可利用 Google 鍵入內部網址搜尋網站目錄、檔案類型等方式找到網站設定檔(config)、個人隱私等敏感資訊。

避免 Google Hacking 攻擊的方法如可利用 Google 對企業進行檢索，看是否能找出任何可能造成資安風險的敏感資訊，當發現時企業應移除之或是使用密碼保護。亦可通知 Google 將敏感資訊從搜尋結果及快取中移除，然可能損害於 Google 的搜尋排序。

四、以角色為基礎的存取控制（Role-based Access Control），是在系統安全中被廣為使用的存取控制機制，何謂以角色為基礎的存取控制機制？並說明其在實務運作上的優點及執行上的困難點。（15 分）

【擬答】

RBAC 於 1990 年代快速興起，並以證明其對管理與實施大型企業系統的機制很實用。其觀念是將權限與角色關聯，並將使用者指派到適當的角色，因而讓使用者獲得該角色的權限。

在實務運作上，RBAC 可透過角色—使用者的對應，針對不同的任務讓使用者具備不同的角色，彈性且靈活，適用於開發安全的網站應用。然而，RBAC 可能於繼承或是進行權責區分判斷時發生判斷錯誤，另在進行許可權驗證時需要複雜的驗證流程，影響系統效能。