《資通安全》

一、資料隱碼（SQLInjection）仍是至今常見的網路攻擊，此攻擊包含很多種手法，請回答下列問題：

（一）請說明顛覆邏輯（Subverting Logic）以及盲目注入（Blind Injection）兩種手法的意義。（15分）

（二）參數化查詢（Parameterized Query）是公認防禦SQL Injection 攻擊的有效方法，請說明其防禦原理。（10分）

答題關鍵	本題測驗考生對 SQL Injection 的攻擊與防範相關知識。
考點命中	1.《高點資通安全講義》第一回，金乃傑編撰，頁 92-98。

【擬答】

(一)依照題意說明兩種手法之意義：

1.顛覆邏輯（Subverting Logic）：又稱顛覆應用程式邏輯（Subverting Application Logic），指攻擊者掌握程式運作的結構，使用特定的輸入若操作，讓程式未依程式設計師所計畫的方式執行，以完成特定目的。常用於 SQL 注入攻擊（SQL Injection）或緩衝區溢位攻擊（Buffer Overflow）中，例如在 SQL 語法 WHERE 條件中，若掌握執行順序，便有機會利用註解跳過 WHERE 的檢查，來欺騙身分認證機制，考慮以下 SQL 敘述：

SELECT * FROM users WHERE id = '$id' AND passwd = '$passwd'

若在 MySQL 資料庫中，攻擊者若 id 輸入「1' #」，利用單引號（'）收合「id = '」的查詢，並使用註解（#）跳過後續「passwd…」的檢查，如此攻擊者就可以使用 id = ‘1’ 的身分完成身分認證。

2.盲目注入（Blind Injection）：又稱為盲目 SQL 注入（Blind SQL Injection），屬於 SQL 注入攻擊（SQL Injection）。此攻擊主要為取得資料庫的資訊，但資料庫卻沒有直接回傳。例如攻擊者想要知道資料庫的版本，但是網站只利用資料庫中的「會員等級」，將不同等級會員導向到不同的目標網址，根本沒有輸出會員資訊的地方。假設 SQL 敘述如下：

SELECT level FROM users WHERE id = '$id'

而其中 level 又會再經過程式處理，來決定跳轉的目標網址，沒有直接輸出。此時攻擊者可以利用以下語法傳入 id 中：

「1' UNION SELECT IF(SUBSTRING(VERSION(), 1, 1) = '1'), WAIT FOR DELAY '0:0:10', null) #」

此敘述利用 UNION 接合 SQL 語法，並使用 IF 進行判斷。IF 有三個參數，第一個參數為要執行的敘述，當敘述為 true 時執行第二個參數中的敘述，當敘述為 false 時執行第三個參數中的敘述。

第一個參數使用 VERSION()取得 MySQL 版本，若版本第一個字為 1 時，則會執行第二個參數，也就是等待 10 秒才回應。

因此攻擊者可以使用此方法，根據回應時間一個字一個字推斷資料庫的版本，達到攻擊的目的。

(二) 參數化查詢（Parameterized Query）是使用 SQL 資料庫的內建語法，將要查詢的參數從 SQL 敘述中抽出，使用變數作為參數，達成 DBMS 可以先將 SQL 編譯，僅需代換參數部分，而使得攻擊者無法修改參數來改變 SQL 的執行邏輯。在動態網頁程式語言如 PHP 中，可以使用 PDO（PHP Data Objects）的方式進行。假設攻擊者在使用者 id 輸入「1' #」，因此$id 吃到此變數值，如下語法：

```
$query = "SELECT * FROM users WHERE id = '?'";
$stmt = $this -> pdo -> prepare($query);
$stmt -> bindParam(1, "1' #");
$result = $stmt -> execute();
```

執行此敘述時，會建立對應的 SQL 語法如下：

```
set @id := "1' #";
SELECT * FROM users WHERE id = @id
```

由於 MySQL 的 DBMS 透過剖析樹分析@id 的值。由於@id 不屬於數字，因此剖析樹可以檢查出錯誤，而中止語法；即使剖析樹沒有錯誤，但由於 SELECT 已經被直譯器處理過，因此@id 被視為數值傳入，不會影響 SQL 的執行邏輯。參數化查詢將變數當作參數抽出，避免以傳統字串連接的方式被攻擊者以特殊字串更改 SQL 語法的邏輯，因此可以完全防堵 SQL Injection 攻擊。此外，也由於先將 SELECT 語法解析完成，若有連續的 SQL

查詢（假設差異僅有參數），也可以減少編譯時間，增加 SQL 語法的執行效率。

二、SSL（Secure Socket Layer）協定是非常重要的網際網路安全協定，請回答：

(一)SSL 的工作原理為何？請詳細說明之。(10分)

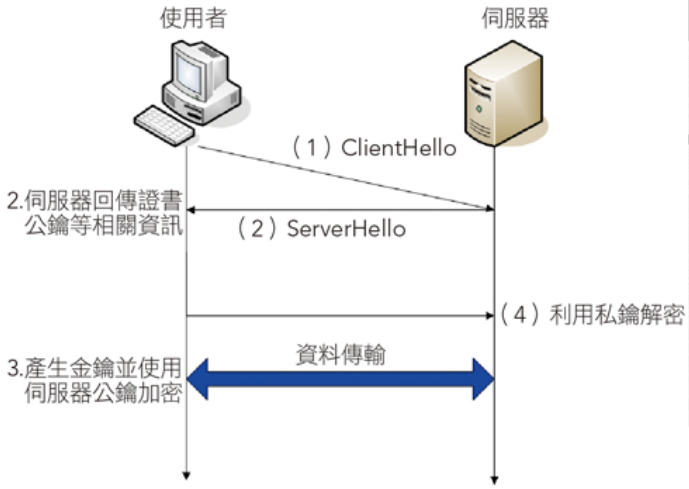
(二)請解釋何謂SSLVPN（Virtual Private Network）？和IPsec VPN 相比，其優缺點為何？（10分）

(三)現今網站多採用SSL 協定，此對資通安全管理造成那些安全威脅？試申論之。(5分)

答題關鍵	本題相似於 105 年國安網路、107 年外交資安 4 等試題，測驗考生對 SSL 相關知識。
考點命中	1.《高點資通安全講義》第一回，金乃傑編撰，頁 25-32。

【擬答】

(一)SSL 使用數位信封技術（Digital Envelope），主要功能是建立使用者瀏覽器與網頁伺服器間資料傳遞的安全通道，為目前最廣泛應用的網頁傳輸安全性協定，即 HTTPS。其工作原理如下所示：



1.使用者瀏覽器發出 ClientHello 給 SSL 網站伺服器：告知伺服器瀏覽器可以使用 SSL 加密及演算法版本序號。

2.SSL 伺服器回應 ServerHello：裡面包含伺服器的數位憑證（存放伺服器公鑰及其他伺服器身分認證的資訊）、這次要使用的演算法。

3.使用者瀏覽器傳送加密後的對稱金鑰給伺服器：瀏覽器依照演算法產生一把對稱金鑰（稱為 session key，僅使用於本次加密），並使用伺服器的公鑰將該金鑰加密（因只有伺服器有解密的私密金鑰，故對稱金鑰不會被傳輸過程中破解）。

4.伺服器解開金鑰取出對稱金鑰進行往後互傳資訊的加解密操作。

(二)將 SSL VPN 與 IPsec VPN 之優缺點比較如下表：

	SSL VPN	IPsec VPN
優點	基於 HTTPS 協定，因非直接網路相通，病毒較難擴散。	只要建立好安全通道，使用者可以直接用內部網路方式連線。 支援各種網路協定，甚至是非 TCP/IP 的 Novell Network 都可以。
缺點	必須安裝 SSL VPN 軟體，基於瀏覽器連線，設定較複雜。 基於 HTTPS 的協定，對於非 HTTPS 協定必須使用轉換器轉成 HTTPS 封包。	若內部網路電腦中毒，會直接影響遠端的電腦。

(三)由於 SSL 具有有效期限，若到期後未更新可能成為最大的資通安全威脅，說明如下：

1.網站受到保護中：當憑證過期後，網站的私密金鑰就有被破解的風險，若被破解，則攻擊者可能監聽到用以傳輸資訊的 session key，進而對加密的內容進行監聽或竄改，破壞機密性與完整性。

2.阻擋合法訪客造訪網站：目前的主流瀏覽器如 Chrome、Firefox 或 Edge 如果偵測到憑證過期，就會阻止使用者連線該網站。因此若憑證過期沒有更換，使用者可能會被瀏覽器阻擋而很難（通常要點選 2 到 3 步驟）造訪網站，致使合法使用者無法檢視網站內容，破壞可用性。

三、資料外洩防護（Data Loss Prevention / Data Leak Prevention, DLP）是近年來受到重視的資訊安全議題，請問：

(一)DLP的意義為何？請詳細說明。(5分)

(二)實現DLP的技術有那些？請詳細說明。(10分)

(三)請比較DLP和DRM（Digital RightManagement）功能的異同。(10分)

答題關鍵	本題測驗考生是否了解 DLP 與 DRM，屬於新出現的題型。
考點命中	1.《高點資通安全講義》第二回，金乃傑編撰，頁 23-29。

【擬答】

(一)資料外洩防護（Data Loss Prevention, DLP）為一種保護資訊安全機密性的硬體或軟體系統，可以安裝在電腦或網路中，透過監視使用者的操作行為，檢核該使用者是否已有分享權限，若無則阻擋使用者；另一方面也可以記錄使用者操作電腦的行為，達到事後追蹤與作為證據，DLP 的目的是達成對資料機密性的保障。由於 DLP 是一個保護機密資料的概念，因此未必是一個獨立的系統，若 DLP 作為一獨立的系統，大致可分為主機型與網路型：

1.主機型 DLP：安裝在電腦裝置上，可以完整記錄使用者操作過程，涵蓋瀏覽器、通訊軟體與 E-mail，資料最完整且可以對已加密的訊息檢測，並達成阻擋；缺點是一定要在電腦上安裝，且記錄之證據可能被刪除。

2.網路型 DLP：在網路中的主機，可以監控區域網路中所有封包，以記錄在區域網路中的機密訊息傳遞事件，由於安裝在區域網路中，因此一個區域網路只需要有一台即可，也可以避免證據被刪除；缺點是無法處理加密的訊息且若要阻止惡意操作需要結合防火牆功能。

(二)達成 DLP 的技術說明如下：

1.格式比對：限制特定的檔案格式傳送，例如限制 Word 文件（.doc/.docx）、PDF 文件（.pdf）不能在網路中傳送。不過這種方法較陽春，只要稍微對電腦熟悉的使用者就可以透過更改副檔名輕易跳過阻擋。

2.關鍵字過濾：限制自定關鍵字及特殊關鍵字的內容傳送，例如若檔案中有出現「總計」則會阻擋改檔案傳遞，此技術類似於中國防火長城（Great Firewall, GFW），當傳遞者傳送到特定關鍵字時就會阻擋造成傳送失敗；另外也可能使用正規表達式（regular expression），針對特定格式如信用卡號碼或身分證字號加以過濾。

3.結構化資料指紋（Structured Data Fingerprinting）：對敏感資料以 hash 方式製作指紋（Fingerprint），當使用者傳送這些資料時就會被系統自動判別出。另外也可能使用標記（Tag）法，將機密檔案加上標籤，系統只要追蹤有標記的檔案即可。

4.機器學習方法：使用異常偵測（Anomaly-based Detection）為基礎的方法，學習使用者平日的操作，當發現使用者操作方法異常時即可進行阻擋。

5.另外也會搭配防毒軟體、防火牆、IDS/IPS 防止攻擊者入侵造成機密資料外洩。

(三)將 DLP 與 DRM 功能異同說明如下：

1.相同：保護組織機密資料安全，避免敏感資料外洩，達到資訊安全的機密性。

2.相異處整理如下表：

	DLP	DRM
系統目標	避免內部機密資料傳送到組織外。	避免傳送到組織外的資料被未授權的開啟。
使用方法	在電腦或網路上安裝特定軟體，用監控技術偵測使用者的外洩行為，並在使用者操作時阻止。	針對單一檔案進行加密，有權限的使用者才可以檢視（或修改）。
優點	(1)導入後可對整個組織進行全面性防護，不須擔心有人為漏洞。 (2)提供資料流動軌跡及電腦詳細操作紀	(1)可以針對不同檔案單獨設置權限。 (2)有需要的使用者才需要安裝相關軟體，沒有此需求的使用者可以直接忽

	錄，以利數位鑑識採證與後續改善。	略。 (3)檔案即使外洩未授權使用者仍無法存取。
缺點	(1)直接套用到一台電腦（或一個網路中）所有的檔案。 (2)需要在每台電腦中安裝。 (3)機密檔案一經外洩則無法防堵。	(1)可能因為使用者操作疏失造成漏洞。 (2)無法記錄檔案的操作紀錄，因此改善策略很難進行。
適用性	安全控管嚴格的大型組織。	僅有部分部門擁有機密資料的組織。

四、數位鑑識（Digital Forensics）是網路安全防禦的重要手段之一，請回答：

（一）何謂數位鑑識？請詳細說明其意義，然後列出並解釋從事數位鑑識時該遵循那些原則？（15分）

（二）電腦犯罪者為了避免被偵測，常會採取反鑑識作為。反鑑識的方法可分為幾類？請各舉例說明之。（10分）

答題關鍵	本題測驗考生對數位鑑識相關的知識。
考點命中	1.《高點資通安全講義》第二回，金乃傑編撰，頁 98-101。

【擬答】

(一)數位鑑識是針對具有使用紀錄的電子設備，如電腦、智慧型手機、大型伺服器、防火牆等，應用嚴謹的程序及科技的方法從中的數位證據，如圖片、音樂、簡訊、檔案、封包、影像等，進行蒐證、檢驗、認證、保存與分析，做為日後法庭能據以判別的法律依據。從事數位鑑識的原則如下：

1.可驗證性：其他鑑識人員若按照蒐證人員宣稱的驗證程序，應可以得出相同的結果。

2.完整性：蒐證時的數位證據，先記錄其雜湊值（Hash Value）於表單中，若法庭對於蒐證的數位證據有疑慮時，只要驗算出的雜湊值和原始紀錄的值一致，就可以證明該數位證據並未被竄改。

3.證物鏈（Chain of Custody）監管：從蒐證現場到法庭的過程中，每一個蒐證和保管的過程環節，都必須清楚被記載在相關的表單中，確保搜到的證物沒有被污染。

4.最小更動原則：鑑識人員必須遵守鑑識流程，非不得已，絕不任意變更電腦狀態，並讓電腦系統維持最小程度的變更。

(二)反鑑識（Anti-forensics）是對資料、工具或攻擊者進行攻擊，進而干擾鑑識工作，避免被取得證物的流程。可分為三類，舉例說明如下：

1.資料隱藏：對敏感資料加密（Encryption），致使鑑識人員無法破解，而無法從中取得數位證據；另外，也可以使用隱寫術（Steganography），將敏感資料藏在圖片、音訊或其他檔案中，使鑑識人員沒有注意到，而逃過鑑識作業。

2.資料抹除：使用資料刪除工具如 Eraser，在鑑識前徹底抹除敏感資料。因為一般操作電腦的「刪除」僅是移除檔案連結、將存放檔案的區域標示為可以寫入，但若沒有新資料寫入，則磁碟內容不會被異動，因此可以使用如 Final Data 等工具進行還原。專業的資料刪除工具可以將磁碟中存放敏感資料的區域多次重覆寫入，以完全清除敏感資料的痕跡，甚至也可以清除緩衝區或 log 的資料，讓鑑識人員沒有發覺有該檔案的存在。

3.蹤跡混淆：創造錯誤資訊，例如變動檔案修改時間、調整 log，誤導鑑識人員；另一種方法為改變數位簽章，此時系統會認為資料有誤，致使資料傳送者與資料接收者都無法信任這個檔案，造成檔案無法被系統開啟；另一種類似的作法是改變 hash 檢查碼，也會使檔案不被信任而無法作為證據。