《資料處理概要》

一、何謂SQL injection？要如何避免SQL injection的攻擊？（20分）

試題評析	SQL Injection題型為資料庫+資訊安全議題，96年高考統計資料處理科目曾經出現過類似考題，有研讀講義與考古題的考生，此題應可應付。
考點命中	《高上資料處理講義》第四回，唐箏編撰，頁117-118。

答：

(一)SQL Injection通常被翻譯成「資料隱碼」攻擊，屬於Input Validation問題。它是描述一個利用輸入欄位寫入特殊SQL程式碼攻擊應用程式的動作。例如：網頁登入頁面，未檢查使用者輸入欄位文字，以致攻擊者透過在輸入欄位輸入特定程式語法，進行攻擊的行為。

換言之，只要提供給使用者輸入的介面，又沒有做到相當嚴密的輸入資料型態管制，就有可能會遭受這種行為的攻擊。

(二)驗證用戶的輸入值，重點在於解析查詢語句，要注意原程式裡對參數值的分析，特別是單引號、注釋符號等的過濾，以避免原來的查詢語句被駭客加註其他查詢語句。此外，資料庫對於連線帳號的權限控管規範，若無特殊必要，不需賦予過大權限，以避免完整資料庫內容遭入侵。

二、考慮下列關聯式資料庫的三個table：顧客（Customer）、產品（Product）和交易（Transaction）。他們的結構（schema）定義如下：Customer（cName, cID, address）、Product（pName, pID, price）、Transaction（cID, pID, amount）。（每小題10分，共20分）

(一)顧客「李大同」要買產品「H牌手機」一支，請寫出SQL指令來更新table。

(二)如果有同名同姓的顧客，依(一)的SQL指令其執行結果是否正確？要如何解決？

試題評析	資料庫的SQL語法，時常出現在資料處理考試中，但今年出的是DML的語法，而且屬於較複雜的語法。除非對SQL語法有較深入研究的考生，否則此題得分會較為困難。
考點命中	《高上資料處理講義》第二回，唐箏編撰，頁82。

答：

(一)假設李大同已為既有顧客，則需新增一交易至Transaction表格。語法如下：

```
Insert Into Transaction
Select cID, (Select pID From Product Where pName=' H牌手機'), 1
From Customer Where cName='李大同'
```

(二)若有同名同姓的顧客，上述SQL執行結果會幫同名同姓顧客各買一支H牌手機；因此，解決方式為，應取得顧客唯一的cID，並以cID為條件新增資料至Transaction表格。

三、資料結構中的堆積（heap）是什麼？如何利用堆積來排序（sorting）？請分析堆積排序（heap sort）的時間複雜度。（30分）

試題評析	資料結構的排序，每隔幾年總是會來個一兩題。Heap Tree與Heap Sort前些年出現次數較少，不過課堂總複習才剛複習過，希望考生們印象還清楚。
考點命中	1.《高上資料處理總複習講義》，唐箏編撰，頁12-15。 2.《高上資料處理講義》第四回，唐箏編撰，頁35。

答：

(一)Heap：Heap在資料結構上是一種二元樹(Binary Tree)型態，分為最大堆積樹(Max Heap Tree)與最小堆積樹(Min Heap Tree)。

1.堆積樹(Heap Tree)是一個完整二元樹(Complete Binary Tree)。
2.每一個節點之鍵值大於/小於或等於其子節點之鍵值。
3.因此樹根節點之鍵值是堆積樹中之最大/最小者。

(二)Heap Sort步驟如下：
將N筆紀錄鍵值K0，K1，K2，…，KN-1，依鍵值由大到小不遞增之順序排列之堆積排序法為：
1.將K0，K1，K2，…，KN-1，轉換成完整二元樹。
2.將完整二元樹轉換成堆積樹。
3.輸出樹根鍵值。
4.將樹中最後一個節點搬到樹根。
5.重複步驟2、3、4直到輸出所有鍵值為止。

(三)1.建heap的最差複雜度：O(n)
2.每次輸出最多使用$\lfloor \log i \rfloor$ (floor log i)次比較，i為剩餘的節點數目。
故Heap sort的最差時間複雜度為O(n log n)

四、IP位址（Internet Protocol Address）、MAC位址（Media Access Control Address）和網頁地址（Uniform Resource Locator, URL）各是什麼？為何需要這麼多不同的地址？它們之間如何對應？（30分）

試題評析	本題屬於電腦網路的考題，IP、MAC、URL都是不難的名詞。但需要對幾個名詞的概念清楚，後面兩題應用題才能作正確的回應。
考點命中	《高上資料處理講義》第一回，唐箏編撰，頁54、60、61、116-118。

答：

(一)IP位址：
網絡是由無數的電腦互相連接所組成，為了確保電腦間的資料傳輸正確，每台電腦都有一個「固定而獨有」的識別地址，IP位址即為網際網路上每一台電腦的邏輯位址。IP位址的指派，與電腦所在的網路網段相關，電腦在不同的網域會有不同的IP位址。

(二)MAC位址：
每一個網路介面卡都有一個獨一無二的識別碼，這個識別碼是由六組16進位數字組成的物理位置，也稱為MAC(Media Access Control)Address，透過MAC位址可以在實體上區分每一張網路卡。理論上，全世界沒有兩張卡的MAC Address是相同的。

(三)網址(Uniform Resource Locator，URL)：
簡單的說，URL就是網際網路伺服主機的位址用來指出某一項資訊的所在位置及存取方式；嚴格一點來說，URL就是在網際網路上指明通訊協定及以位址來享用網路上各式各樣的服務功能。類似網路上的門牌號碼。

(四)為何需要這麼多種位址：
URL是使用者通常在瀏覽器上輸入的網址，是人類使用的；IP位址是用來確定電腦所在網路位址，是網路辨識位址用；MAC位址則為網路卡位址，是判斷實體電腦位址用的。同一個MAC位址表是為同一台電腦；同一個IP位址或子網路表示其在同一個特定區域網路中，MAC位址即電腦變動，IP位址可能重複使用；同一個URL表示其對應相同的網路服務，也有可能同一個URL連結至不同IP位址。

(五)之間如何對應：
1.URL與IP位址，透過DNS(Domain Name System)伺服器作對應。網際網路上的網站和IP位址為數眾多，使用者不可能知道每個網站IP位址所在何處，而DNS類似網路電話簿，可以將使用者輸入的URL網址部份轉換為IP位址，接著指引前往所需網站。
2.IP位址與MAC位址：透過ARP協定(Address Resolution Protocol)與RARP協定(Reverse Address Resolution Protocol)來對應。ARP協定主要為將IP位址對應到它的MAC位址；RARP協定則反向將一台只知道自己MAC位址的機器使用RARP協定來找出其IP位址。