選擇題

1. 有關於「資料隱碼」（SQL Injection），下列敘述何者為誤？
(1) 特別容易發生在以資料庫儲存帳號和密碼的網頁認證系統。
(2) 除了破解認證保護外，其它形式的資料隱碼也可能造成整個資料表的遺失。
(3) 只會發生在微軟的資料庫。
(4) 最簡單的解法，是刪除使用者輸入的單引號。

2. 有關於 ASP 與 Access 資料庫的整合，下列敘述何者為誤？
(1) 我們可由 Access 資料庫的圖形使用者介面，產生所要的查詢，再轉換成 SQL 指令，然後再貼到 ASP 的程式碼裡面。
(2) Access 資料庫的運算效率比 MS SQL Server 較差。
(3) 我們可以將網頁伺服器和資料庫伺服器放在兩台不同的機器。
(4) Access 資料庫所用的 SQL 語法與 MS SQL Server 相去甚遠。

簡答題

1. 請列舉三點，說明將網頁資料儲存於資料庫的好處。

2. 要讓 ASP 程式碼和資料庫溝通，首先要知道資料庫所在位置以及其相關資訊，有兩種方法可以達成此任務，請簡單說明，並解釋這兩個方法的優缺點。

3. ODBC 的全名為何？意義為何？

4. SQL 的全名為何？此程式語言的功能與特性？

5. 在 Access 資料庫中，text 欄位和 memo 欄位有什麼重要差異？

6. 在 Access 軟體內執行 SQL 指令時，如何比對一個字元？如何比對多個字元？

7. 在 ASP 程式碼內執行 SQL 指令時，如何比對一個字元？如何比對多個字元？

8. 有關於「資料隱碼」（SQL Injection）：

a. 請簡單說明（不超過五句）什麼是「資料隱碼」？

b. 請簡單說明（不超過五句）如何避免這個問題？

9. 對於一般的帳號密碼認證，如何使用資料隱碼的方式來進行駭客任務？

10. 假設有一個資料庫包含兩個資料表：

- Player 包含球員的資料，其中 TeamID 是球員所隸屬的籃球隊代號（載明在 Team 資料表），Percentage 是投籃的命中率。
- Team 包含籃球隊的資料，其中 WinNo 是本季的贏球次數。

相關內容如下：

資料庫 "example/database/basketball.mdb"

資料表 "Player" 的內容

ID	NickName	Name	TeamID	Percentage
1	jean	吳志銘	1	38.25
2	jones	張秤嘉	5	49.77
3	ben	陳孜彬	1	50.26
4	asser	林惠娟	3	37.22
5	window	李宜揚	1	36.67
6	roger	張智星	2	25.88
7	cosh	許文豪	6	70.98
8	banny	洪鵬翔	6	88.97
9	shyba	邱中人	5	67.45
10	batty	楊璧如	4	65.55
11	joey	許嘉晉	3	47.65
12	roland	吳瑞千	1	55.87
13	sony	林頌華	1	54.77
14	beball	葉佳慧	5	33.33

資料表 "Team" 的內容

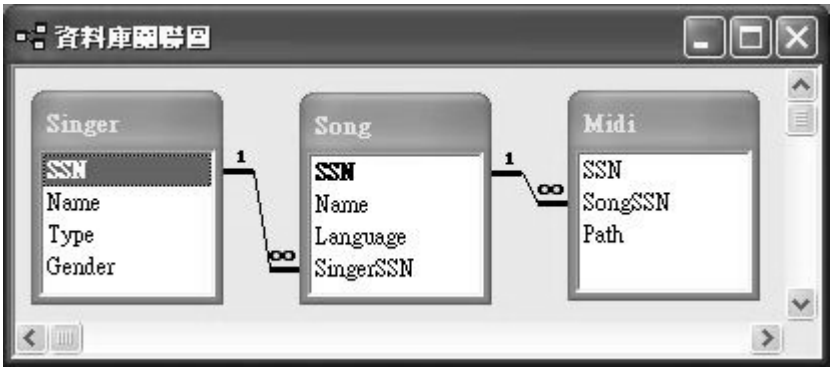
ID	Name	WinNo
1	台北隊	12
2	新竹隊	7
3	台中隊	10
4	南投隊	12
5	台南隊	17
6	高雄隊	16
7	澎湖隊	11

資料庫 "example/database/basketball.mdb"					
資料表 "Player" 的內容					資料表 "Team" 的內容
15	gavins	林政源	5	55.65	
16	jojo	陳俊傑	5	44.65	
17	jtchen	陳江村	3	48.76	
18	Gao	高名揚	1	67.88	
19	Wayne	陳智偉	7	65.87	
20	chingz	陳晴	5	57.28	

請根據此資料庫寫出符合下列需求的最簡單 SQL 指令：

a. 所有球隊資料
b. 所有球隊資料，但只抓前三筆
c. 綽號為 gavins 的球員姓名及命中率
d. 隊名以「台」開頭的球隊資料
e. 「姓陳且名字有三個字」的球員姓名及命中率
f. 「勝場數大於 10」的球隊名稱及其勝場數
g. 「勝場數大於 10」的球隊名稱及其勝場數，並根據勝場數由大到小排列
h. 「球隊代碼為 5」的球員命中率排行榜
i. 每一隊的球員命中率排行榜
j. 「勝場數大於 10」的球隊總數
k. 所有球員的最高命中率
l. 具有最高命中率的球員資料
m. 每個球隊的球員人數及平均命中率
n. 每個球隊的球員人數，但只顯示球員人數大於 2 位的資料
o. 台北隊的球員資料
p. 高雄隊和台中隊的射手排行榜
q. 每個球隊的相關統計數字

11. 假設我們有一個資料庫，內含三個資料表，他們的關聯圖如下：



請寫出最簡潔的 SQL 指令，以執行以下查詢。

a. 列出所有的國語歌曲

b. 所有歌曲共包含哪幾種不同語言（不可重複）

c. 歌曲共包含幾種不同語言

d. 唱過台語歌的歌星（不可重複）

程式題

請使用本章所學到的 JavaScript/JScript 程式技巧（用於伺服器端）來完成下列作業：

1. **(***) 利用 SQL 從資料庫抓資料**：本題作業的目的，是讓同學熟悉 Access 資料庫的使用以及 SQL 的語法，並將 SQL 命令所回傳的資料顯現在網頁上。所用到的資料庫是 example/databsae/song.mdb，共包含三個資料表 (Singer, Song, Midi)， 表和表之間有關聯性存在，此關聯性可由「工具/資料庫關聯圖」來顯示。 每個表的欄位名稱應可望文生義， 其中 SSN 代表 System Serial Number，是每筆資料在資料表中獨一無二的編號。你的工作，就是產生一個網頁 selectQuery01.asp，包含下列連結，當使用者點選某一個連結時，你的程式碼就會自動從資料庫中取出下列資料，並顯示在另一個網頁上。

a. 歌曲共包含哪幾種不同語言
b. 唱過台語歌的歌星
c. 伍佰所唱的台語歌
d. 伍佰所唱的國語歌的總數
e. 唱過台語歌曲的女藝人及所唱的台語歌
f. 張宇所唱的國語歌及其 Midi 檔案的路徑
g. 張宇所唱的國語歌的 Midi 檔案的總數
h. 歌曲共包含幾種不同語言
i. Song 中重複的歌名
j. 有歌名卻沒有 Midi 檔的歌曲資料（提示：此題會用到 Outer Join）

注意事項：

- 可以使用 listQueryResult() 函數來進行資料列表。
- 資料庫中「查詢」的部份，包含前三小題作業要用到的 SQL 命令，同學可參考之。
- 所有的作業，都可以經由 SQL 命令來取出所要的資訊。
- 我們用的資料庫是 Office 2000 中的 Access，如果你還在用 Office 97，那就該升級了。
- 助教在測試你的程式時，會以另一個資料庫（欄位相同但資料不同）來進行測試。

2. (***) 設計有用的查詢：如果你做過上一題，應該就會對 SQL 指令及 example/databsae/song.mdb 資料庫有基本的瞭解。請延續上題的查詢及相關的 SQL 指令，創造出五個更複雜且「有意義」的查詢，並將此查詢的中文意義及相關的 SQL 指令列在一個 ASP 網頁 selectQuery02.asp，當使用者點選時，可將查詢結果顯示在另一個新開啟的視窗。（本題並沒有標準答案，請各位盡量發揮創意！）

3. **(***) SQL 語法在 MS Access 與 MS SQL Server 的差異：**雖然說 SQL 是一個標準化的資料庫程式語言，但是在不同的軟體，也會有些差異。本作業麻煩各位同學到 Google 大師搜尋一下，比較看看 SQL 語法在 MS Access 與 MS SQL Server 這兩個資料庫軟體的差異，並以列表方式，逐一說明其差異所在及可能造成的影響。

4. **(***) 以資料庫設計留言版：** 本作業之目的是讓同學更進一步瞭解 ASP 與資料庫的整合，並能對資料庫的資料進行各種處理，含列表及新增。本作業的成品是一個 Web 留言版，你必須從讀者（或伺服器）取得下列資訊，並將之顯示在你的留言版：
   - 由使用者輸入：
     - 貴姓大名
     - 性別
     - 伊媚兒
     - 個人網址
     - 留言內容
   - 由 ASP 程式碼自動抓取：
     - 登錄時間和日期
     - 訪客 IP(是真正的 IP，而非代理伺服器的 IP，可由 Request.ServerVariables("REMOTE_ADDR") 或 Request.ServerVariables("HTTP_X_FORWARDED_FOR") 來取得。)
     - 訪客所用的瀏覽器 (由 Request.ServerVariables("HTTP_USER_AGENT"))
     - 來源網頁 (由 Request.ServerVariables("HTTP_REFERER"))

   注意事項：
   - 本次作業需用 ASP 完成（你可以任選 JScript 或 VBScript 或 PerlScript），但不可以使用 CGI 來完成。

- 留言版資料必須存在資料庫之中，網頁必須具備「新增」及「列表」的功能。
- 必須防範別人留下一些亂七八糟的標籤，造成網頁格式的混亂。（可使用 Server.HTMLEncode() 函數。）
- 不須要對姓名及留言進行基本的表單驗證。
- 我相信你可以在網路上找到很多相關範例及原始碼。這裡是一個不完全的範例：
  - 這裡有一個半成品，請多加利用，並歡迎測試！
  - 所有的程式碼都放在 guestBook.zip，請多加抄襲！

5. (***) 以資料庫設計留言版之二：除了滿足前一題的要求外，你的網頁還需要具備下列功能：

a. 加上留言管理功能：可讓管理員不需開啟資料庫，直接經由網頁輸入密碼後，即可有「修改」及「刪除」的權限。（進行修改時，必須把原資料列出在表單之中。）

b. 自動分頁功能，當留言數量龐大時，可允許使用者選擇使用分頁功能來瀏覽留言， 並可允許使用者設定每一頁留言的數目。

c. 加入搜尋功能，允許使用者找出含有搜尋字串的留言資料。為簡化起見，可以只使用一個搜尋字串，尋找所有的欄位。（為便於察看結果，建議在回傳內容中將符合的字串變色。）

d. 利用 cookie 功能記錄使用者留言時所登錄的基本資料， 並於下次使用者欲留言時，由系統預先將資料放置於 input 欄位中。

6. (***) 以資料庫設計線上通訊錄：本作業之目的是讓同學更進一步瞭解 ASP 與資料庫的整合，並能對資料庫的資料進行各種處理，含查詢、新增、修改、刪除。本作業的成品是一個 Web 的個人通訊錄，你必須從使用者（應該就是你自己）取得下列資訊，存入資料庫，並將之顯示在你的通訊錄：

- 由使用者輸入的聯絡人資訊：
  - 貴姓大名
  - 性別
  - 伊媚兒
  - 網址
  - 電話
  - 大哥大
  - 地址
  - 類別（例如高中同學、親戚、社團同學等）
- 由 ASP 程式碼自動抓取：
  - 登錄時間和日期
  - 訪客 IP(是真正的 IP，而非代理伺服器的 IP，可由 Request.ServerVariables("REMOTE_ADDR") 或 Request.ServerVariables("HTTP_X_FORWARDED_FOR") 來取得。)
  - 訪客所用的瀏覽器 (由 Request.ServerVariables("HTTP_USER_AGENT"))
  - 來源網頁 (由 Request.ServerVariables("HTTP_REFERER"))

請注意：

- 本次作業需用 ASP 完成（你可以任選 JScript 或 VBScript 或 PerlScript），但不可以使用 CGI 來完成。
- 無論顯示或修改通訊錄等，都需經過密碼認證。
- 必須具有四大功能：列表、新增、修改、刪除。（進行修改時，必須把原資料列出在表單之中。）
- 不需要進行表格驗證。（自己輸入的東西，自己負責就可以了！）
- 我相信你可以在網路上找到很多相關範例及原始碼。這裡是留言版的範例，其功能和個人通訊錄非常接近：

- 這裡有一個半成品，請多加利用，並歡迎測試！
- 所有的程式碼都放在 guestBook.zip，請多加抄襲！

7. **(***) 以資料庫設計線上通訊錄之二**：除了滿足前一題的要求外，你的網頁還需要具備下列功能：
   - 分頁功能:：當通訊錄資料數量龐大時，可允許使用者選擇使用分頁功能來瀏覽留言。
   - 排序功能：可根據不同的欄位（如類別、性別、姓名等）來進行排序顯示。
   - 搜尋功能：允許使用者根據不同欄位來進行搜尋。