臺灣銀行 108 年新進人員甄試試題

甄試類別【代碼】:程式設計人員(一)【O8605】、程式設計人員(二)【O8606】、資訊人員【O8608】
科目三：程式設計(含安全程式設計)

＊入場通知書編號：_____

注意：①作答前先檢查答案卷，測驗入場通知書編號、座位標籤、應試科目是否相符，如有不同應立即請監試人員處理。使用非本人答案卷作答者，不予計分。
②本試卷為一張雙面，非選擇題共 4 大題，每題各 25 分，共 100 分。
③非選擇題限以藍、黑色鋼筆或原子筆於答案卷上採**橫式**作答，**請參照答案卷所載注意事項，於各題指定作答區內作答，並標明題號及小題號**。
④**請勿於答案卷上書寫姓名、入場通知書號碼或與答案無關之任何文字或符號。**
⑤本項測驗僅得使用簡易型電子計算器（不具任何財務函數、工程函數、儲存程式、文數字編輯、內建程式、外接插卡、攝（錄）影音、資料傳輸、通訊或類似功能），且不得發出聲響。應考人如有下列情事扣該節成績 10 分，如再犯者該節不予計分。1.電子計算器發出聲響，經制止仍執意續犯者。2.將不符規定之電子計算器置於桌面或使用，經制止仍執意續犯者。
⑥**答案卷務必繳回，未繳回者該節以零分計算。**

第一題：【解答方式以 JAVA+SQL、.NET C#+SQL 二擇一】

下列 Product 資料表為某公司產品資料表，請撰寫一程式可讓使用者輸入產品名稱作為查詢條件，查詢後，顯示出產品名稱中所有包含查詢條件的產品資料（例如：輸入查詢條件為「茶」，則顯示所有產品名稱包含「茶」的資料，如下列之「查詢結果範例」)。【15 分】程式設計時需考量避免資料隱碼攻擊（SQL Injection）。【10 分】

資料表名稱：Product		
產品名稱	產品分類	價格
水果茶	飲料	50
洋芋片	零食	30
檸檬愛玉	飲料	60
冰咖啡	飲料	15
綠茶蛋糕	點心	80

查詢結果範例：

產品名稱	產品分類	產品價格
水果茶	飲料	50
綠茶蛋糕	點心	80

第二題：【解答方式以 JAVA+SQL、.NET C#+SQL 二擇一】

當網頁輸入帳號密碼時，在資料庫中如果有吻合的資料，代表帳號密碼是對的。如果設計的程式碼如下，會產生何種問題？應該如何修改？【25 分】

JAVA codes:

```
protected final void Verify_Click(object sender, EventArgs e) {
    string connectionString = "myConnectionString";
    int count;
    SqlConnection cn = new SqlConnection(connectionString);
    cn.Open();
    string sqlStatement = ("Select Count(1) From SomeTable Where ID= \'" +
        (this.Id.Text + ("\' AND Password= \'" +
            (this.Password.Text + "\'"))));
    SqlCommand sqlCommand = new SqlCommand(sqlStatement, cn);
    count = ((int)(sqlCommand.ExecuteScalar()));
    if (count > 0) this.Result.Text = "Pass";
    else this.Result.Text = "Invalid Id or Password";
}
```

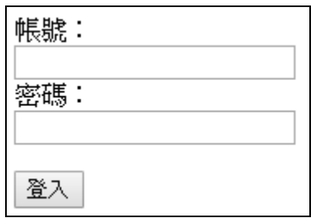
.NET C# codes:

```
protected void Verify_Click(object sender, EventArgs e) {
  string connectionString = @ "myConnectionString";
  int count;
  using(SqlConnection cn = new SqlConnection(connectionString)) {
    cn.Open();
    string sqlStatement = @ "Select Count(1) From SomeTable Where ID= '" + this.Id.Text + "' AND
Password= '" + this.Password.Text + "'";
    SqlCommand sqlCommand = new SqlCommand(sqlStatement, cn);
    count = (int) sqlCommand.ExecuteScalar();
  }
  this.Result.Text = (count > 0) ? "Pass" : "Invalid Id or Password";
}
```

【請接續背面】

第三題：【解答方式以 JAVA+SQL、.NET C#+SQL 二擇一】

請撰寫一程式，當使用者按下登入後，程式可接收使用者所輸入的帳號與密碼，並透過 User 資料表判斷所輸入的帳號與密碼是否正確。若帳號與密碼正確則導向首頁(home.html)，若帳號與密碼錯誤則顯示「帳號或密碼錯誤」提示訊息。【20 分】程式設計時需考量避免跨網站指令碼攻擊（XSS, Cross-Site Scripting）。【5 分】



資料表名稱：User		
欄位名稱	屬性	欄位說明
ID	varchar(10)	帳號
PWD	varchar(10)	密碼

第四題：【解答方式以 JAVA+SQL、.NET C#+SQL 二擇一】

請使用 JAVA 或.NET C#撰寫 regular expression 來過濾 SQL Injection 及 XSS 攻擊字串。【25 分】