```
public DataTable GetCustomerInfo(string id)
{
  var dt = new DataTable();
  using (var conn = new SqlConnection("...")) // Connection string is hardcoded
  {
    conn.Open();
    var sql = "SELECT * FROM Customer WHERE id = '" + id + "'";
    using (var da = new SqlDataAdapter(sql, conn))
    {
      da.Fill(dt);
    }
  }
  return dt;
}
```

1. In your own words, what is the primary purpose of this function?

   (ฟังค์ชั่นนี้มีหน้าที่หลักอะไรในความคิดของคุณ)

   - ฟังค์ชั่นนี้มีหน้าที่หลักในการในการ ค้นหาข้อมูลลูกค้า (อ้างอิงจาก SELECT * FROM Customer) ผ่านการนำค่าผ่านเข้า parameter id ของฟังค์ชั่น โดยตัวฟังค์ชั่นจะทำการเชื่อมต่อ database และทำการป้อนคำสั่ง SQL แก่ database เพื่อใช้คำสั่ง SELECT ในการค้นหาข้อมูลลูกค้าผ่าน ID ที่ป้อนเข้ามาและสุดท้ายตัวฟังค์ชั่นจะส่งข้อมูลที่ SELECT มาได้กลับไปในรูปแบบ DataTable

-

2. Identify at least three distinct problems with this implementation. Consider aspects such as security, maintainability, and performance.

   (เขียนปัญหามาอย่างน้อย 3 ปัญหาเกี่ยวกับโค้ดนี้ โดย คำนึงถึงด้านต่าง ๆ เช่น ความปลอดภัย การดูแลรักษา และประสิทธิภาพในการทำงาน)

   - 1) มีการ Hardcode ผ่านการเชื่อมต่อฐานข้อมูลส่งผลให้เมื่อเปลี่ยนตัวฐานข้อมูล ทำให้การเปลียนชื่อของฐานข้อมูลหรือการเพิ่ม Parameter ต่าง ๆ เพื่อการเชื่อมต่อต่างจัดการได้ยาก และอาจส่งผลให้ข้อมูลสำคัญต่าง ๆ เกี่ยวกับฐานข้อมูลเช่น Password ของฐานข้อมูลหลุดออกไปได้หากตัว Souce code ถูกเปิดเผย

     2) เสี่ยงต่อการ SQL Injection เนื่องจากการใช้คำสั่งของ SQL นั้นใช้โดยการผ่านค่า Parameter id ที่รับเข้ามาไปเป็น String ตรง ๆ ซึ่งทำให้การทำ SQL injection นั้นสามารถทำได้ผ่านการส่งคำสั่ง SQL อื่น ๆ ผ่าน Parameter id ได้

     3) ไม่มีการทำ Error handling เพื่อหาสาเหตุของบัคเมื่อเกิดขึ้น

     4) ไม่มีการเช็ค Parameter ทำให้ไม่มีการเช็คอาจมีการทำงานของฟังค์ชั่นแม้ตัว Parameter ที่ส่งนั้นจะเป็นค่าว่าง

     5) ทุกการเรียกใช้ฟังค์ชั่นจะมีการเชื่อมต่อฐานข้อมูลทุกครั้งซึ่งอาจส่งผลแก่ประสิทธิภาพโดยรวม

3. For each problem identified, briefly propose a specific improvement.

(บอกวิธีการแก้ปัญหาแต่ละปัญหา)

- 1) ปัญหา Hardcode ควรใช้วิธีการดึงค่าต่าง ๆ ในการเชื่อมต่อดาต้าเบสผ่านไฟล์ bin ข้างนอกเช่นไฟล์ .json หรือไฟล์ .env ต่าง ๆ ตัวอย่าง เช่น

  using (var conn = new

  SqlConnection(_configuration.GetConnectionString("DefaultConnection")))

  โดยตัวอย่างที่ภายในไฟล์ .json ควรจะมีคือ

  ```
  {
  "ConnectionStrings": {
      "DefaultConnection":
      "Server=localhost;Database=MyAppDB;Trusted_Connection=true;",
      "BackupConnection": "Server=backup-server;Database=MyAppDB;User
      Id=myuser;Password=mypass;"
      },
      "Logging": {
              "LogLevel": {
                      "Default": "Information"
              }
      }
  }
  ```

2) ปัญหา SQL injection ควใช้วิธีการ parameterize query แทนการใส่ค่าผ่าน string ตรง ๆ เพื่อให้ Database engine สามารถแยกแยะได้ว่าส่วนไหนคือ SQL command กับ data ได้อย่างชัดเจนที่เช่น

```
var sql = "SELECT * FROM Customer WHERE id = @id";
var command = new SqlCommand(sql, conn);
command.Parameters.AddWithValue("@id", id);
```

3) ปัญหาการ Error Hanling สามารถแก้โดยทำการ Try catch ครอบทุกคำสั่งในฟังค์ชั่น

4) ปัญหาการเช็ค Parameter สามารถแก้ได้โดยการเช็คค่า Parameter เมื่อฟังค์ชั่นทำงาน เช่น

```
if (string.IsNullOrWhiteSpace(id))
    throw new ArgumentException("Customer ID cannot be null or empty");
```

5) ปัญหาการเชื่อมต่อฐานข้อมูลทุกครั้งที่ฟังค์ชั่นทำงานสามารถแก้ได้โดยการเพิ่ม connection string เข้าไปในไฟล์ .json หรือ commad line ที่ใช้ในการเชื่อมต่อฐานข้อมูล เช่น

```
"Server=localhost;Database=MyAppDB;Trusted_Connection=true;" +
"Pooling=true;" +  //เปิดใช้ connection pooling
"Min Pool Size=5;" + //connection ขั้นต่ำใน pool
"Max Pool Size=100;" + //connection สูงสุดใน pool
"Connection Timeout=30;" + //timeout สำหรับการเชื่อมต่อ
"Command Timeout=30;" //timeout สำหรับการรัน command
```

Part 4

Briefly describe how a function like the one you built might be used by an employee on an internal web dashboard.

Consider the following points in your description or high-level sketch:

- What input fields would a user (e.g., a customer service representative) need on the

screen to search for customer data?

- After the search is performed, what would the output look like on their screen? (e.g., a table, a profile card, a list of transactions).

- ตัวฟังค์ชั่นที่เขียนขึ้นนั้นควรที่จะใช้เพื่อหาข้อมูลลูกค้าต่าง ๆ ตั้งแต่ชื่อ อายุ เพศ สถานะการสมรส ยอดการซื้อของลูกค้า ออกมาเป็นตาราง และทางที่ดีที่สุดควร export ข้อมูลออกมาเป็นไฟล์ excel ได้ เพื่อให้ผู้ใช้นำไปวิเคราะห์ถึงโอกาสทางธุรกิจต่าง ๆ เช่น การกำหนดโปรโมชั่นในอนาคตหรือการวิเคราะห์หากลุ่มเป้าหมายที่เป็นลูกค้าประจำเป็นต้น