## **Written Test**

### **Question 1:**

You have taken over the management of a web application written in ASP.NET C# MVC. The application requires a username and password to login, and the url to access the system is:

<http://made-up-application.com/>

When a user logs into the application they can view their existing details that are stored in the database by going to the following url:

<http://made-up-application.com/customer/details?customerid=1001>

Here is all of the code used in the details action:

A screen shot of a computer program

Description automatically generated

Please list any improvements you think can be made to the above code.

### **ANS:**

**Use Parameterized Queries:**  The current code is vulnerable to SQL injection attacks since it directly concatenates the “*id”* parameter into the SQL query. Instead, use parameterized queries to prevent SQL injection.

A computer screen shot of a black background with white text

Description automatically generated

**Close Database Connection:** It's essential to close the database connection after performing the query to release resources. Use “*using*” statement to ensure proper disposal of the SQL Connection:

A black screen with white text

Description automatically generated

**Encrypt Passwords:** If the passwords are stored in the database, make sure they are properly encrypted using a strong encryption algorithm. Avoid storing plain text passwords.

### **Question 2**

Given a base URL of <https://made-up-api.com/> for a set of RESTful web services, what URL and HTTP verb might you expect to use to carry out each of the following actions:

* Get a list of all customers.
* Get the details of order number 25.
* Delete the customer with an ID of 133.
* Update a single field for all orders.
* Update all fields for the customer with an ID of 1701.

### **ANS:**

• Get a list of all customers.

URL: https://made-up-api.com/customers

HTTP Verb: GET

• Get the details of order number 25.

URL: https://made-up-api.com/orders/25

HTTP Verb: GET

• Delete the customer with an ID of 133.

URL: https://made-up-api.com/customers/133

HTTP Verb: DELETE

• Update a single field for all orders.

URL: https://made-up-api.com/orders

HTTP Verb: PUT

• Update all fields for the customer with an ID of 1701.

URL: https://made-up-api.com/customers/1701

HTTP Verb: PATCH