

# **Pakistan Institute of Engineering and Applied Sciences**



## **Report**

### **Lab-13: Semester Project**

**Submitted By:** M. Hammad Tahir

**Registration No:** 03-3-1-033-2022

**Course Name:** Internet application development

**Instructor:** Dr. Irfan Hameed

**Problem 1) What are the necessary security features of your semester project? After identifying the security features of your project, prepare a list of at least 07 security features and write a brief description about each of them?**

**Security features:**

The following are the security features of my project:

- **Authentication**

Only authenticated users are allowed to use my system. The system will verify the given credentials by the user from the Database and then allow access to it if authenticated by the system or disallow the access if the credentials are incorrect.

- **Authorization**

There are 4 different roles in this project admin, customer, artist, and employee. Each of them has specific functionalities and access to resources. When the user is logged in, its role is verified by the system and related functionalities are accessible to that user.

- **Secure storage of user's session data:**

During the whole user session, important data is stored in the session state and kept safe on the server which is required for the proper function of the system. This data will not be accessible to the outside world so in this way user data privacy is implemented.

- **Input Validation**

No user is allowed to send bogus data on the server, so it is necessary to implement input validation. So only predictable and accurate data is sent to the server.

- **No SQL injection:**

Our system should be protected from SQL injection attacks, so it is necessary to implement proper SQL on the backend to save users' data from unauthorized access.

- **Path Traversal Protection:**

There should be no path traversal variability in the system. Such that no user can access the pages related to other roles by simply typing the URL of that page.

- **Broken access control protection:**

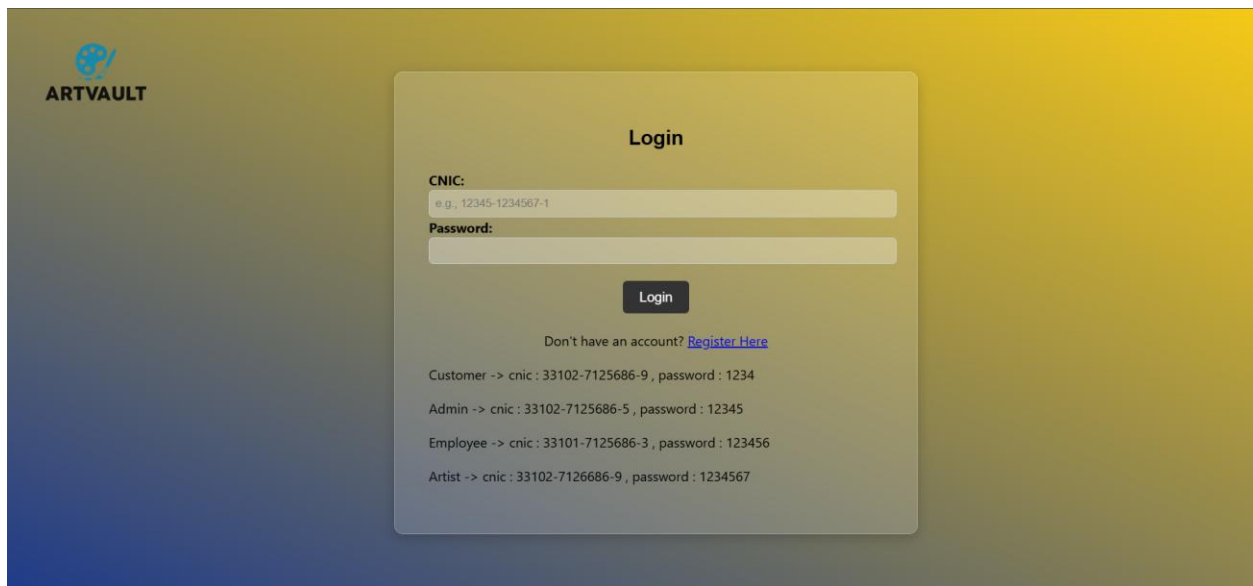
Enforce server-side controls that users can only modify and access their own data not the data of other people.

**Problem 2) Implement identified security features for your project and make a live demonstration available.**

A live demonstration is available for this problem

**Problem 3) Develop test cases for all security features and prepare a report about testing of security features?**

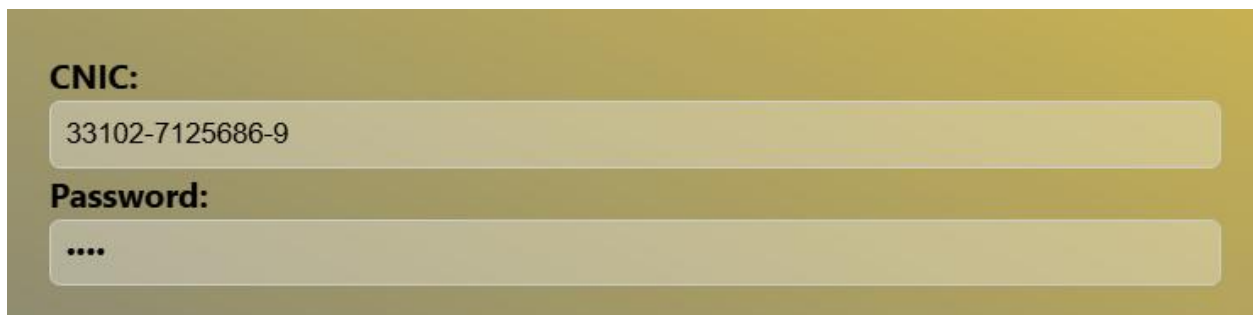
### Authentication:



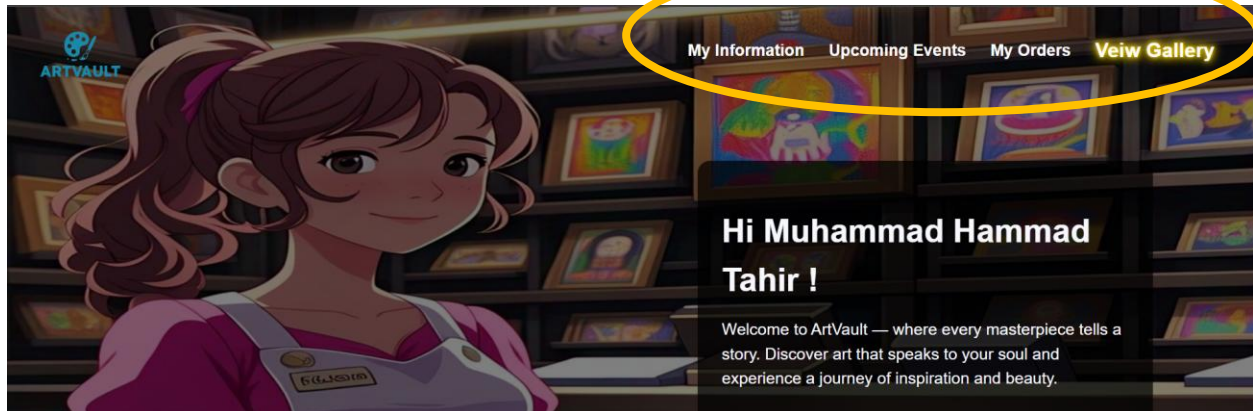
The screenshot shows the ARTVAULT Login page. The page has a yellow and blue gradient background. In the top left corner, there is a logo with a globe icon and the text "ARTVAULT". The main content is a white login form with the title "Login". It contains two input fields: "CNIC:" with a placeholder "e.g., 12345-1234567-1" and "Password:". Below the password field is a "Login" button. Under the button, there is a link "Don't have an account? [Register Here](#)". At the bottom of the form, there are four lines of text providing test credentials: "Customer -> cnic : 33102-7125686-9 , password : 1234", "Admin -> cnic : 33102-7125686-5 , password : 12345", "Employee -> cnic : 33101-7125686-3 , password : 123456", and "Artist -> cnic : 33102-7126686-9 , password : 1234567".

### Authorization:

#### As Customer

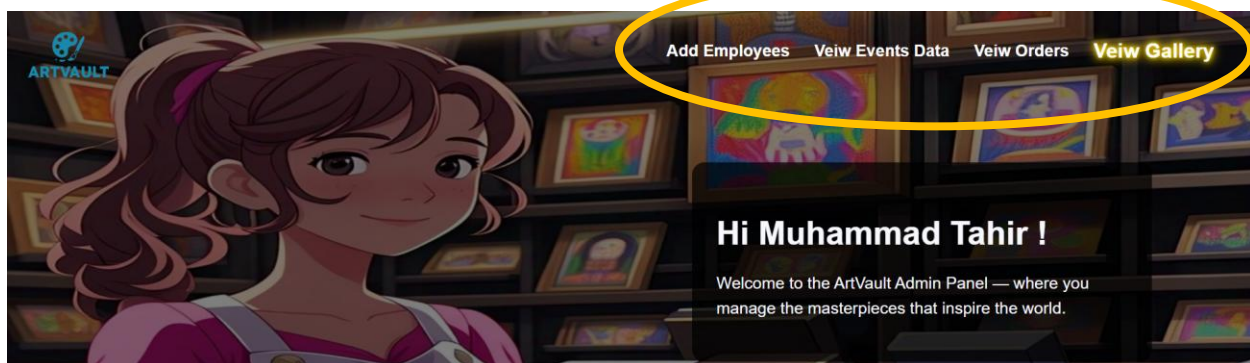


The screenshot shows the ARTVAULT Authorization form for a Customer. The form is white and has a yellow and blue gradient background. It contains two input fields: "CNIC:" with the value "33102-7125686-9" and "Password:" with four dots "....".



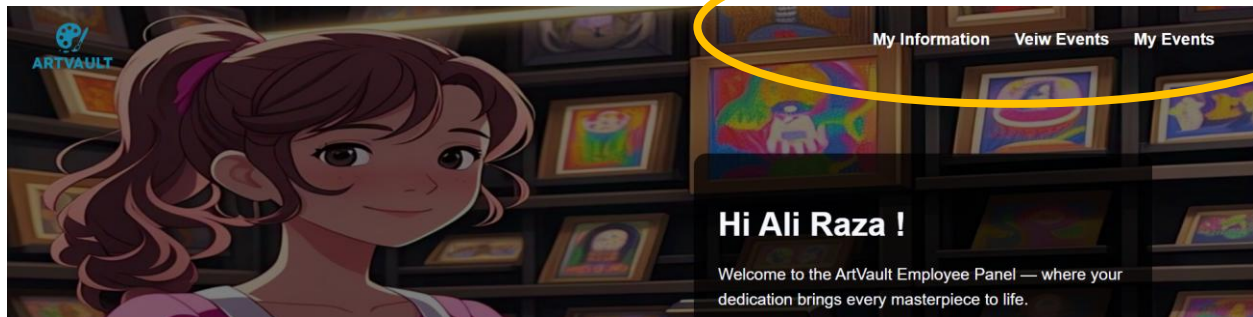
As admin:

The screenshot shows the ArtVault Admin Panel login form. The background is a solid yellow color. At the top, the word "Login" is written in a large, bold, black font. Below it, there are two input fields. The first field is labeled "CNIC:" and contains the text "33102-7125686-5". The second field is labeled "Password:" and contains five dots. The form is simple and clean, with a focus on the login fields.



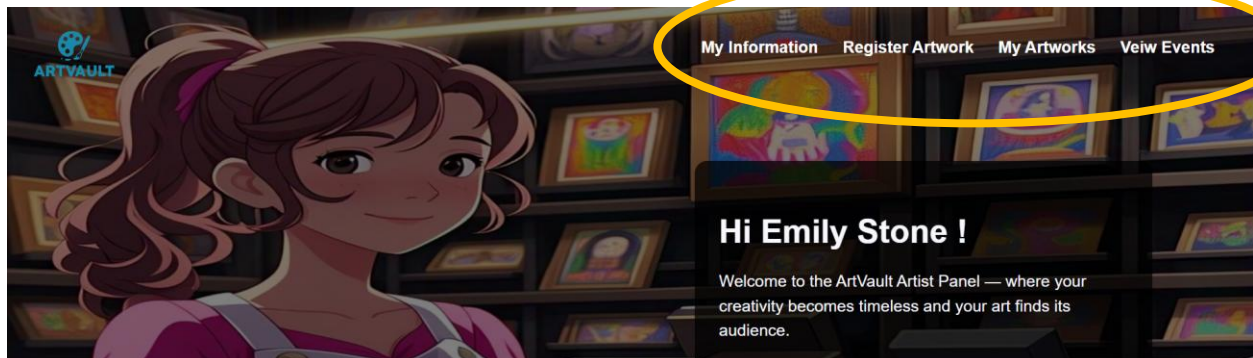
As a employee:

The screenshot shows the ArtVault employee login form. The background is a solid yellow color. At the top, the word "Login" is written in a large, bold, black font. Below it, there are two input fields. The first field is labeled "CNIC:" and contains the text "33101-7125686-3". The second field is labeled "Password:" and contains five dots. At the bottom of the form, there is a dark grey button with the word "Login" in white text.



As a artist:

This screenshot shows the ArtVault Login page. The background is a solid olive green color. The word 'Login' is centered at the top in a large, black, sans-serif font. Below it, the label 'CNIC:' is followed by a text input field containing the value '33102-7126686-9'. Underneath, the label 'Password:' is followed by a password input field with masked characters '.....'. At the bottom center, there is a dark grey button with the word 'Login' in white text.



## Secure storage of user's session data:

```

Try
    con.Open()
    dr = cmd.ExecuteReader
    If dr.Read() Then
        message_box.Style.Add("opacity", "1")
        message_box.InnerText = "Login Successful"
        Authenticated = True
        Session_Cnic = dr("PERSON_ID")
        Session_Password = dr("PASSWORD")
        Session_Role = dr("ROLE")
        First_Name = dr("FIRST_NAME")
        Last_Name = dr("LAST_NAME")
        Session("Cnic") = Session_Cnic
        Session("Password") = Session_Password
        Session("Role") = Session_Role
        Session("Authenticated") = Authenticated
        Session("First_Name") = First_Name
        Session("Last_Name") = Last_Name
    Else
        message_box.Style.Add("opacity", "1")
        message_box.InnerText = "CNIC or Password is Incorrect"
        is_error = True
    End If
End Try

```

Session state

## Input Validation

```

<h2>Login</h2>

<div class="login-container">
    <div runat="server">
        <label for="person_id">CNIC:</label>
        <input id="person_id" type="text" placeholder="e.g., 12345-1234567-1" class="form-control" runat="server" required="required" pattern="\d{5}-\d{7}-\d{1}" />
    </div>

    <div runat="server">
        <label for="password">Password:</label>
        <input id="password" type="password" class="form-control" runat="server" required="required" />
    </div>
</div>

```

Client side input validation

**Login**

**CNIC:**

**Password:**

Please fill out this field.

**Login**

**CNIC:**

**Password:**

Please match the requested format.



**Input server-side validation:****Code:**

```

<%@ Page Language="VB" AutoEventWireup="false" CodeFile="Registration.aspx.vb"
Inherits="_Default" %>

<!DOCTYPE html>
<html xmlns="http://www.w3.org/1999/xhtml">
<head runat="server">
    <title>Register</title>
    <link rel="icon" type="image/png" href="logo_new.png" />
    <link rel="stylesheet" type="text/css" href=" ../StyleSheet.css" />
</head>
<body>
    

    <form id="form1" runat="server">

        <div id="message_box" runat="server"></div>

        <h2>Register</h2>

        <div class="grid-container">
            <div runat="server">
                <label for="person_id">CNIC:</label>
                <input id="person_id" type="text" placeholder="e.g., 12345-1234567-
1" class="form-control" runat="server" required />
                <asp:RequiredFieldValidator ID="RequiredFieldValidator1"
runat="server" ControlToValidate="person_id" ErrorMessage="CNIC is required."
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
                <asp:RegularExpressionValidator ID="RegularExpressionValidator1"
runat="server" ControlToValidate="person_id" ErrorMessage="Invalid CNIC format."
Display="Dynamic" ForeColor="Red" ValidationExpression="\d{5}-\d{7}-
\d{1}"></asp:RegularExpressionValidator>
            </div>

            <div runat="server">
                <label for="first_name">First Name:</label>
                <input id="first_name" type="text" class="form-control"
runat="server" required />
                <asp:RequiredFieldValidator ID="RequiredFieldValidator2"
runat="server" ControlToValidate="first_name" ErrorMessage="First Name is required."
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
            </div>

            <div runat="server">
                <label for="last_name">Last Name:</label>
                <input id="last_name" type="text" class="form-control"
runat="server" />
            </div>

            <div runat="server">
                <label for="email">Email:</label>
                <input id="email" type="email" class="form-control" runat="server"
required />

```

```

        <asp:RequiredFieldValidator ID="RequiredFeildValidator3"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
        <asp:RegularExpressionValidator ID="RegularExpressionValidator2"
runat="server" ControlToValidate="email" ErrorMessage="Invalid email formate."
Display="Dynamic" ForeColor="Red"
ValidationExpression="\S+@\S+\.\S+"></asp:RegularExpressionValidator>
    </div>

    <div runat="server">
        <label for="phone">Phone No:</label>
        <input id="phone" type="text" class="form-control" runat="server"
required />
        <asp:RequiredFieldValidator ID="RequiredFeildValidator4"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="gender">Gender:</label>
        <select id="gender" class="form-control" runat="server" required>
            <option value="M">M</option>
            <option value="F">F</option>
            <option value="O">O</option>
        </select>
        <asp:RequiredFieldValidator ID="RequiredFieldValidator5"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="city">City:</label>
        <input id="city" type="text" class="form-control" runat="server"
required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator6"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="state">State:</label>
        <input id="state" type="text" placeholder="e.g., CA" class="form-
control" runat="server" required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator7"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="postal_code">Postal Code:</label>
        <input id="postal_code" type="text" class="form-control"
runat="server" required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator8"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">

```



```

        <label for="country">Country:</label>
        <input id="country" type="text" class="form-control" runat="server"
required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator9"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="role">Role:</label>
        <select id="role" class="form-control" runat="server" required>
            <option value="" selected disabled>User</option>
            <option value="Artist">Artist</option>
            <option value="Customer">Customer</option>
        </select>
        <asp:RequiredFieldValidator ID="RequiredFieldValidator10"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>

    <div runat="server">
        <label for="password">Password:</label>
        <input id="password" type="password" class="form-control"
runat="server" required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator11"
runat="server" ControlToValidate="email" ErrorMessage="This feild is required"
Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>
</div>

<div class="submit-container" runat="server">
    <input id="add" type="submit" value="Submit" runat="server" />
</div>
</form>
</body>
</html>

```

```


<div runat="server">
        <label for="person_id">CNIC:</label>
        <input id="person_id" type="text" placeholder="e.g., 12345-1234567-1" class="form-control" runat="server" required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator1" runat="server" ControlToValidate="person_id" ErrorMessage="CNIC is required." Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
        <asp:RegularExpressionValidator ID="RegularExpressionValidator1" runat="server" ControlToValidate="person_id" ErrorMessage="Invalid CNIC format." Display="Dynamic" ForeColor="Red"></asp:RegularExpressionValidator>
    </div>

    <div runat="server">
        <label for="first_name">First Name:</label>
        <input id="first_name" type="text" class="form-control" runat="server" required />
        <asp:RequiredFieldValidator ID="RequiredFieldValidator2" runat="server" ControlToValidate="first_name" ErrorMessage="First Name is required." Display="Dynamic" ForeColor="Red"></asp:RequiredFieldValidator>
    </div>


```

Server side input  
validation

## Register

<b>CNIC:</b> <input type="text" value="e.g., 12345-1234567-1"/> <b>CNIC is required.</b>	<b>First Name:</b> <input type="text"/> <b>First Name is required.</b>
<b>Last Name:</b> <input type="text"/>	<b>Email:</b> <input type="text"/> <b>This feild is required</b>
<b>Phone No:</b> <input type="text"/> <b>This feild is required</b>	<b>Gender:</b> <input type="text" value="M"/> <b>This feild is required</b>
<b>City:</b> <input type="text"/> <b>This feild is required</b>	<b>State:</b> <input type="text" value="e.g., CA"/> <b>This feild is required</b>
<b>Postal Code:</b> <input type="text"/> <b>This feild is required</b>	<b>Country:</b> <input type="text"/> <b>This feild is required</b>
<b>Role:</b> <input type="text" value="User"/> <b>This feild is required</b>	<b>Password:</b> <input type="password"/> <b>This feild is required</b>

## Register

<b>CNIC:</b> <input type="text" value="wdwddw"/> <b>Invalid CNIC format.</b>	<b>First Name:</b> <input type="text"/> <b>First Name is required.</b>
<b>Last Name:</b> <input type="text"/>	<b>Email:</b> <input type="text"/> <b>This feild is required</b>
<b>Phone No:</b> <input type="text"/> <b>This feild is required</b>	<b>Gender:</b> <input type="text" value="M"/> <b>This feild is required</b>

**No SQL injection:**

```

Private Sub Login(sender As Object, e As EventArgs) Handles btnLogin.Click
    Dim constr As String
    constr = "Data Source= localhost; Initial Catalog= ARTVAULT; User ID=sa; Password= Hammad"
    Dim con As New SqlConnection
    con.ConnectionString = constr
    Dim cmd As New SqlCommand
    cmd.Connection = con
    'cmd.CommandText = "SELECT PERSON_ID, ROLE, PASSWORD, FIRST_NAME, LAST_NAME FROM PERSON WHERE PERSON_ID = '" & person_id.Value & "' AND PASSWORD = '" & password.Value & "'"
    cmd.CommandText = "SELECT PERSON_ID, ROLE, PASSWORD, FIRST_NAME, LAST_NAME FROM PERSON WHERE PERSON_ID = @user_id AND PASSWORD = @password"
    cmd.Parameters.AddWithValue("@user_id", person_id.Value)
    cmd.Parameters.AddWithValue("@password", password.Value)
    Dim dr As SqlDataReader

```

**Path Traversal Protection:****Partial Class Customer****Inherits** System.Web.UI.Page

```

Private Sub Customer_Load(sender As Object, e As EventArgs) Handles Me.Load
    Dim Authenticated As Boolean = CType(Session("Authenticated"), Boolean)
    Dim Role As String = CType(Session("Role"), String)

    If Authenticated = False Then
        Response.Redirect("Login.aspx")
    End If
    If Role Is Nothing Then
        Response.Redirect("Login.aspx")
    End If
    If Role <> "Customer" Then
        Response.Redirect("Login.aspx")
    End If

    Dim First_Name As String = CType(Session("First_Name"), String)
    Dim Last_Name As String = CType(Session("Last_Name"), String)
    Dim greeting_string As String = "Hi " & First_Name & " " & Last_Name & " !"
    greeting_Name.InnerText = greeting_string
    greeting_text.InnerText = "Welcome to ArtVault – where every masterpiece tells a story. Discover art that speaks to your soul and experience a journey of inspiration and beauty."

```

**End Sub**  
**End Class**

```

Private Sub Customer_Load(sender As Object, e As EventArgs) Handles Me.Load
    Dim Authenticated As Boolean = CType(Session("Authenticated"), Boolean)
    Dim Role As String = CType(Session("Role"), String)

    If Authenticated = False Then
        Response.Redirect("Login.aspx")
    End If
    If Role Is Nothing Then
        Response.Redirect("Login.aspx")
    End If
    If Role <> "Customer" Then
        Response.Redirect("Login.aspx")
    End If

    Dim First_Name As String = CType(Session("First_Name"), String)
    Dim Last_Name As String = CType(Session("Last_Name"), String)
    Dim greeting_string As String = "Hi " & First_Name & " " & Last_Name & " !"
    greeting_Name.InnerText = greeting_string
    greeting_text.InnerText = "Welcome to ArtVault – where every masterpiece tells a story. Discover art that speaks to your soul and experience a journey of inspiration and beauty."

```

**Broken access control protection:**

User id Stored in session and used in database queries for that user

```
2 references
Partial Class Myinfo
    Inherits System.Web.UI.Page
    0 references
    Private Sub Myinfo_Load(sender As Object, e As EventArgs) Handles Me.Load
        Dim Authenticated As Boolean = CType(Session("Authenticated"), Boolean)
        Dim Session_Cnic As String = CType(Session("Cnic"), String)
        Dim Role As String = CType(Session("Role"), String)

        Dim Session_Password As String = CType(Session("Password"), String)

        If Authenticated = False Then
            Response.Redirect("Login.aspx")
        End If
        If Role Is Nothing Then
            Response.Redirect("Login.aspx")
        End If
        If Role <> "Customer" And Role <> "Employee" And Role <> "Artist" Then
            Response.Redirect("Login.aspx")
        End If
    End Sub
End Class
```

```
Dim constr As String
constr = "Data Source= localhost; Initial Catalog= ARTVAULT_Testing; User ID=Hammad; Password= Hammad"
Dim con As New SqlConnection
con.ConnectionString = constr
Dim cmd As New SqlCommand
cmd.Connection = con
cmd.CommandText = "SELECT PERSON_ID, FIRST_NAME, LAST_NAME, EMAIL, PHONE_NO, GENDER, CITY, STATE, POSTAL_CODE, COUNTRY, ROLE, PASSWORD FROM PERSON WHERE PERSON_ID = '"
cmd.CommandText += Session_Cnic + "' AND PASSWORD = '" + Session_Password + "'"
Dim dr As SqlDataReader
Try
    con.Open()
    dr = cmd.ExecuteReader()
Catch ex As Exception
    Response.Redirect("Login.aspx")
End Try
```

User id Stored in session is unique for that user

**Test cases:**

ID	Feature	Test Description	Input	Expected Result	Actual Result	Status	Page on which this feature is implemented
1.	Authentication	Wrong credentials	<b>Id:</b> 11111-7111111-1 <b>Pass:</b> 12344545	Access Denied	Access Denied	PASS	Login.aspx
2.	Authentication	Correct credentials	<b>Id:</b> 33102-7125686-9 <b>Pass:</b> 1234	Access Granted	Access Granted	PASS	Login.aspx
3.	Authorization	As Customer	Login As Customer	Customer Panel	Customer panel	PASS	Customer.aspx
4.	Authorization	As Employee	Login As Employee	Employee Panel	Employee Panel	PASS	Employee.aspx
5.	Authorization	As Admin	Login As Admin	Admin Panel	Admin Panel	PASS	Admin.aspx
6.	Authorization	As Artist	Login As Artist	Artist Panel	Artist Panel	PASS	Artist.aspx
7.	Secure storage of user's session data	Only user-specific information shows	Login As Customer -> My Information	Users' information should be displayed	Users' information is displayed	PASS	Myinfo.aspx
8.	Input Validation	Empty input	Empty Feilds	Error Should be displayed	Error displayed	PASS	Register.aspx
8.	Input Validation	Wrong input	23321321 in CNIC field	Format error be Displayed	Format error is Displayed	PASS	Register.aspx
9.	Input Validation	Correct input	33102-7124686-9 In CNIC field	No errors and data should be inserted	No errors and data are inserted	PASS	Register.aspx
10.	No SQL injection	Inject SQL	<b>Id:</b> " or ""=" <b>Pass:</b> " or ""="	The system should refuse it	The system refused it	PASS	Login.aspx
12.	Path Traversal Protection	Access Customer.aspx without login	/Customer.aspx	Redirect to the Login page	Redirected to the Login page	PASS	Direct access to Customer.aspx
13.	Path Traversal Protection	Access Customer.aspx with login as Employee	/Customer.aspx	Redirect to the Login page	Redirected to the Login page	PASS	Access to Customer.aspx after login as Employee
13.	Path Traversal Protection	Access Customer.aspx with login as Customer	/Customer.aspx	The customer panel should be displayed	The customer panel is displayed	PASS	Access to Customer.aspx after login as Customer
14.	Broken access control protection	Update information	Login as Customer -> click on My Information -> click on Edit -> make changes -> click on Update	Only that user's information should be edited	Only that user's information is edited	PASS	At Myinfo.aspx click Edit then click Update