

PROBLEM 2

Problem Statement:

Implement identified security features for your project and make a live demonstration available.

Implementation of Security Features

I am implementing **Problem 2** using the **main page** that includes:

- Customer Login and Registration
 - Staff Login
 - Customer and Staff Dashboards
-

Implemented Security Features:

- Login System with roles (e.g., Admin, Staff).
 - Use FormsAuthentication in ASP.NET for token-based auth
 - SQL commands with parameters instead of string concatenation.
 - Input fields validated with RequiredFieldValidator, regex validation, etc.
 - Sessions used to maintain logged-in state and logout after inactivity.
-

.aspx

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

```
<!DOCTYPE html>
```

```
<html xmlns="http://www.w3.org/1999/xhtml">
```

```
<head runat="server">
```

```
<title>Movie Rental System</title>
```

```
<style>
```

```
body {
```

```
font-family: Arial, sans-serif;
```

```
background: linear-gradient(to right, #232526, #414345);
```

```
color: white;
text-align: center;
padding: 50px;
}
```

```
.container {
margin: auto;
max-width: 800px;
background-color: rgba(0,0,0,0.7);
padding: 30px;
border-radius: 10px;
}
```

```
h2 {
font-size: 36px;
margin-bottom: 20px;
}
```

```
.btn {
padding: 12px 30px;
font-size: 18px;
background-color: #ff5722;
color: white;
border: none;
border-radius: 5px;
cursor: pointer;
margin: 10px;
}
```

```

.btn:hover {
    background-color: #e64a19;
}

.form-group {
    margin: 10px 0;
}

</style>
</head>
<body>
    <form id="form1" runat="server">
        <div class="container">
            <h2>Movie Rental System</h2>

            <!-- Role Selection -->
            <asp:Panel ID="pnlRoleSelection" runat="server" Visible="True">
                <asp:Button ID="btnCustomerLoginView" runat="server" Text="Customer Login"
                CssClass="btn" OnClick="btnCustomerLoginView_Click" />
                <asp:Button ID="btnStaffLoginView" runat="server" Text="Staff Login"
                CssClass="btn" OnClick="btnStaffLoginView_Click" />
            </asp:Panel>

            <!-- Customer Login or Register Choice -->
            <asp:Panel ID="pnlCustomerChoice" runat="server" Visible="False">
                <asp:Button ID="btnCustomerLoginForm" runat="server" Text="Login"
                CssClass="btn" OnClick="btnCustomerLoginForm_Click" />
                <asp:Button ID="btnCustomerRegisterForm" runat="server" Text="Register"
                CssClass="btn" OnClick="btnCustomerRegisterForm_Click" />
            </asp:Panel>
        </div>
    </form>

```

```
<!-- Customer Login -->

<asp:Panel ID="pnlCustomerLogin" runat="server" Visible="False">

    <h3>Customer Login</h3>

    <div class="form-group">Customer ID: <asp:TextBox ID="txtCustomerId"
runat="server" /></div>

    <div class="form-group">Name: <asp:TextBox ID="txtCustomerName"
runat="server" /></div>

    <asp:Button ID="btnCustomerLogin" runat="server" Text="Login" CssClass="btn"
OnClick="btnCustomerLogin_Click" />

    <br />

    <asp:Label ID="lblCustomerStatus" runat="server" ForeColor="Red" />

</asp:Panel>
```

```
<!-- Customer Registration -->

<asp:Panel ID="pnlCustomerRegister" runat="server" Visible="False">

    <h3>Register New Customer</h3>

    <div class="form-group">Name: <asp:TextBox ID="txtNewCustomerName"
runat="server" /></div>

    <div class="form-group">Contact: <asp:TextBox ID="txtNewCustomerContact"
runat="server" /></div>

    <div class="form-group">Address: <asp:TextBox ID="txtNewCustomerAddress"
runat="server" /></div>

    <asp:Button ID="btnRegisterCustomer" runat="server" Text="Register"
CssClass="btn" OnClick="btnRegisterCustomer_Click" />

    <br />

    <asp:Label ID="lblRegisterStatus" runat="server" ForeColor="Green" />

</asp:Panel>
```

```

<!-- Staff Login -->

<asp:Panel ID="pnlStaffLogin" runat="server" Visible="False">

    <h3>Staff Login</h3>

    <div class="form-group">Staff ID: <asp:TextBox ID="txtStaffId" runat="server"
/></div>

    <div class="form-group">Name: <asp:TextBox ID="txtStaffName" runat="server"
/></div>

    <asp:Button ID="btnStaffLogin" runat="server" Text="Login" CssClass="btn"
OnClick="btnStaffLogin_Click" />

    <br />

    <asp:Label ID="lblStaffStatus" runat="server" ForeColor="Red" />

</asp:Panel>


<!-- Customer Dashboard -->

<asp:Panel ID="pnlCustomerDashboard" runat="server" Visible="False">

    <h3>Welcome, Customer!</h3>

    <asp:Button ID="btnViewMovies" runat="server" Text="View Available Movies"
OnClick="btnViewMovies_Click" /><br /><br />

    <asp:Panel ID="pnlMovies" runat="server" Visible="False">

        <h3>Available Movies:</h3>

        <asp:GridView ID="gvMovies" runat="server" AutoGenerateColumns="True"
/>

        <br />

    </asp:Panel>

    <asp:Button ID="btnGoToRentals" runat="server" Text="Rental History"
CssClass="btn" PostBackUrl="~/Lab13/ViewRentals.aspx" />

    <asp:Button ID="btnGoToRent" runat="server" Text="Rent a Movie"
CssClass="btn" PostBackUrl="~/Lab13/RentMovies.aspx" />

    <asp:Button ID="btnGoToPayments" runat="server" Text="Make a Payment"
CssClass="btn" PostBackUrl="~/Lab13/MakePayments.aspx" />

    <br /><br />

```

```

        <asp:Button ID="btnCustomerLogout" runat="server" Text="Logout"
        CssClass="btn" OnClick="btnLogout_Click" />

    </asp:Panel>

    <!-- Admin Dashboard -->

    <asp:Panel ID="pnlStaffDashboard" runat="server" Visible="False">

        <h3>Admin Dashboard</h3>

        <asp:Button ID="btnGoToManageMovies" runat="server" Text="Manage Movies"
        CssClass="btn" PostBackUrl="~/Lab13/ManageMovies.aspx" />

        <asp:Button ID="btnGoToManagePayments" runat="server" Text="Manage
        Rentals" CssClass="btn" PostBackUrl="~/Lab13/Default.aspx" />

        <br /><br />

        <asp:Button ID="btnStaffLogout" runat="server" Text="Logout" CssClass="btn"
        OnClick="btnLogout_Click" />

    </asp:Panel>

</div>

</form>

</body>

</html>

```

.aspx.vb

Imports System.Data.SqlClient

Imports System.Data

Partial Class _Default

Inherits System.Web.UI.Page

```

    Dim conStr As String = "workstation id=movierental.mssql.somee.com;packet
    size=4096;user id=hajra_SQLLogin_3;pwd=7jt2lvnzho;data
    source=movierental.mssql.somee.com;persist security info=False;initial
    catalog=movierental;TrustServerCertificate=True"

```

Protected Sub Page_Load(sender As Object, e As EventArgs) Handles Me.Load

 If Not IsPostBack Then

 pnlRoleSelection.Visible = True

 End If

End Sub

Protected Sub btnCustomerLoginView_Click(sender As Object, e As EventArgs)

 pnlRoleSelection.Visible = False

 pnlCustomerChoice.Visible = True

End Sub

Protected Sub btnCustomerLoginForm_Click(sender As Object, e As EventArgs)

 pnlCustomerChoice.Visible = False

 pnlCustomerLogin.Visible = True

End Sub

Protected Sub btnCustomerRegisterForm_Click(sender As Object, e As EventArgs)

 pnlCustomerChoice.Visible = False

 pnlCustomerRegister.Visible = True

End Sub

Protected Sub btnRegisterCustomer_Click(sender As Object, e As EventArgs)

 Dim name As String = txtNewCustomerName.Text.Trim()

 Dim contact As String = txtNewCustomerContact.Text.Trim()

 Dim address As String = txtNewCustomerAddress.Text.Trim()

' Check if all fields are filled

If String.IsNullOrEmpty(name) Or String.IsNullOrEmpty(contact) Or
String.IsNullOrEmpty(address) Then

lblRegisterStatus.Text = "All fields are required."

lblRegisterStatus.ForeColor = Drawing.Color.Red

Return

End If

' Fetch the next available customer_id

Dim newCustomerId As Integer

Using con As New SqlConnection(conStr)

Dim cmd As New SqlCommand("SELECT ISNULL(MAX(customer_id), 0) + 1
FROM CUSTOMER", con)

con.Open()

newCustomerId = Convert.ToInt32(cmd.ExecuteScalar())

End Using

' Insert the new customer into the database with the next customer_id

Using con As New SqlConnection(conStr)

Dim cmd As New SqlCommand("INSERT INTO CUSTOMER (customer_id, name,
contact, address) VALUES (@customer_id, @name, @contact, @address)", con)

cmd.Parameters.AddWithValue("@customer_id", newCustomerId)

cmd.Parameters.AddWithValue("@name", name)

cmd.Parameters.AddWithValue("@contact", contact)

cmd.Parameters.AddWithValue("@address", address)

con.Open()

cmd.ExecuteNonQuery()

' Display success message with the newly generated customer ID

```
        lblRegisterStatus.Text = "Registered successfully! Your Customer ID is: " &  
newCustomerId
```

```
        lblRegisterStatus.ForeColor = Drawing.Color.Green
```

```
    End Using
```

```
End Sub
```

```
Protected Sub btnStaffLoginView_Click(sender As Object, e As EventArgs)
```

```
    pnlRoleSelection.Visible = False
```

```
    pnlStaffLogin.Visible = True
```

```
End Sub
```

```
Protected Sub btnCustomerLogin_Click(sender As Object, e As EventArgs)
```

```
    Dim customerId As Integer
```

```
    If Not Integer.TryParse(txtCustomerId.Text, customerId) Then
```

```
        lblCustomerStatus.Text = "Invalid Customer ID."
```

```
        Return
```

```
    End If
```

```
    Dim name As String = txtCustomerName.Text.Trim()
```

```
    Using con As New SqlConnection(conStr)
```

```
        Dim cmd As New SqlCommand("SELECT COUNT(*) FROM CUSTOMER  
WHERE customer_id = @id AND name = @name", con)
```

```
        cmd.Parameters.AddWithValue("@id", customerId)
```

```
        cmd.Parameters.AddWithValue("@name", name)
```

```
        con.Open()
```

```
        Dim count As Integer = Convert.ToInt32(cmd.ExecuteScalar())
```

```
        If count = 1 Then
```

```
            Session("CustomerID") = customerId
```

```

        pnlCustomerLogin.Visible = False
        pnlCustomerDashboard.Visible = True
    Else
        lblCustomerStatus.Text = "Invalid Customer ID or Name."
    End If
End Using
End Sub

```

```

Protected Sub btnViewMovies_Click(sender As Object, e As EventArgs)
    pnlMovies.Visible = True
    LoadMovies()
End Sub

```

```

Private Sub LoadMovies()
    Using con As New SqlConnection(conStr)
        Dim cmd As New SqlCommand("SELECT movie_id, title, genre, release_year,
rental_rate FROM MOVIE", con)
        Dim da As New SqlDataAdapter(cmd)
        Dim dt As New DataTable()
        da.Fill(dt)
        gvMovies.DataSource = dt
        gvMovies.DataBind()
    End Using
End Sub

```

```

Protected Sub btnStaffLogin_Click(sender As Object, e As EventArgs)
    Dim staffId As Integer
    If Not Integer.TryParse(txtStaffId.Text, staffId) Then
        lblStaffStatus.Text = "Invalid Staff ID."
    End If
End Sub

```

Return

End If

Dim name As String = txtStaffName.Text.Trim()

Using con As New SqlConnection(conStr)

Dim cmd As New SqlCommand("SELECT COUNT(*) FROM STAFF WHERE
staff_id = @id AND name = @name", con)

cmd.Parameters.AddWithValue("@id", staffId)

cmd.Parameters.AddWithValue("@name", name)

con.Open()

Dim count As Integer = Convert.ToInt32(cmd.ExecuteScalar())

If count = 1 Then

Session("StaffID") = staffId

pnlStaffLogin.Visible = False

pnlStaffDashboard.Visible = True

Else

lblStaffStatus.Text = "Invalid Staff ID or Name."

End If

End Using

End Sub

Protected Sub btnLogout_Click(sender As Object, e As EventArgs)

Session.Clear()

pnlCustomerDashboard.Visible = False

pnlStaffDashboard.Visible = False

pnlCustomerLogin.Visible = False

pnlStaffLogin.Visible = False

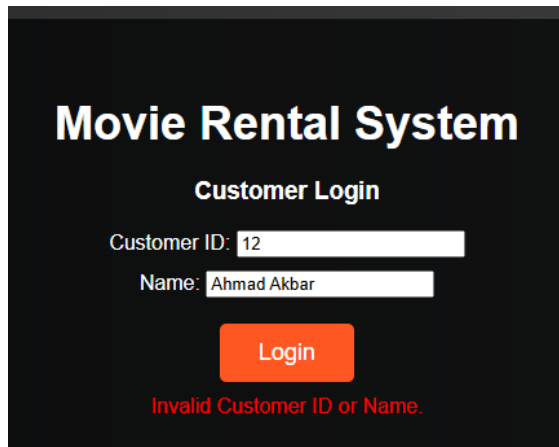
pnlCustomerChoice.Visible = False

pnlCustomerRegister.Visible = False

```
pnlRoleSelection.Visible = True
```

```
End Sub
```

```
End Class
```



Movie Rental System

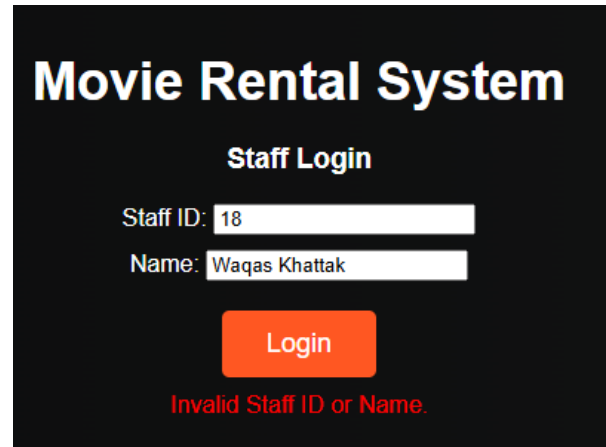
Customer Login

Customer ID: 12

Name: Ahmad Akbar

Login

Invalid Customer ID or Name.



Movie Rental System

Staff Login

Staff ID: 18

Name: Waqas Khattak

Login

Invalid Staff ID or Name.