Internet Application Development

Lab 13

Dated: Tuesday, 13th May 2025

Registration No: 03-3-1-061-2022

Full Name: Zoya Zahra

Problem 1) Refer to your semester project as outlined below:

Task 1: To develop a brief project proposal document of a web development project.

- It must be a data driven web application
- Incorporate state management
- Validation is mandatory
- Data security is essential
- Users and roles based software functionalities to be incorporated

Task 2: To write software requirements specification

Task 3: To develop the analysis and design model of web application including:

- Use case model
- Sequence diagrams
- Activity diagrams
- Class diagrams

Task 3A To develop component model and deployment model Task 4: Develop database model including:

- ER Model
- Relational Model
- Normalization of relational model
- Physical Model
- SQL Implementation

Task 5: To implement the web application using concepts and examples studied in course.

Task 6: To host the application on a web domain.

- Database can be on local machine
- Or on web hosting platform

Task 7: Testing of Web Application

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?

SECUTIRY FEATURES FOR MY PROJECT:

- HASHED PASSWORDS USING SHA 256 ALGORITHM: Storing passwords in plaintext in a database is not secure. If the database gets leaked in case of a cyberattack, passwords do not get leaked due to these hashed values as these values are irreversible. So, this acts as a strong security feature in any web application.

- LONG PASSWORDS: COMBINATION OF ANY TWO: CAPITAL AND SMALL LETTERS, AND NUMBERS: Another way I added security in my web application is by implementing checks on my passwords. The passwords must be atleast 8 character long and should be a combination of at least two of the following: capital, small alphabets and digits. This makes brute force attacks painful for the malicious users.

- PARAMETRIZED SQL COMMANDS: SQL injection is one of the most common attacks in the cyber world so we must secure our website from it. Using parametrized commands is a great way to secure the SQLi attacks on the website. It ensures that the user input is treated as data and not SQL code.

- INPUT VALIDATION: The input is validated to ensure the correct format is being given to out Database and the web application. This prevents malicious input that could lead to security vulnerabilities such as XXS or SQLi. Ensure only correct and safe data is processed on the system.

- AUTHENTICATION: The first A from the famous term AAA i.e. Authentication, Authorization, Accessibility. Our step to secure the system by logging in our users before they can perform their work. This ensures no invalid user can get to our system resources for malicious purposes.

- AUTHORIZATION: Another security feature after authentication is authorization. All users are divided into roles. The users can perform specific actions according to their privileges based on their roles.

- SECURE WEBSITE USING HTTPS PROTOCOL: Using HTTPS secures the communication between browser and the client by encrypting it so no one can understand it even if the traffic is sniffed preventing man-in-the-middle attacks and eavesdropping on sensitive data. This ensures the Confidentiality and Integrity of the data. It prevents the stealing of sensitive information such as passwords or bank account details etc.

- SESSION ABANDON WHEN LOGOUT: When user logs out, its session data is cleared to ensure session data can not be reused by an attacker.

- ALLOW LIMITED NUMBER OF ATTEMPTS FOR LOGIN: This prevents brute force attacks on the system. Limiting login attempts prevents automated bots from continuously trying to guess user credentials. This significantly reduces the likelihood of successful brute force or credential stuffing attacks. (This feature implementation is in progress. Not fully built yet)

- SESSION TIMEOUT AFTER 15 MINUTES OF ACTIVITY: User session automatically expires if an inactivity of some time is observed. This reduces the risk of unauthorized access to a user's account in case the user forgets to logout or leave the system open, and some malicious person gains hold of it. (I tried this by adding session timeout in the web.config file but I ran into errors. Have to resolve this issue yet.)

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

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

Hashing Passwords:

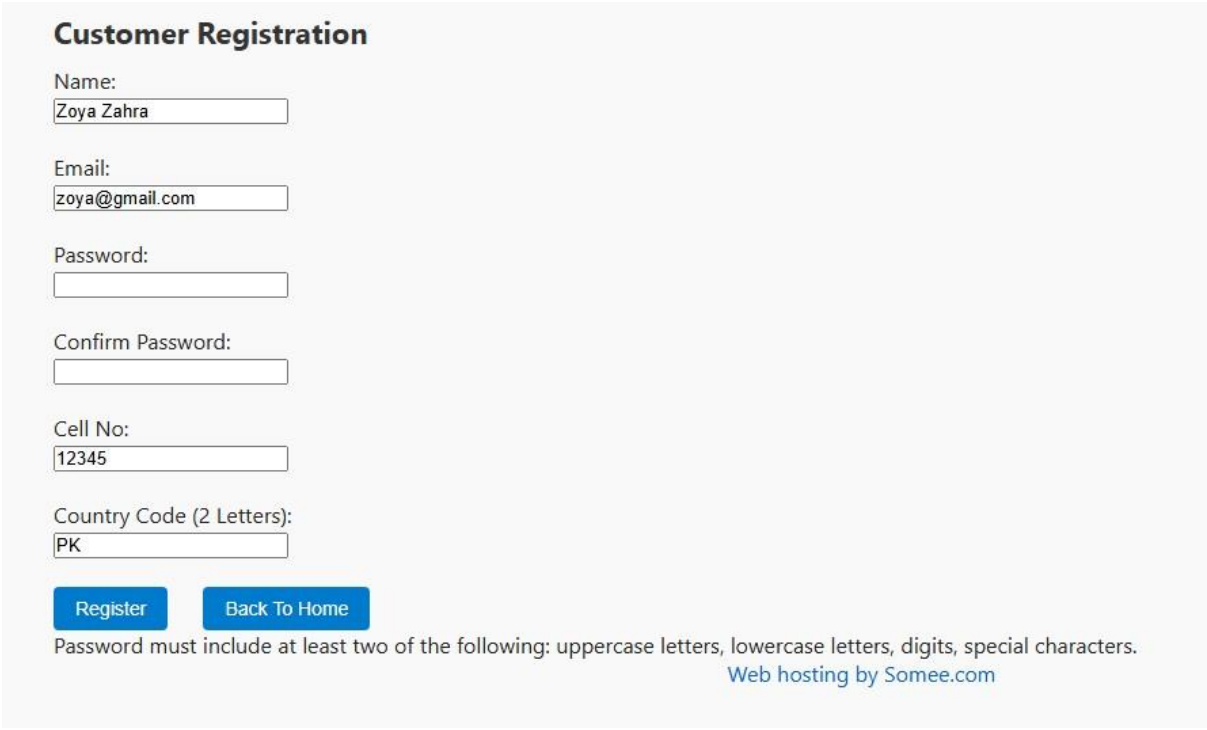
```
1 reference
Private Function ComputeSha256Hash(rawData As String) As String
    Using sha256 As SHA256 = sha256.Create()
        Dim bytes As Byte() = sha256.ComputeHash(Encoding.UTF8.GetBytes
          (rawData))
        Dim builder As New StringBuilder()
        For Each b As Byte In bytes
            builder.Append(b.ToString("x2"))
        Next
        Return builder.ToString()
    End Using
End Function
```

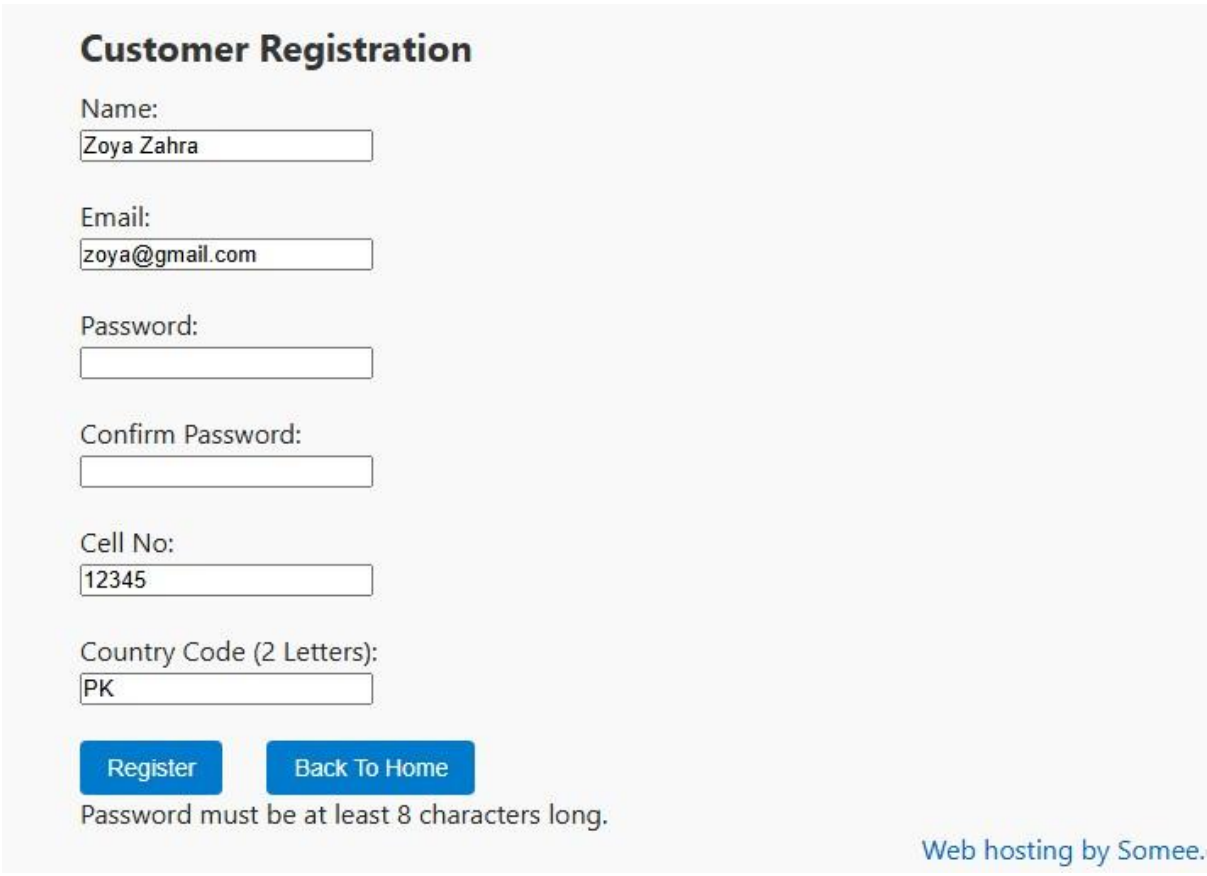
```
Dim hashedPassword As String = ComputeSha256Hash(password)
```

Customer_Id	Email	Name	Cell_NO	Country	password
C1	jane.smith@email.com	Jane Smith	12345678902	US	0b14d501a594442a01c6859541bcb3e8164d183d32937b851835442f69d5c94
C10	james.white@email.com	James White	12345678910	AU	aa4a9ea03fcac15b5fc63c949ac34e7b0fd17906716ac3b8e58c599cdc5a52f0
C11	robert.garcia@email.com	Robert Garcia	12345678911	IN	53d453b0c08b6b38ae91515dc88d25fbecdd1d6001f022419629df844f8ba433
C12	mary.martin@email.com	Mary Martin	12345678912	IN	b3d17ebbe4f2b75d27b6309cfaae1487b667301a73951e7d523a039cd2dfe110
C13	charles.lewis@email.com	Charles Lewis	12345678913	US	48caafb68583936afd0d78a7bfd7046d2492fad94f3c485915f74bb60128620d
C14	sophia.walker@email.com	Sophia Walker	12345678914	US	c6863e1db9b396ed31a36988639513a1c73a065fab83681f4b77adb648fac3d6
C15	george.hall@email.com	George Hall	12345678915	CA	c63c2d34ebe84032ad47b87af194fedd17dacf8222b2ea7f4ebfee3dd6db2dfb
C16	irfanhameed@gmail.com	Sir Irfan Hameed	12345678	PK	32da4bc6855ce0b57f191e7d02314de2101715f63c9c14d1306db62735816b74
C2	john.doe@email.com	John Doe	12345678901	US	6cf615d5bcaac778352a8f1f3360d23f02f34ec182e259897fd6ce485d7870d4
C3	mike.jones@email.com	Mike Jones	12345678903	CA	5906ac361a137e2d286465cd6588ebb5ac3f5ae955001100bc41577c3d751764
C4	emily.davis@email.com	Emily Davis	12345678904	CA	b97873a40f73abedd8d685a7cd5e5f85e4a9cfb83eac26886640a0813850122b

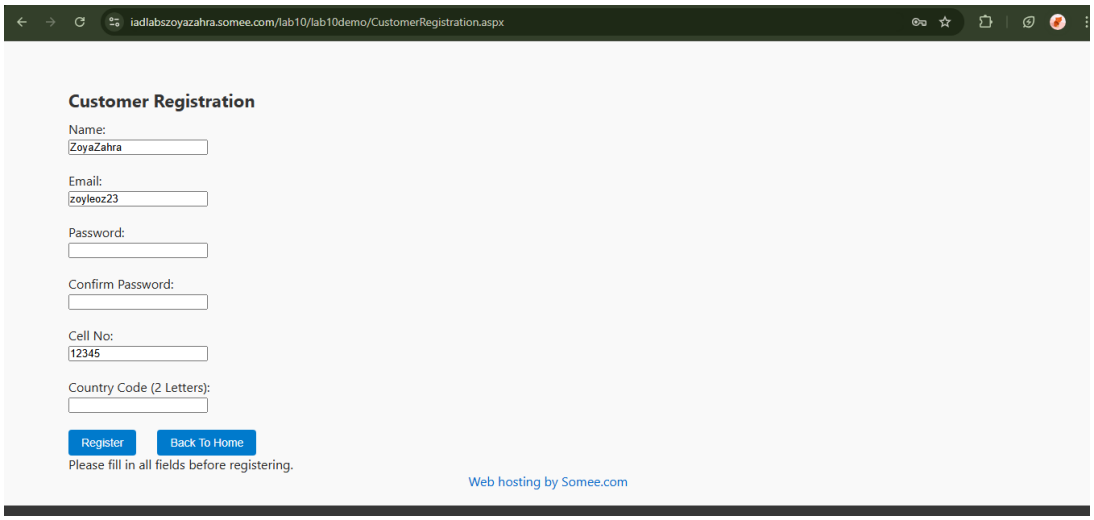
LONG PASSWORDS:

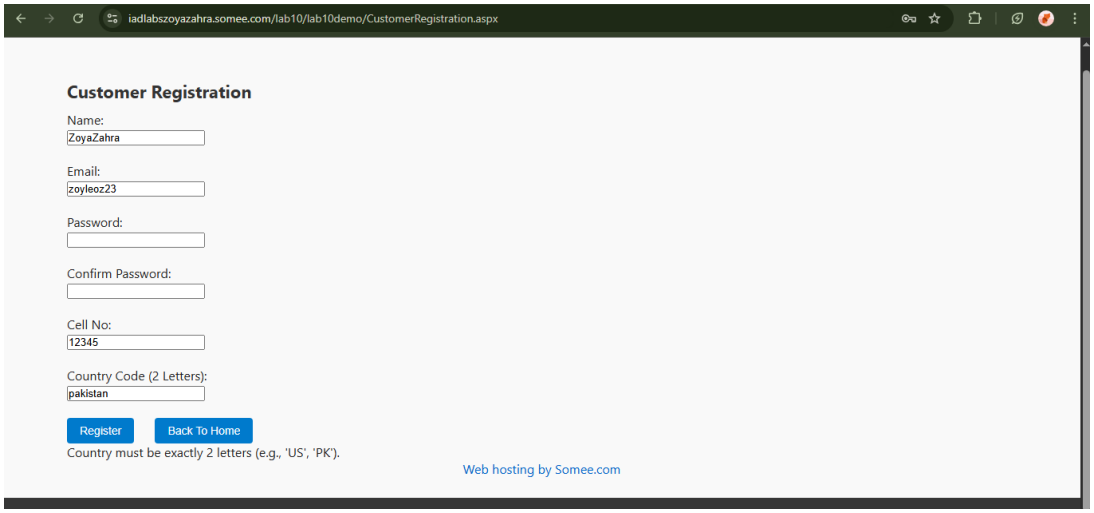
```
Dim hasUpper As Boolean = Regex.IsMatch(password, "[A-Z]")
Dim hasLower As Boolean = Regex.IsMatch(password, "[a-z]")
Dim hasDigit As Boolean = Regex.IsMatch(password, "\d")
Dim hasSpecial As Boolean = Regex.IsMatch(password, "[^A-Za-z0-9]")


Dim strengthCount As Integer = 0
If hasUpper Then strengthCount += 1
If hasLower Then strengthCount += 1
If hasDigit Then strengthCount += 1
If hasSpecial Then strengthCount += 1
```

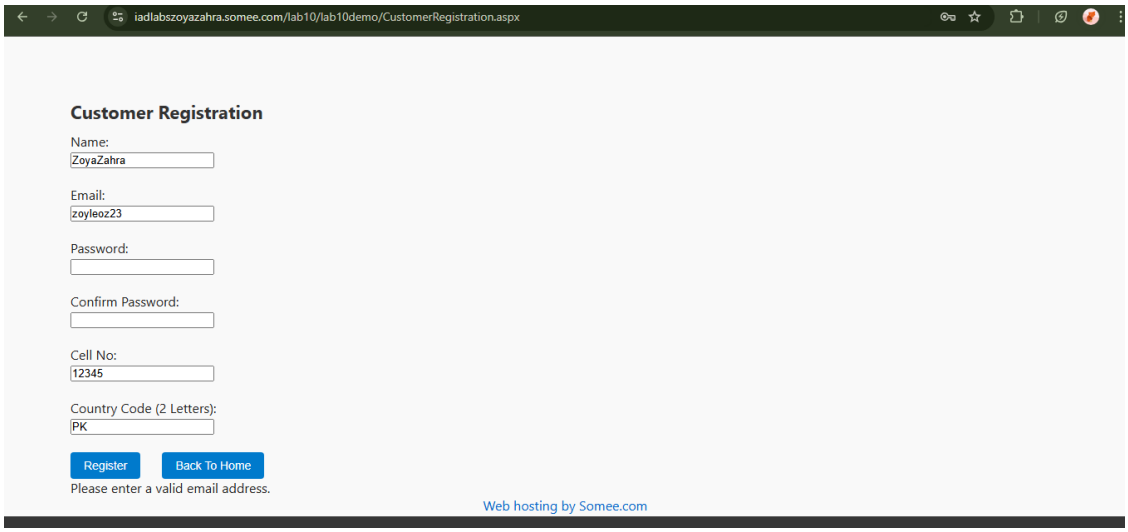

Customer Registration
Name:
Zoya Zahra
Email:
zoya@gmail.com
Password:
Confirm Password:
Cell No:
12345
Country Code (2 Letters):
PK
Register
Back To Home
Password must include at least two of the following: uppercase letters, lowercase letters, digits, special characters.
Web hosting by Somee.com

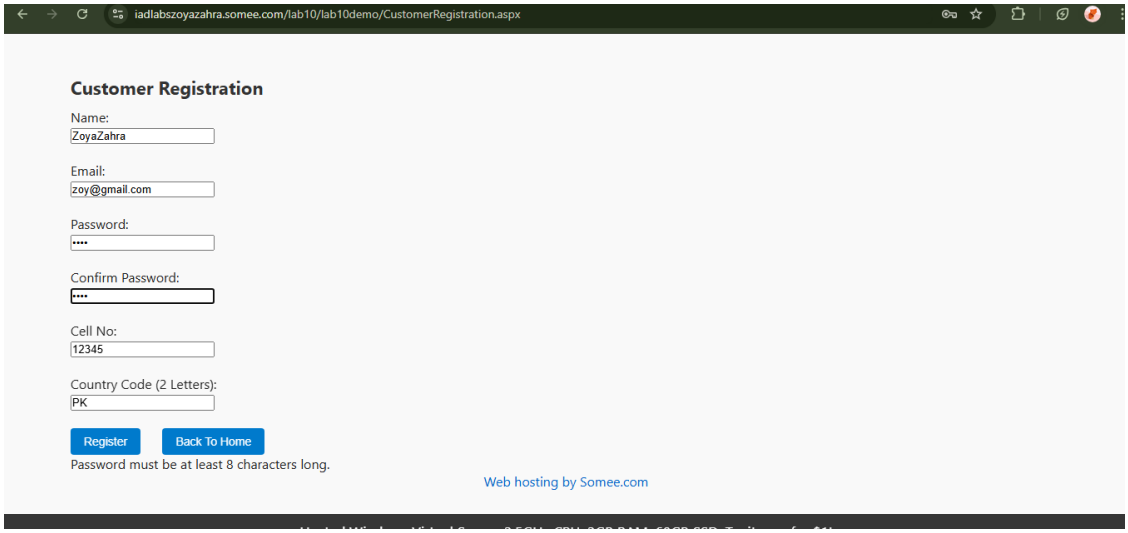

Customer Registration
Name:
Zoya Zahra
Email:
zoya@gmail.com
Password:
Confirm Password:
Cell No:
12345
Country Code (2 Letters):
PK
Register
Back To Home
Password must be at least 8 characters long.
Web hosting by Somee.

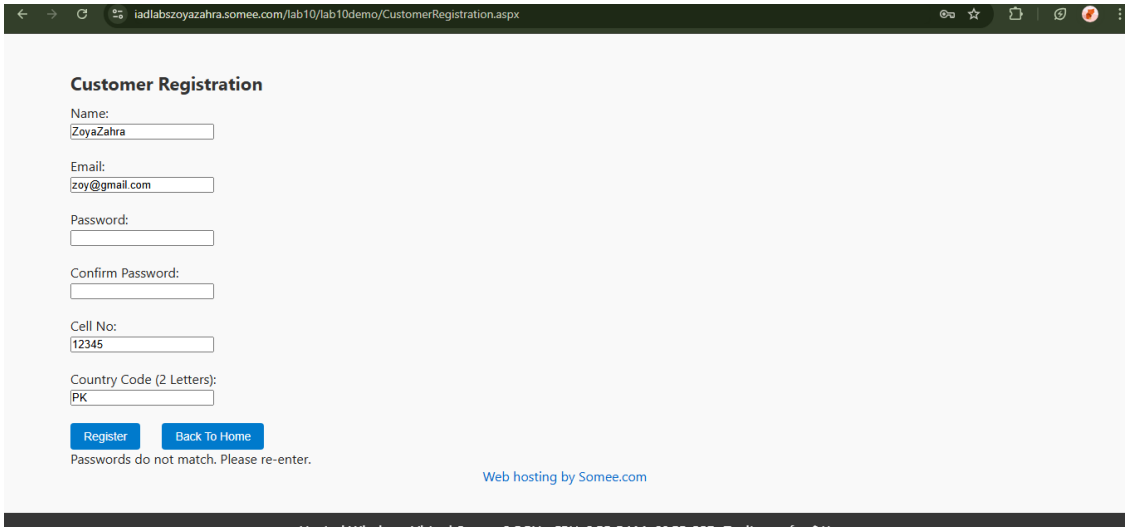
INPUT VALIDATION:

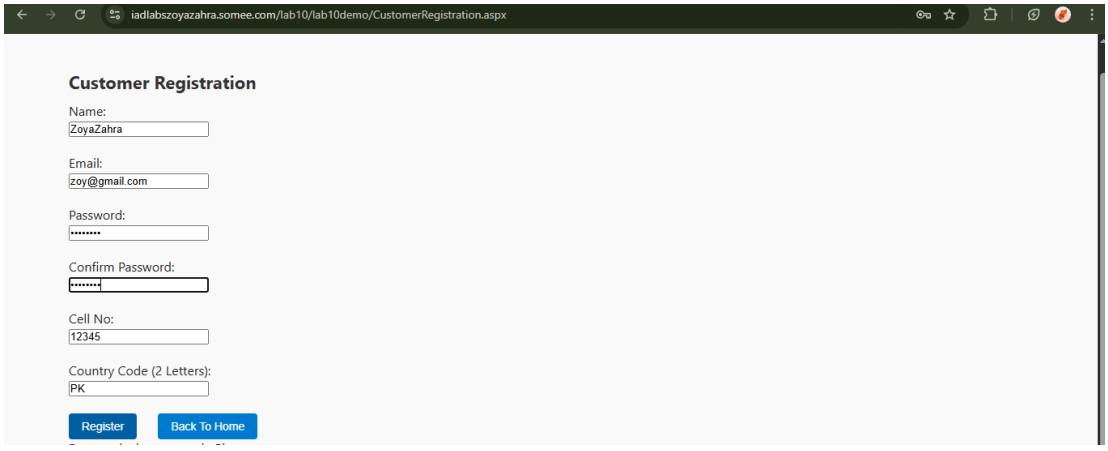


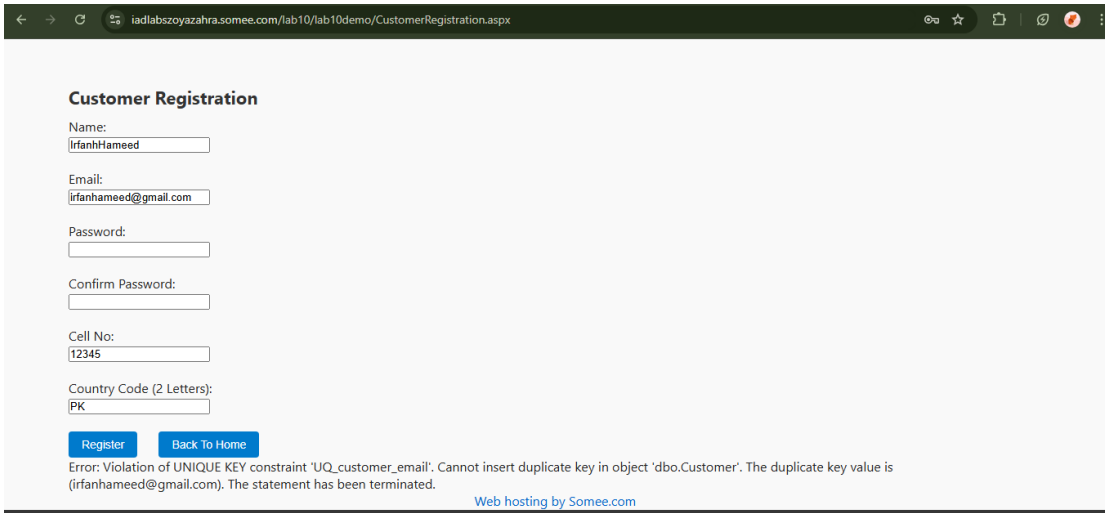


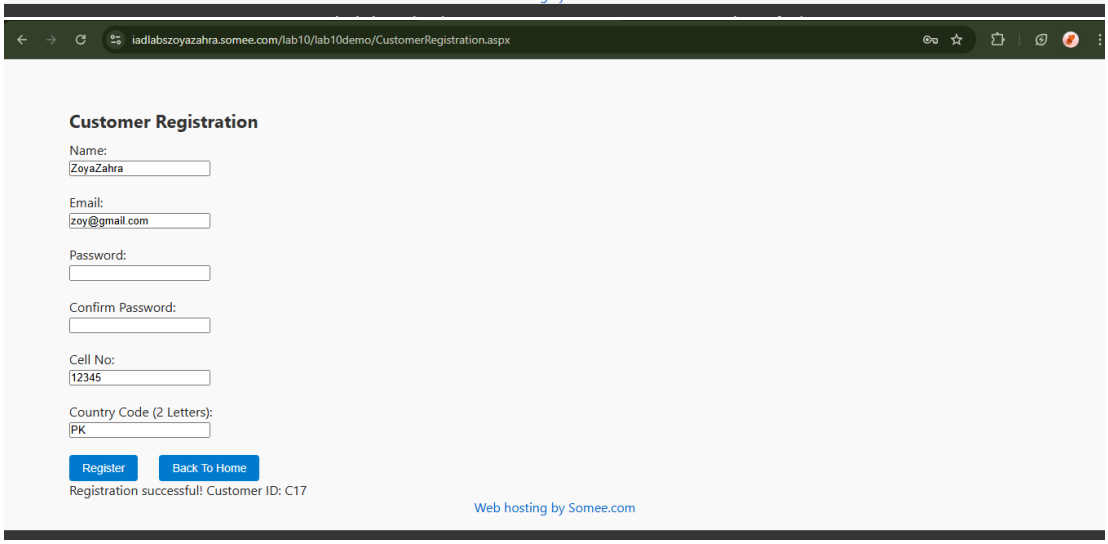



iadlabszoyazahra.somee.com/lab10/lab10demo/CustomerRegistration.aspx
Customer Registration
Name:
ZoyaZahra
Email:
zoy@gmail.com
Password:
Confirm Password:
Cell No:
12345
Country Code (2 Letters):
PK
Register
Back To Home
Password must be at least 8 characters long.
Web hosting by Somee.com


iadlabszoyazahra.somee.com/lab10/lab10demo/CustomerRegistration.aspx
Customer Registration
Name:
ZoyaZahra
Email:
zoy@gmail.com
Password:
Confirm Password:
Cell No:
12345
Country Code (2 Letters):
PK
Register
Back To Home
Passwords do not match. Please re-enter.
Web hosting by Somee.com


iadlabszoyazahra.somee.com/lab10/lab10demo/CustomerRegistration.aspx
Customer Registration
Name:
ZoyaZahra
Email:
zoy@gmail.com
Password:
Confirm Password:
Cell No:
12345
Country Code (2 Letters):
PK
Register
Back To Home

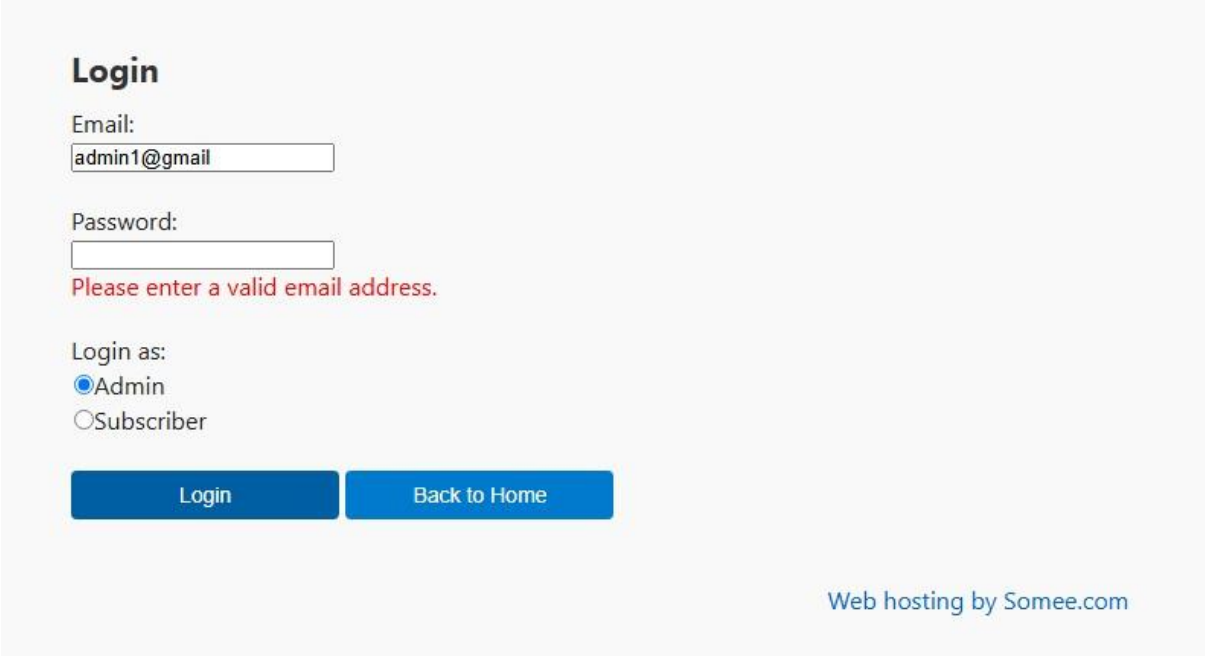




PARAMETRIZED SQL COMMANDS:

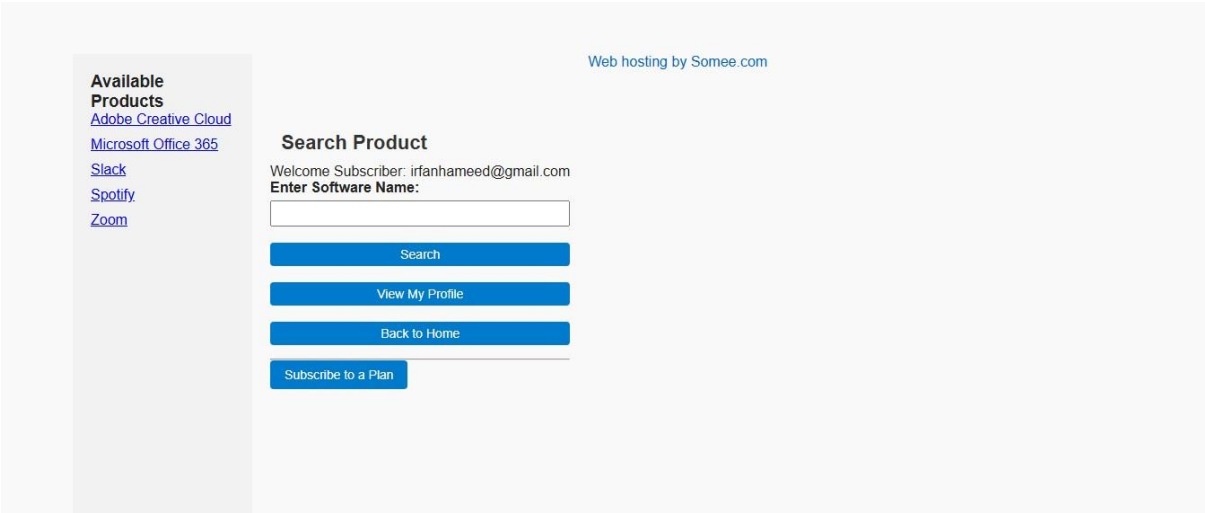
```
cmd.CommandText = "INSERT INTO Customer (Customer_Id, Email, Name,
  Cell_NO, Country, password) " &
            "VALUES (@Customer_Id, @Email, @Name, @Cell_NO,
        @Country, @password)"
cmd.Parameters.Clear()
cmd.Parameters.AddWithValue("@Customer_Id", newId)
cmd.Parameters.AddWithValue("@Email", email)
cmd.Parameters.AddWithValue("@Name", name)
cmd.Parameters.AddWithValue("@Cell_NO", cellNo)
cmd.Parameters.AddWithValue("@Country", country)
cmd.Parameters.AddWithValue("@password", hashedPassword)

cmd.ExecuteNonQuery()
lblMessage.Text = "Registration successful! Customer ID: " & newId
```

AUTHENTICATION:

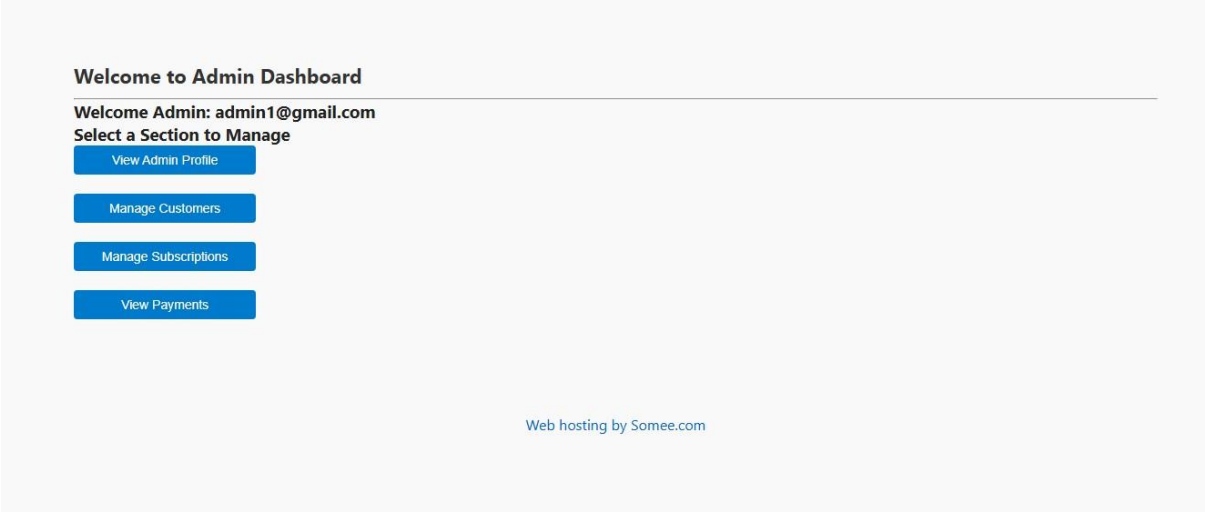


AUTHORIZATION:

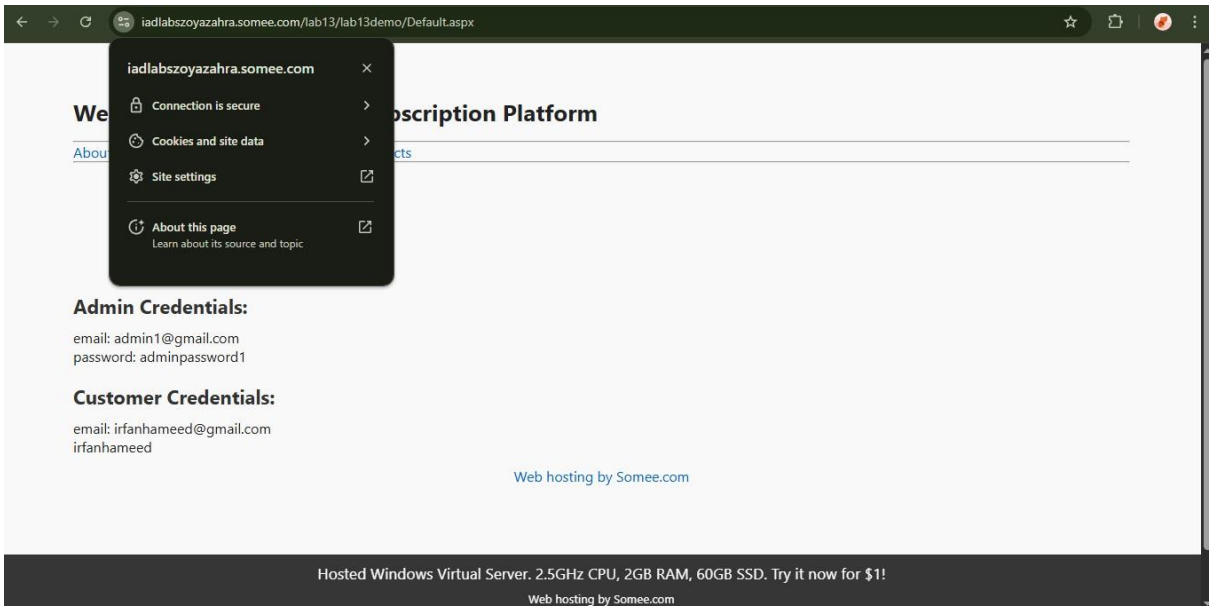
Fos Subscriber Login



For Admin Login:



SECURING WEBSITE USING HTTPS PrOTOCOL:

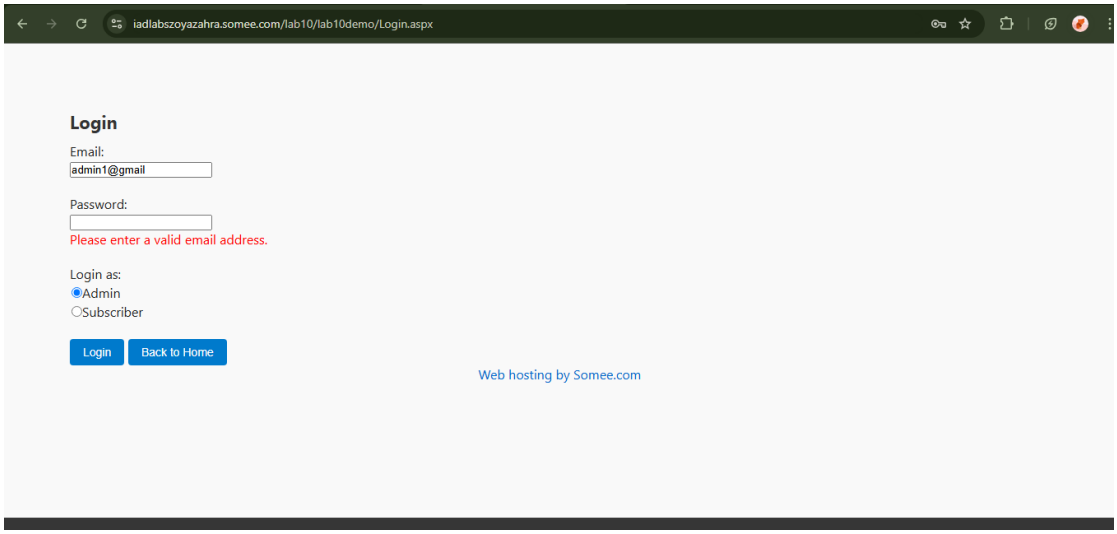


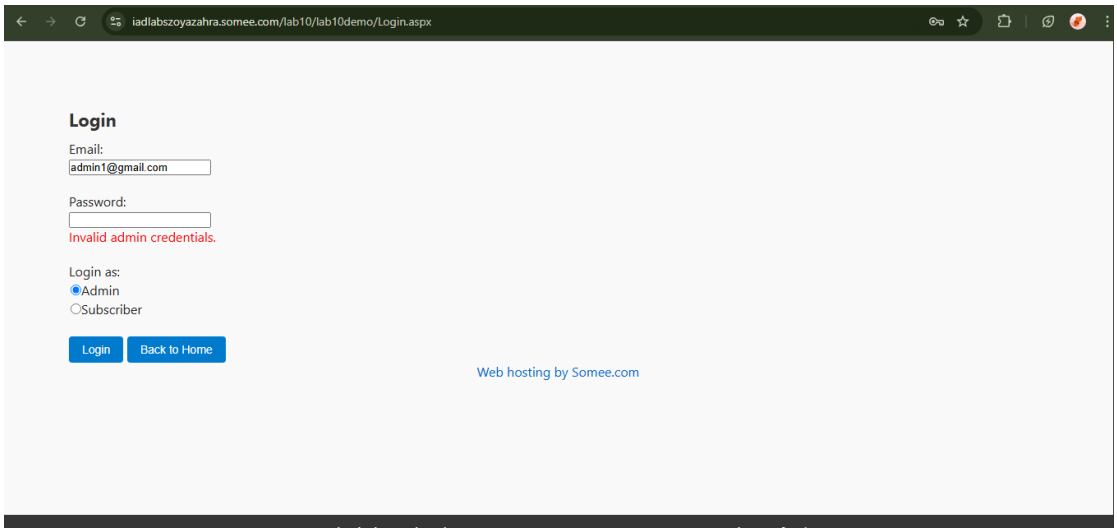
Session Abandon When Logging Out

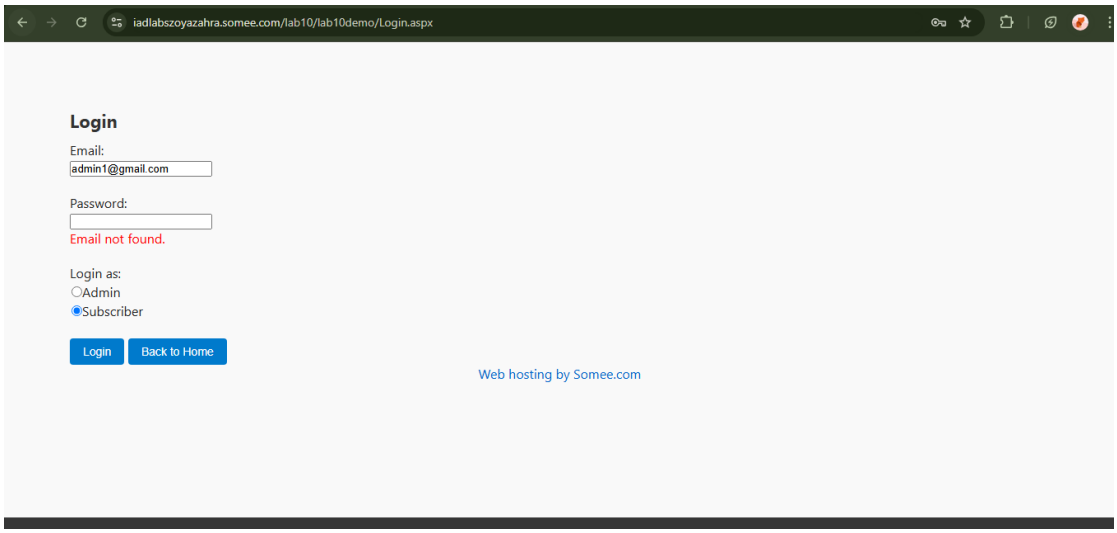
```
Protected Sub btnadminlogout_Click(sender As Object, e As EventArgs) Handles
  btnadminlogout.Click

    Session("Email") = Nothing
    Session("Role") = Nothing


    Session.Clear()
    Session.Abandon()


    Response.Redirect("Default.aspx")
End Sub
```

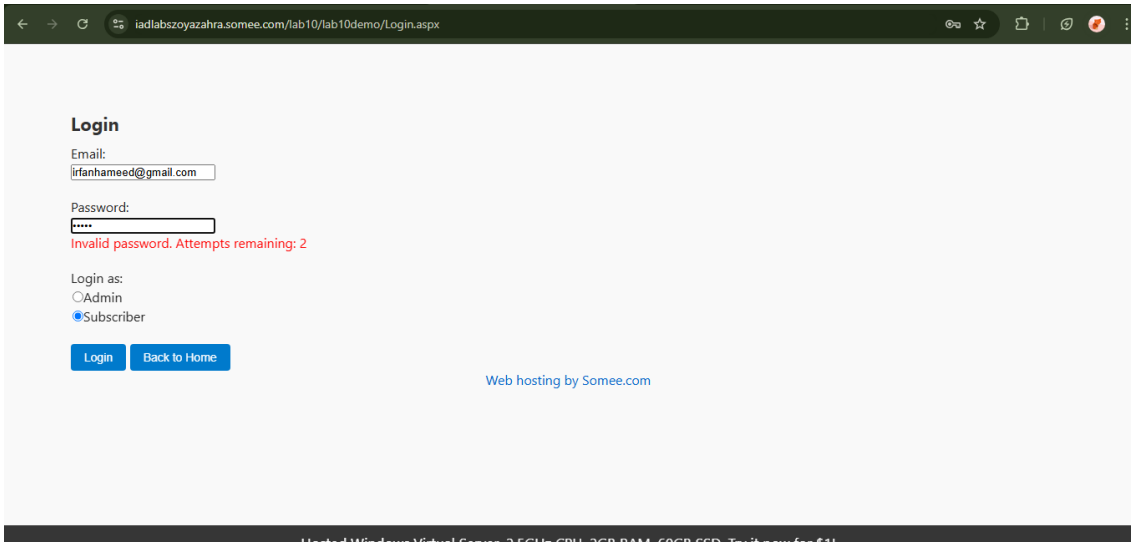
LIMITED LOGIN ATTEMPTS:

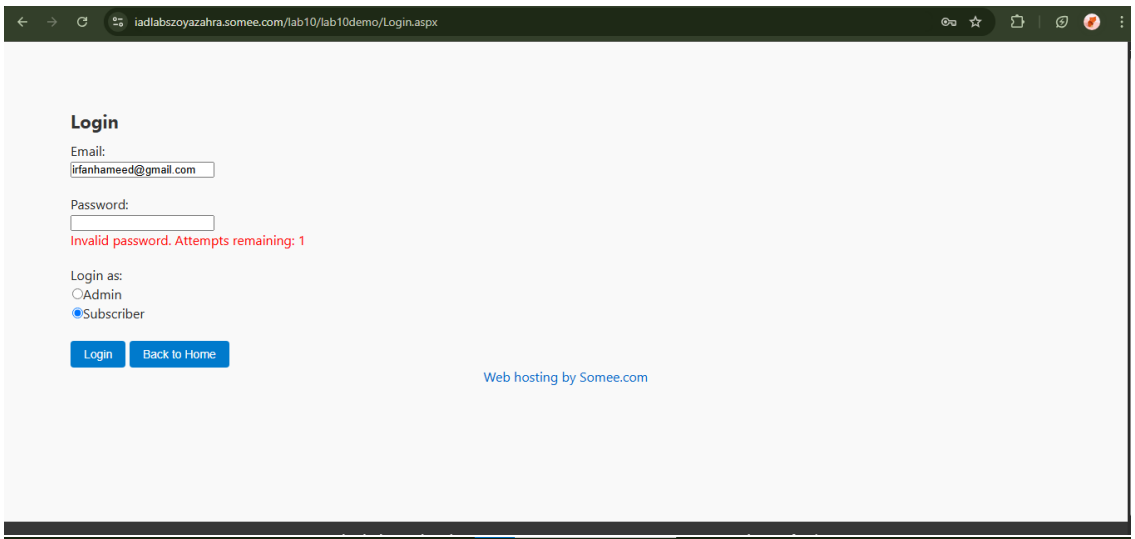
```
    If result > 0 Then

        If userType = "Subscriber" Then

            ResetFailedLogin(con, email)
        End If

        Session("Email") = email
        Session("Role") = userType

        If userType = "Admin" Then
            Response.Redirect("AdminHomePage.aspx")
        Else
            Response.Redirect("SubscriberHomePage.aspx")
        End If
    Else

        failedAttempts += 1

        If failedAttempts >= 3 Then

            LockUserAccount(con, email)
            lblMessage.Text = "Your account has been locked due to 3 failed login
              attempts."
        Else

            UpdateFailedLogin(con, email, failedAttempts)
            lblMessage.Text = String.Format("Invalid email or password. You have {0}
               attempt(s) remaining.", 3 - failedAttempts)
```

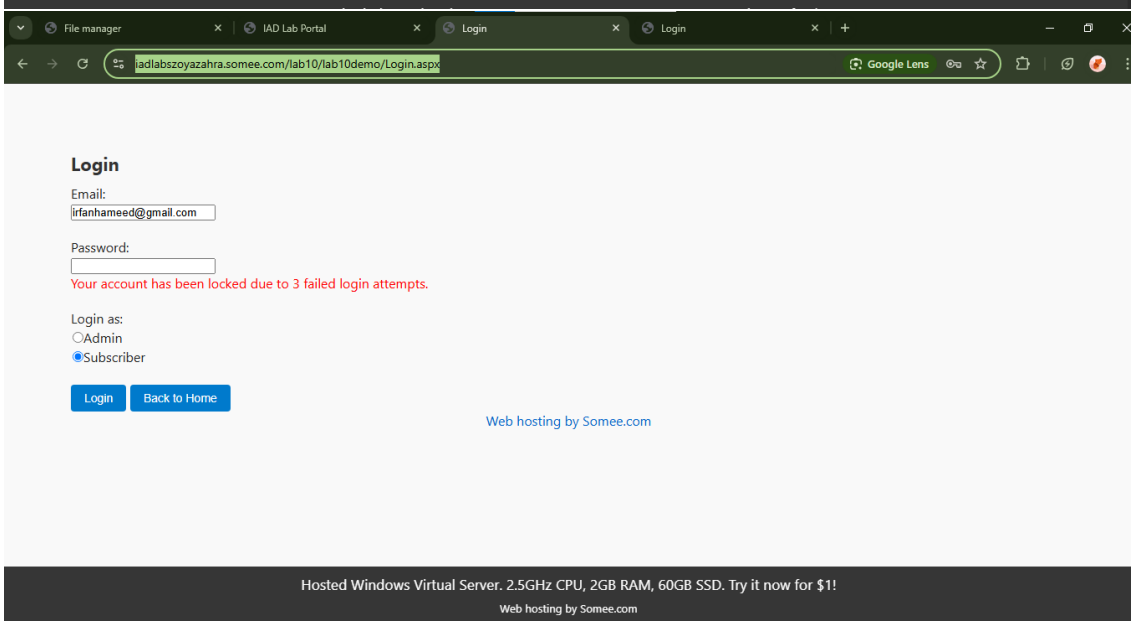

iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Login
Email:
admin1@gmail
Password:
Please enter a valid email address.
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com

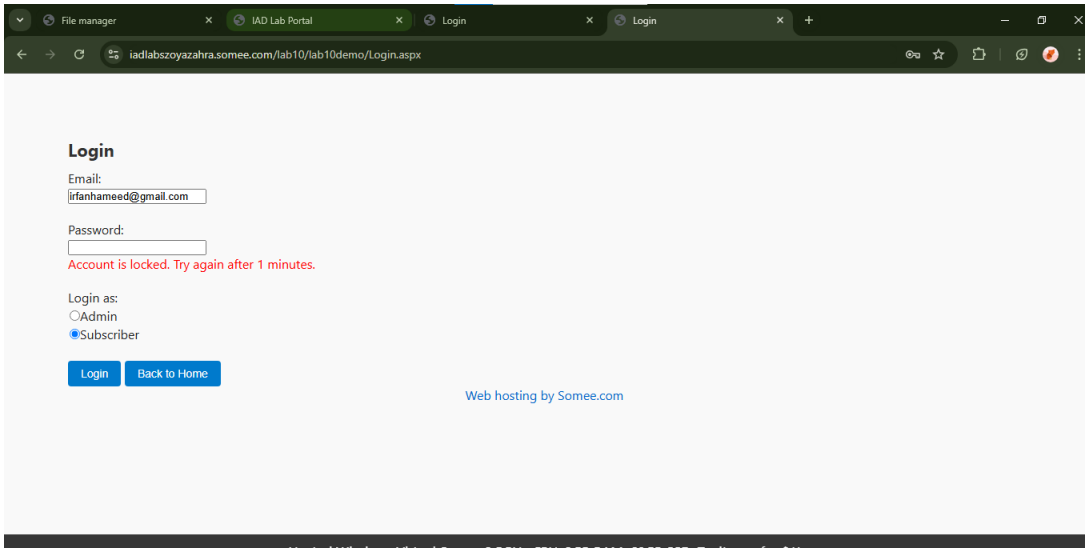

iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Login
Email:
admin1@gmail.com
Password:
Invalid admin credentials.
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com


iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Login
Email:
admin1@gmail.com
Password:
Email not found.
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com


iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Login
Email:
irfanhameed@gmail.com
Password:
Invalid password. Attempts remaining: 2
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com


iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Login
Email:
irfanhameed@gmail.com
Password:
Invalid password. Attempts remaining: 1
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com


File manager
IAD Lab Portal
Login
Login
iadlabszoyazahra.somee.com/lab10/lab10demo/Login.aspx
Google Lens
Login
Email:
irfanhameed@gmail.com
Password:
Your account has been locked due to 3 failed login attempts.
Login as:
Admin
Subscriber
Login
Back to Home
Web hosting by Somee.com
Hosted Windows Virtual Server. 2.5GHz CPU, 2GB RAM, 60GB SSD. Try it now for $1!
Web hosting by Somee.com



SESSION TIMEOUT: (Giving Errors, when I added it in vs code web.config, it worked perfectly, but when I added this timeout in hosted web.config, it gave configuration error)

```
    The following attributes can be set on the <httpRuntime> tag.
      <system.Web>
        <httpRuntime targetFramework="4.8.1" />
      </system.Web>
  -->
  <system.web>
    <compilation debug="false" targetFramework="4.8.1">
      <assemblies>
        <add assembly="System.Transactions, Version=4.0.0.0, Culture=neutral, PublicKeyToken=B77A5C561934E089"/>
      </assemblies>
    </compilation>
    <pages controlRenderingCompatibilityVersion="4.0"/>

  </system.web>
  <system.web>
<sessionState timeout="15" />
  </system.web>
</configuration>
```

Note:

(i) This is an individual student assignment.

(ii) All report and implementation work must be non AI generated / non copilot generated in order to get good score.

(iii) Submission of copied work (by any means/through any channel) will lead to poor grades

Submission of "Lab 13"

(i) Deadline is 22:00 on 13th May 2025.

(ii) Submit all above problems by creating suitable links (under Lab 13) on your own portal.

(iii) For problem 1 and 3 you may upload pdf file or create html pages.

(iv) For problem 2 make a live demo available online.

(v) Submit all codes and interfaces through suitable links.

(vi) On first page of your portal clearly write your name and registration number.

(vii) Do not change your portal address / url.