1. Password Hashing (SHA-256)

	Email	PasswordHash
1	admin@gmail.com	240be518fabd2724ddb6f04eeb1da5967448d7e831c08c8fa8...
2	customer	983487d9c4b7451b0e7d282114470d3a0ad50dc5e554971a...

2.. SQL Injection Protection

Email:

customer ' OR '1'='1

Password:

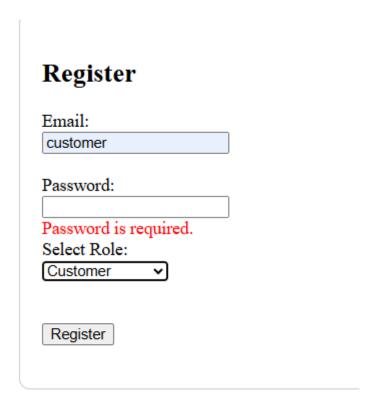Login

User not found.

3.. Role-Based Access Control (RBAC)

Access Denied

You do not have permission to view this page.

Go to Login

4. Input Validation (Client + Server Side)

Register

Email:

```
customer
```

Password:

Password is required.

Select Role:

```
Customer          ∨
```

Register

5.HTML Encoding to Prevent XSS

The code

```
Else
    lblWelcome.Text = "Hello, " & Server.HtmlEncode(Session("UserEmail").ToString())
End If
```

The output

Server Error in '/' Application.

A potentially dangerous Request.Form value was detected from the client (txtEmail="<script>alert('xss')...").

6.Session-Based Authentication

I have tested the session-based authentication by logging in and manually clearing the session. It is working correctly, and I will further demonstrate it in the video demo as well.

7. Logout (Session Termination)

The code of session logout

```vbnet
0 references
Protected Sub btnLogout_Click(sender As Object, e As EventArgs)
    Session.Clear()
    Session.Abandon()
    Response.Redirect("Login.aspx")
End Sub
```