

Phát triển ứng dụng Web

Bảo mật ứng dụng Web ASP.NET

Ths. Trần Thị Bích Hạnh

Khoa CNTT – ĐH.KHTN

Nội dung

- Một số khái niệm về Bảo mật
- Các cấp độ bảo mật trong một ứng dụng ASP.NET
- Đăng nhập, Quản lý thành viên, phân quyền trong ASP.NET

Nội dung

- Một số khái niệm về Bảo mật
- Các cấp độ bảo mật trong một ứng dụng ASP.NET
- Đăng nhập, Quản lý thành viên, phân quyền trong ASP.NET

Một số Khái niệm Bảo mật

- **Authentication – Chứng thực**

- Qui trình chứng thực người dùng
- Thường yêu cầu người dùng nhập Tên đăng nhập & mật khẩu

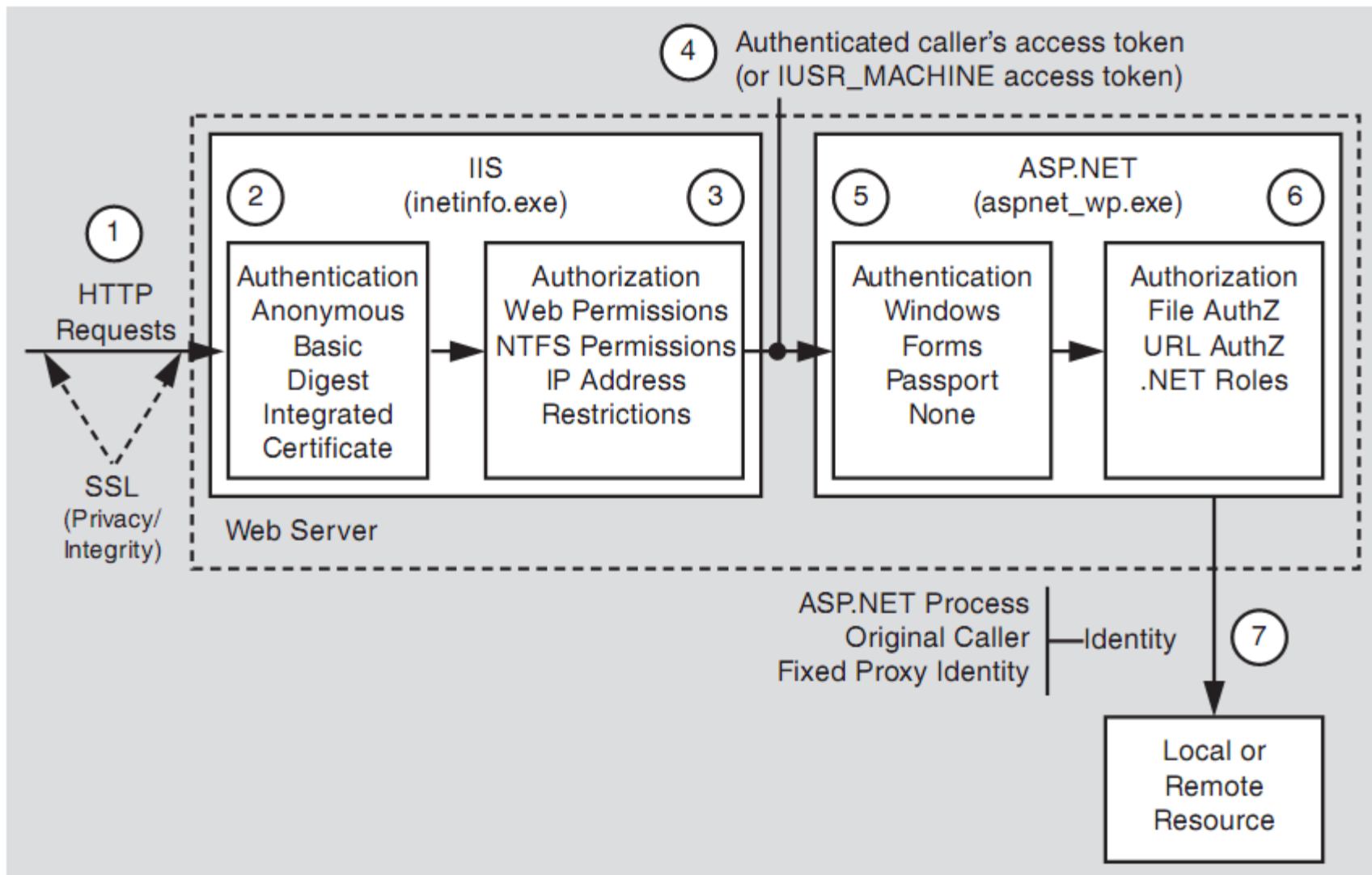
- **Authorization – Cấp quyền**

- Qui trình quyết định user đã chứng thực được phép truy cập các tài nguyên nhất định
- Thường cấp quyền dựa trên Loại người dùng (**role-based authorization**)

Nội dung

- Một số khái niệm về Bảo mật
- Các cấp độ bảo mật trong một ứng dụng ASP.NET
- Đăng nhập, Quản lý thành viên, phân quyền trong ASP.NET

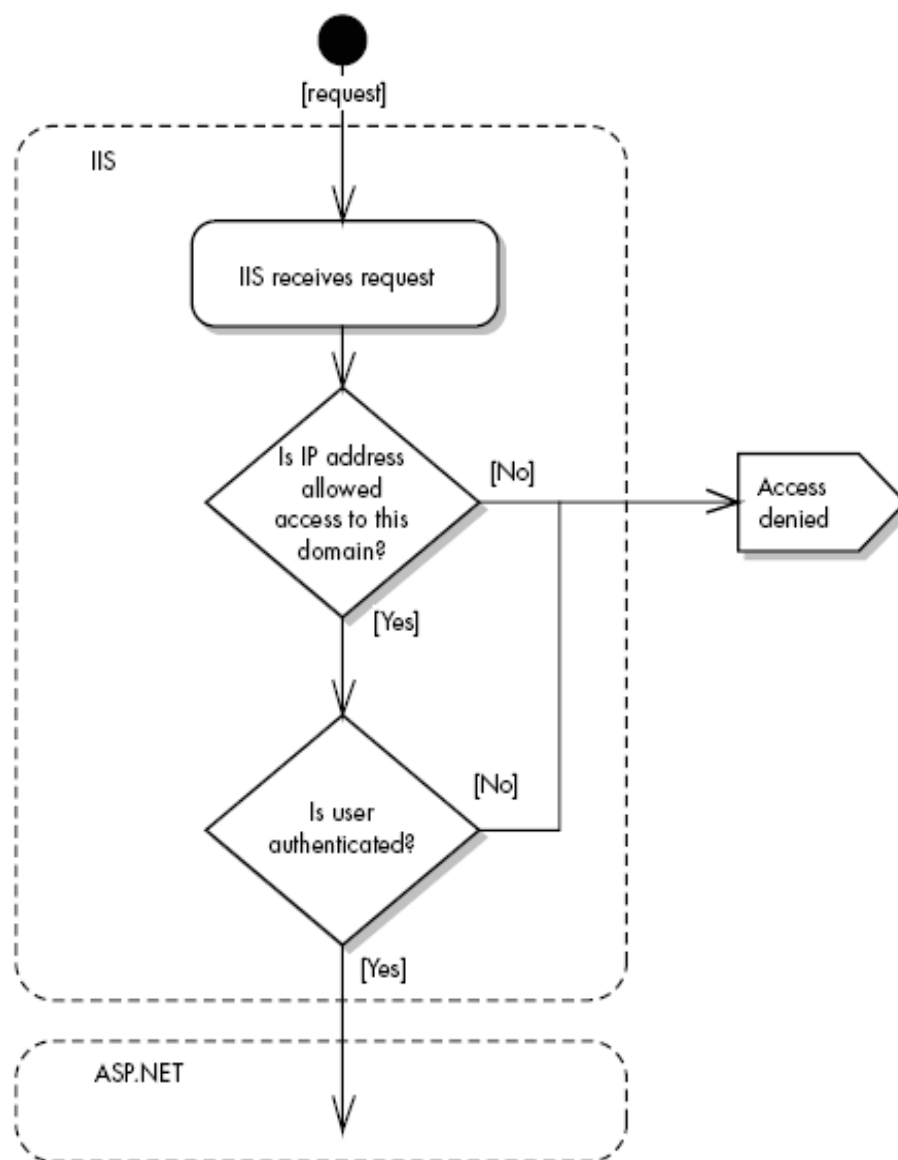
Các cấp độ bảo mật trong ASP.NET



IIS Security

- Là cấp độ bảo mật đầu tiên được thực hiện khi có yêu cầu đến webpage (request).
- Các bước kiểm tra:
 - IIS kiểm tra địa chỉ IP của request có được truy cập vào domain hay không
 - Chứng thực người dùng (nếu cần)
 - Nếu thành công chuyển request qua ASP.NET
 - Ngược lại thông báo cho người dùng biết không được phép truy cập

IIS Security

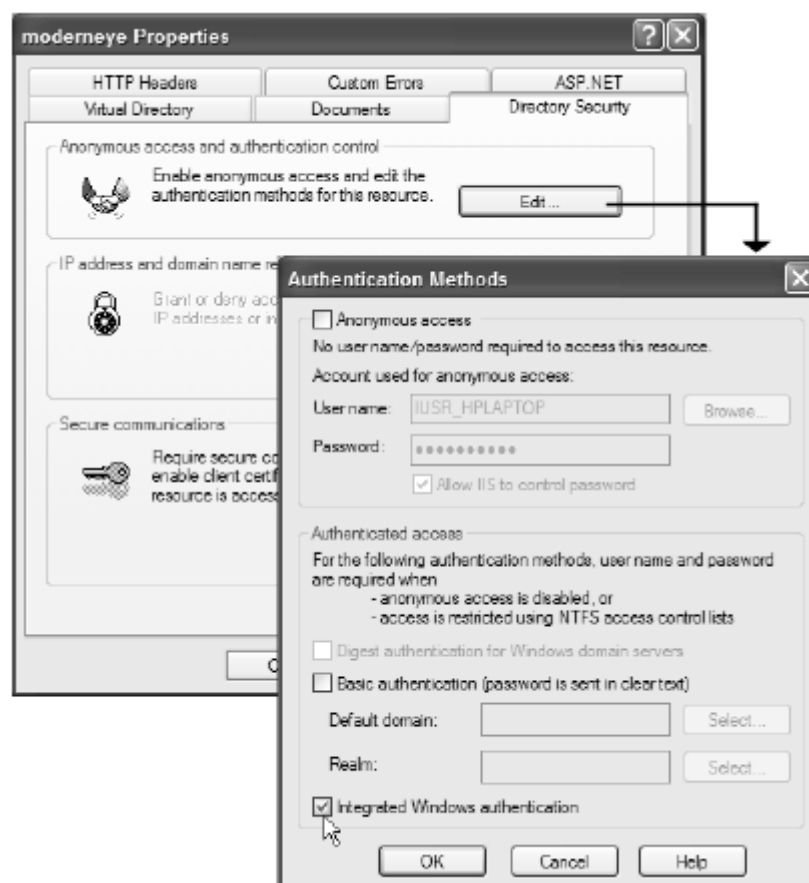


Các hình thức chứng thực trong IIS

- Anonymous
- Basic
- Digest
- Integrated Windows Authentication
- Certificate

IIS Anonymous Authentication

- Mặc định IIS cho phép **anonymous** truy cập vào một ứng dụng Web



IIS Basic & Digest Authentication

- **Basic**

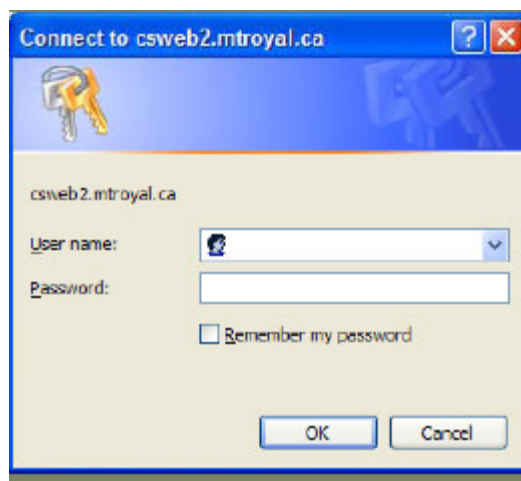
- Yêu cầu user nhập username & password
- Username & password được mã hóa và truyền qua HTTP header
- Username & password được kiểm tra khớp với tài khoản Windows trên server
- Chỉ nên sử dụng với HTTPS

- **Digest**

- Password được xử lý với hàm hash và gửi lên server
- Server thực hiện cùng xử lý với hàm hash với password trên server và kiểm tra với giá trị nhận được

IIS Integrated Windows Authentication

- IIS chứng thực user với tài khoản user trên Windows
- Khi sử dụng trong mạng intranet, Windows Authentication cho phép IIS quyết định yêu cầu của người dùng dựa vào việc đăng nhập của user trên Windows

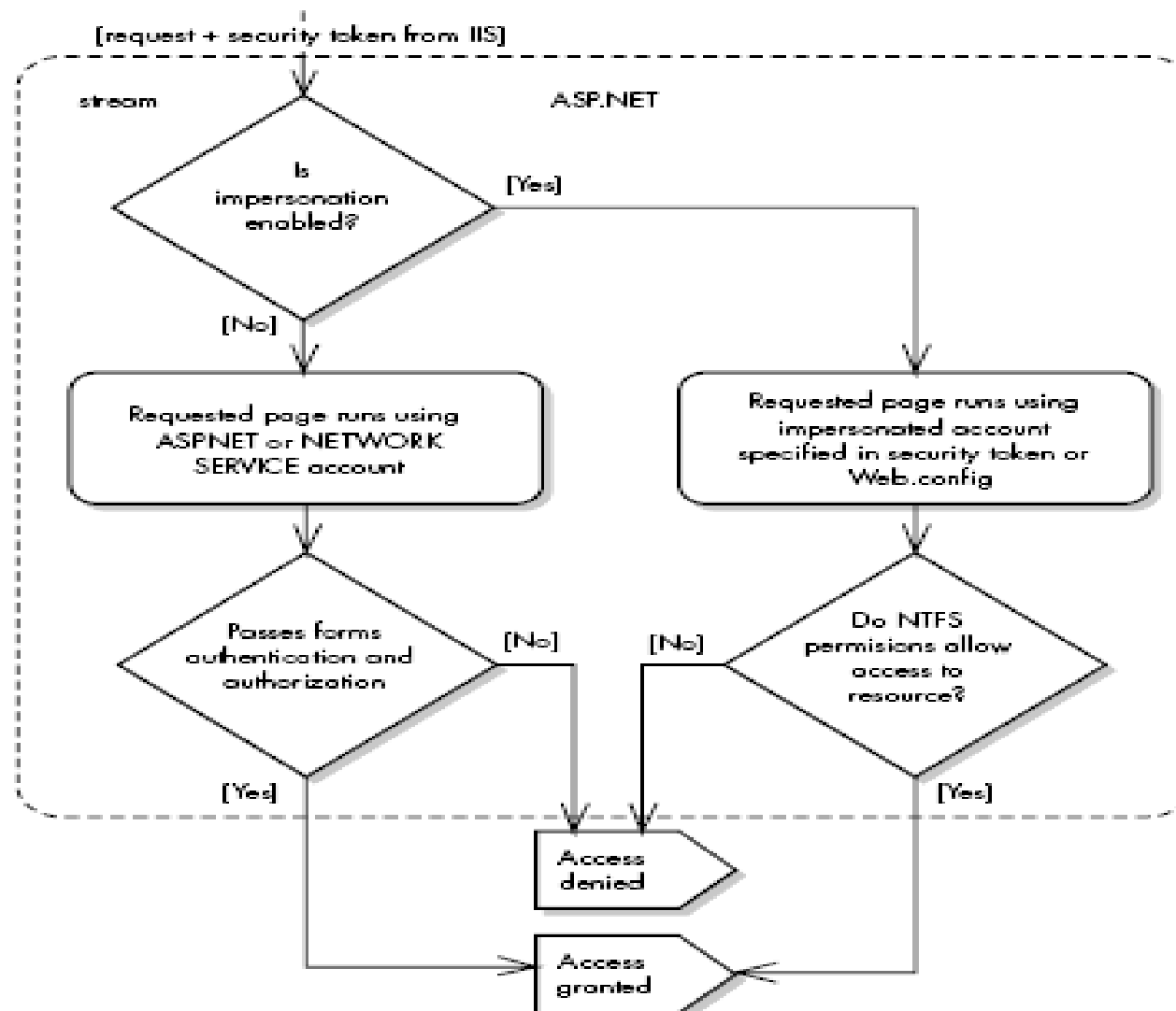


IIS Certificate Authentication

■ Certificate

- Sử dụng các certificate của user để thực hiện việc chứng thực
- Trong mã hóa khóa công khai (public-key cryptography) một certificate sử dụng một chữ ký điện tử (digital signature) và một khóa công khai đi kèm với định danh người dùng

ASP.NET Security



Impersonation

- Mặc định Impersonation là disabled
 - Tất cả ASP.NET request được thực thi bởi định danh mặc định dành cho các ứng dụng ASP.NET
 - Tài khoản ASPNET tự động được tạo khi cài .NET Framework
 - Tài khoản NETWORK SERVICE được định nghĩa sẵn trong Windows Server 2003 và có quyền truy cập như tài khoản ASPNET

Impersonation

- Khi thiết lập impersonation là enabled cho một ứng dụng Web, ứng dụng sẽ được thực thi dưới định danh được chỉ định bởi một security token truyền từ IIS
- Sử dụng impersonation khi
 - Ứng dụng web dựa vào IIS để chứng thực user
 - Server cho phép host nhiều ứng dụng từ nhiều khách hàng khác nhau, cung cấp cho mỗi ứng dụng web một tài khoản Windows riêng biệt để ngăn không cho ứng dụng này truy cập vào tài nguyên của ứng dụng khác

```
// Web.Config  
<authentication mode="Windows" />  
<identity impersonate="true" />
```


Code Access Security

- Tính năng được hỗ trợ trong CLR
- Qui định những ràng buộc cho phép các loại mã lệnh trong assembly được quyền thực thi
- **Trust level là một tập các luật** định nghĩa các class trong .NET Framework mà ứng dụng ASP.NET được phép sử dụng

```
// Web.config
<system.web>
  ...
  <trust level="Medium"/>
</system.web>
```

Trust Levels

- **Full**
 - Tất cả .NET class được phép sử dụng & thực thi
- **High**
 - Không được sử dụng unmanaged code, enterprise services, reflection
- **Medium**
 - Ứng dụng chỉ được phép truy xuất trong cấu trúc thư mục của nó
- **Low**
 - Read-only application
- **Minimal**
 - Không được phép truy cập tài nguyên

ASP.NET Authentication

- **None**

- ASP.NET không thực hiện việc chứng thực

- **Windows**

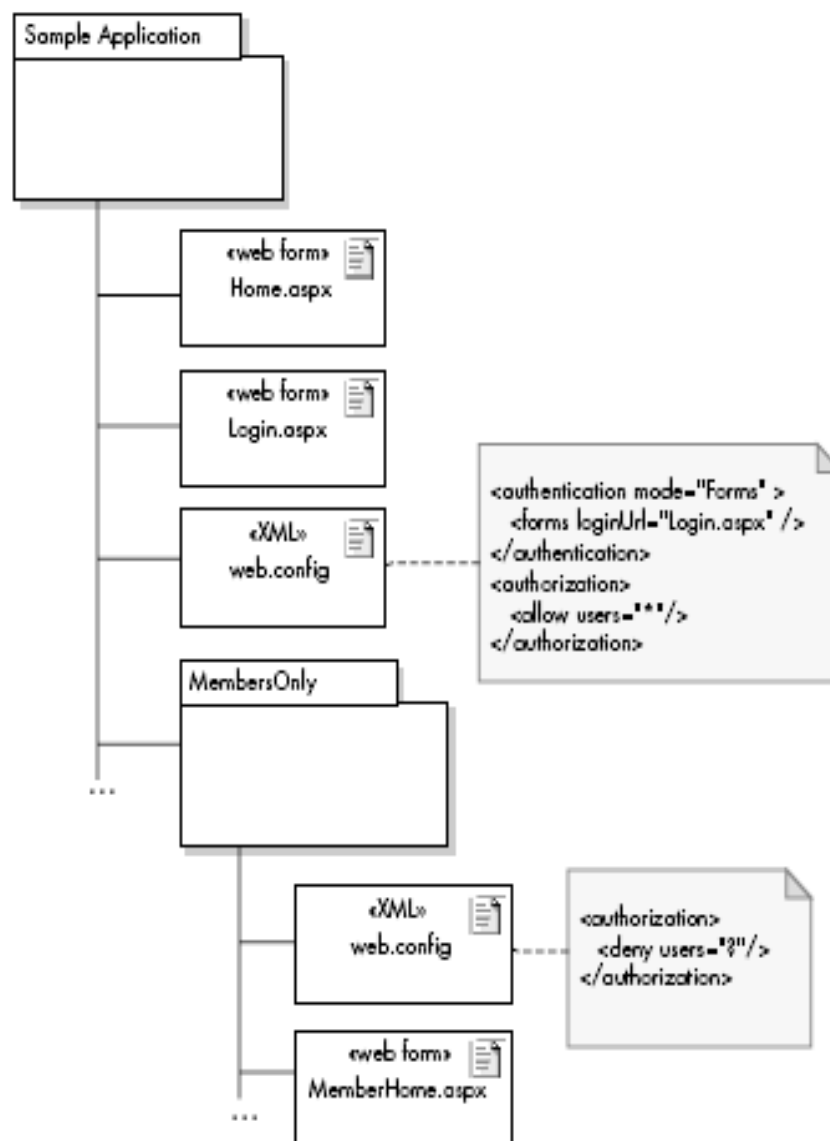
- Sử dụng kết quả từ cơ chế chứng thực trong cấu hình của IIS

- **Forms**

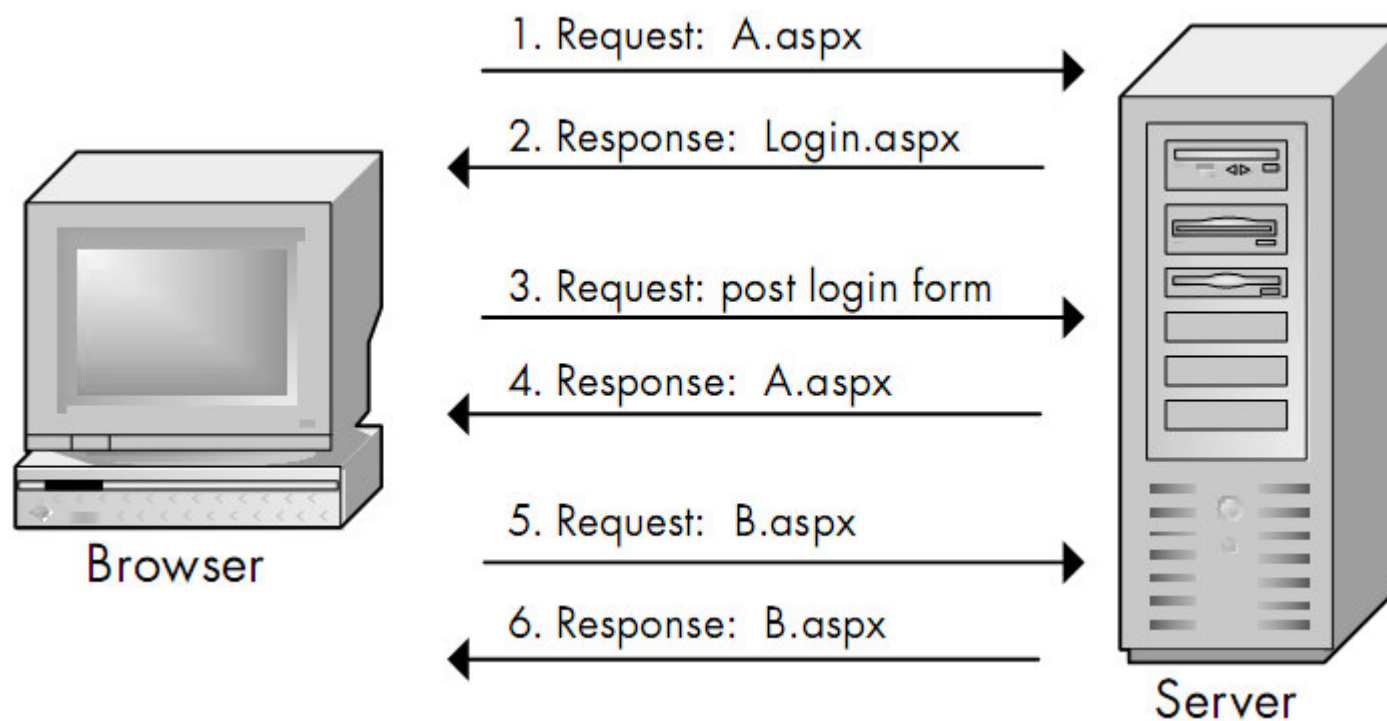
- Cho phép chứng thực thông qua form đăng nhập

- **Passport**

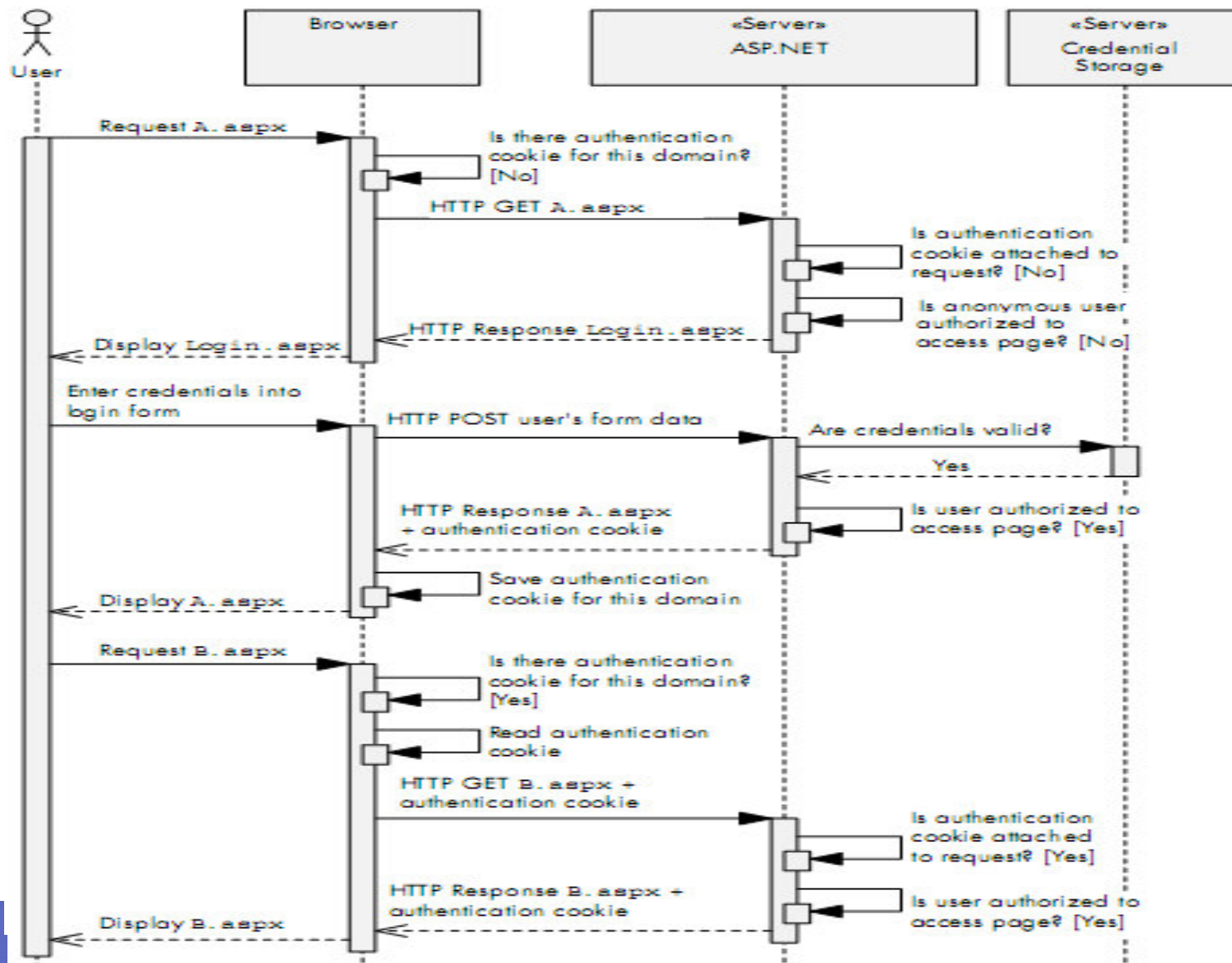
- Sử dụng dịch vụ chứng thực của Microsoft Passport



Forms Authentication



Forms Authentication



Forms Authentication

Thuộc tính	Ý nghĩa
Cookieless (UseDefaultProfile)	Qui định việc chứng thực lưu trong cookie: UseCookies, UseUri (nhúng ticket trong URL), và AutoDetect
defaultUrl	Đường dẫn đến trang web sau khi chứng thực user thành công
loginUrl	Đường dẫn đến trang login
protection (All)	Qui định cách thức mã hóa authentication ticket: All (hash & encrypt), Encryption, None, Validation (check ticket có bị sửa đổi)
requireSSL (false)	Yêu cầu sử dụng kết nối SSL khi truyền dữ liệu

Forms Authentication

Thuộc tính	Ý nghĩa
domain	Domain chứng thực cookie
enableCrossAppRedirects (false)	Cho phép nhiều ứng dụng web sử dụng cùng 1 chứng thực
name	Tên cookie
path	Đường dẫn cho cookie
slidingExpiration (false)	Reset lại thời gian expire của cookie sau lần truy cập cuối
timeout (30 phút)	Qui định thời gian expire của cookie

```
// Web.Config
<authentication mode="Forms" >
  <forms loginUrl="Login.aspx" timeout="86400"
    slidingExpiration="true" />
</authentication>
```

Nội dung

- Một số khái niệm về Bảo mật
- Các cấp độ bảo mật trong một ứng dụng ASP.NET
- Đăng nhập, Quản lý thành viên, phân quyền trong ASP.NET

Membership Provider

- Là tập các lớp của .NET cho phép developer xử lý các chức năng quản lý chứng thực người dùng
 - Thêm người dùng mới
 - Lưu thông tin người dùng trong CSDL
 - Chứng thực người dùng
 - Phân quyền người dùng
 - Quản lý mật khẩu (tạo, sửa, reset)
- Membership Provider mặc định là SqlMembershipProvider
 - Tạo CSDL **aspnetdb** trong SQLExpress và lưu trong thư mục App_Data

Role Management Provider

- Là tập các lớp của .NET cho phép developer xử lý các chức năng quản lý cấp quyền người dùng
 - Thêm role mới
 - Chỉ định người dùng vào các roles
 - Phân quyền cho phép người dùng truy cập vào tài nguyên web
- Role Management Provider mặc định là SqlRoleProvider

ASP.NET Login Controls

- CreateUserWizard
- Login
- LoginName & LoginStatus
- LoginView
- ChangePassword
- PasswordRecovery

CreateUserWizard Control

```
<asp:CreateUserWizard ID="createUser" runat="server" ... >  
  
    <WizardSteps>  
        <asp:WizardStep >  
            ...  
        </asp:WizardStep>  
        <asp:WizardStep >  
            ...  
        </asp:WizardStep>  
    </WizardSteps>  
</asp:CreateUserWizard>
```

CreateUserWizard Control

This page demonstrates the CreateUserWizard control.

Sign Up for Your New Account

User Name:

Password:

Confirm Password:

E-mail:

Security Question:

Security Answer:

Internet Explorer

http://localhost:1046/Chapter 13/CreateUserControl.aspx

Complete

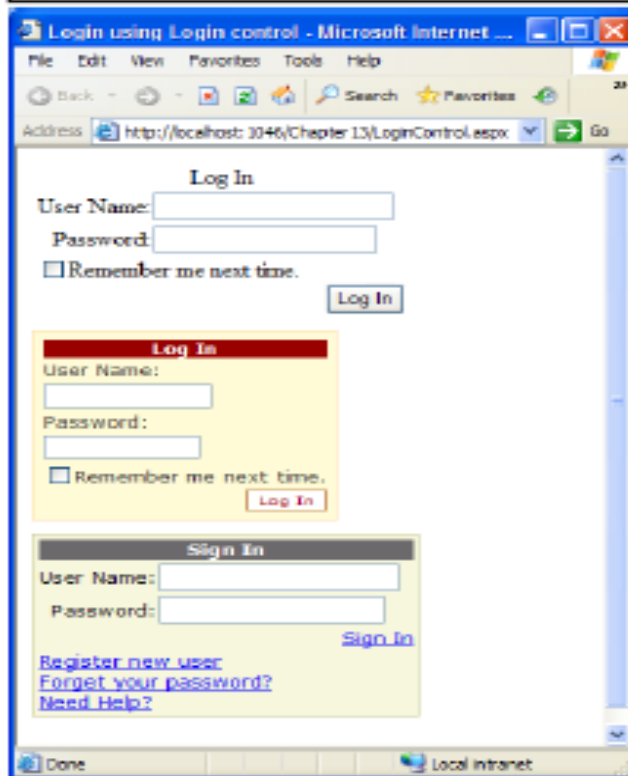
Your account has been successfully created.

Login Control

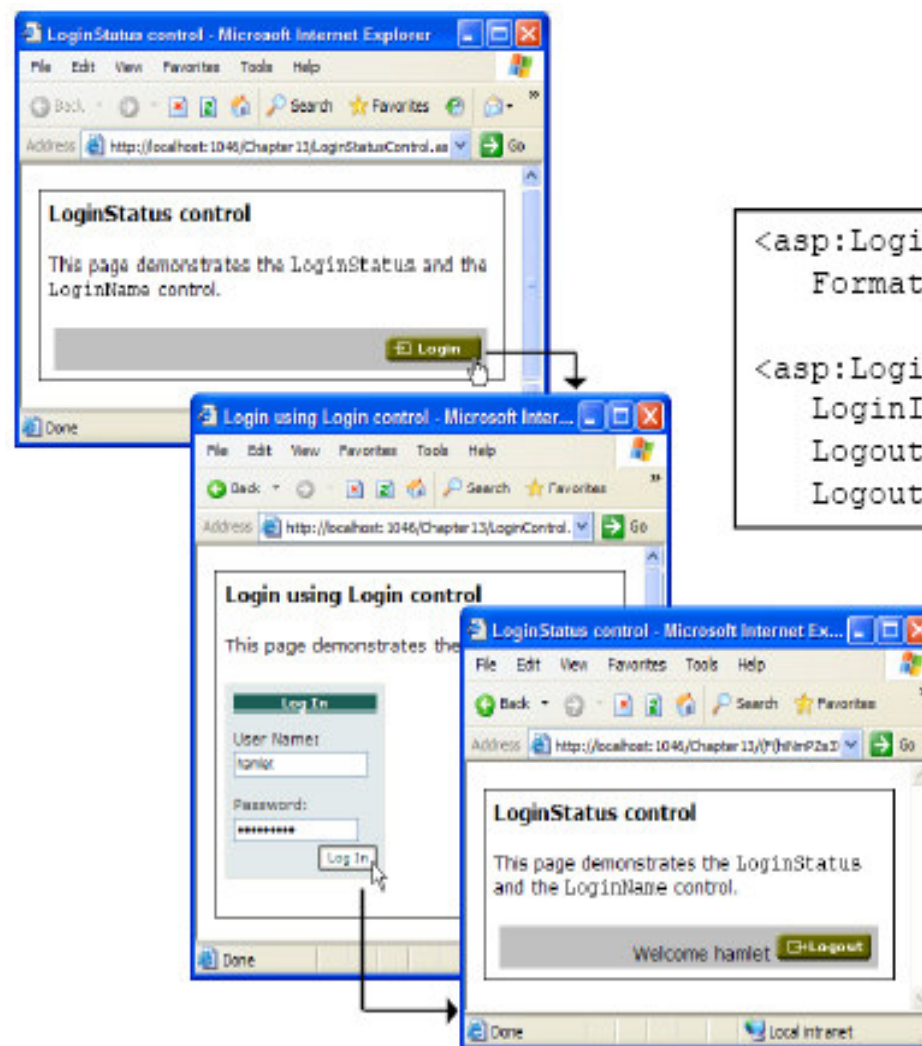
```
<asp:Login ID="logSignin2" runat="server"
    TextLayout="TextOnTop" CssClass="loginStyle">

    <TitleTextStyle CssClass="loginTitle" />
    <InstructionTextStyle Font-Italic="True" ForeColor="Black" />
    <TextBoxStyle Font-Size="0.8em" />
    <LoginButtonStyle CssClass="buttonStyle" />

</asp:Login>
```



LoginName and LoginStatus Controls



The image displays three overlapping screenshots of a web application running in Microsoft Internet Explorer, demonstrating the LoginStatus and LoginName controls.

- Top Screenshot:** Shows the initial state of the **LoginStatus control**. The text reads: "This page demonstrates the LoginStatus and the LoginName control." Below the text is a single button labeled **Login**.
- Middle Screenshot:** Shows the login form. The text reads: "Login using Login control". Below the text is a form with fields for **User Name:** (containing "hamlet") and **Password:** (masked with asterisks). A **Login** button is present.
- Bottom Screenshot:** Shows the state after successful login. The text reads: "LoginStatus control". Below the text, it says "Welcome hamlet" followed by a **Logout** button.

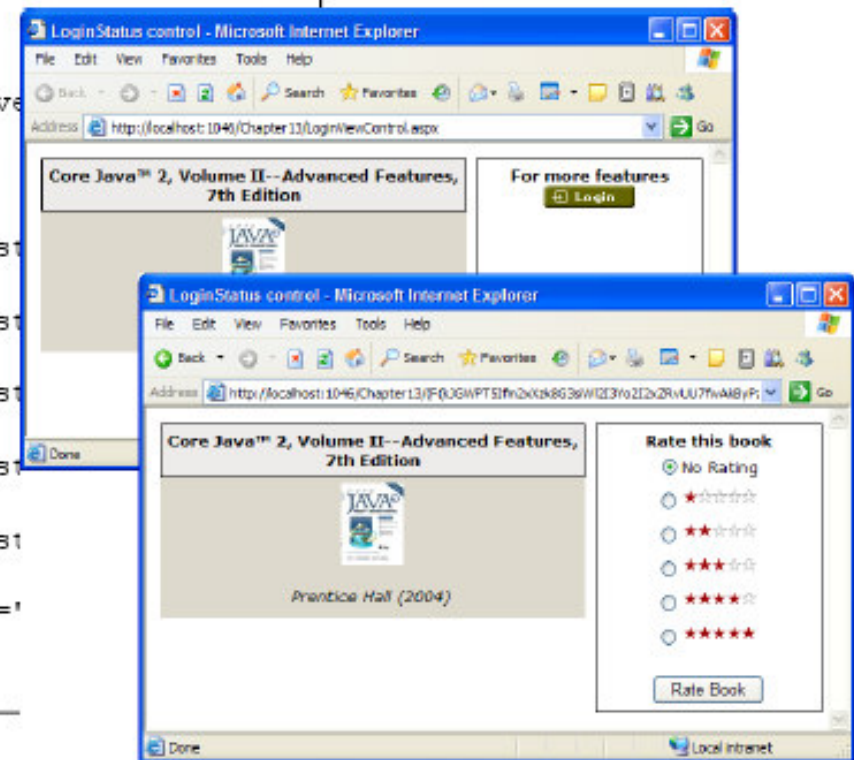
```
<asp:LoginName ID="logName" runat="server"
    FormatString="Welcome {0}" />

<asp:LoginStatus ID="logStat" runat="server"
    LoginImageUrl="images/btn_login.gif"
    LogoutImageUrl="images/btn_logout.gif"
    LogoutAction="Refresh" />
```

LoginView Control

```
<asp:LoginView ID="logView" runat="server">
  <AnonymousTemplate>
    <strong>For more features</strong><br />
    <asp:LoginStatus ID="logStat" runat="server"
      LoginImageUrl="images/btn_login.gif"
      LogoutImageUrl="images/btn_logout.gif"
      LogoutAction="Refresh" />
  </AnonymousTemplate>

  <LoggedInTemplate>
    <strong>Rate this book</strong><br />
    <asp:RadioButtonList ID="radList" runat="server">
      <asp:ListItem Selected="true">
        No Rating</asp:ListItem>
      <asp:ListItem>
        <img src='images/stars1.gif' /></asp:ListItem>
      <asp:ListItem>
        <img src='images/stars2.gif' /></asp:ListItem>
      <asp:ListItem>
        <img src='images/stars3.gif' /></asp:ListItem>
      <asp:ListItem>
        <img src='images/stars4.gif' /></asp:ListItem>
      <asp:ListItem>
        <img src='images/stars5.gif' /></asp:ListItem>
    </asp:RadioButtonList>
    <asp:Button ID="btnRate" runat="server" Text="Rate Book" />
  </LoggedInTemplate>
</asp:LoginView>
```



ChangePassword Control

```
<asp:ChangePassword ID="chngPass" runat="server"
    CssClass="passChangeStyle" >

    <CancelButtonStyle CssClass="buttonStyle" />
    <ChangePasswordButtonStyle CssClass="buttonStyle" />
    <ContinueButtonStyle CssClass="buttonStyle" />
    <TitleTextStyle CssClass="titleStyle" />
    <TextBoxStyle CssClass="textboxStyle" />

</asp:ChangePassword>
```



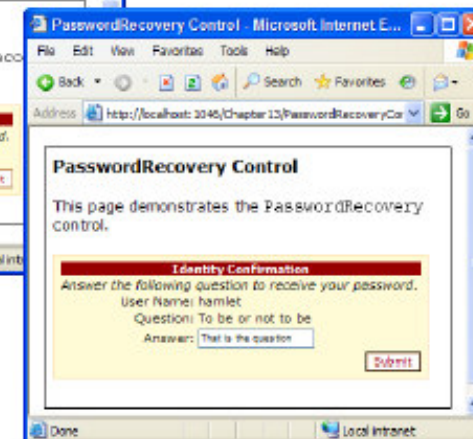
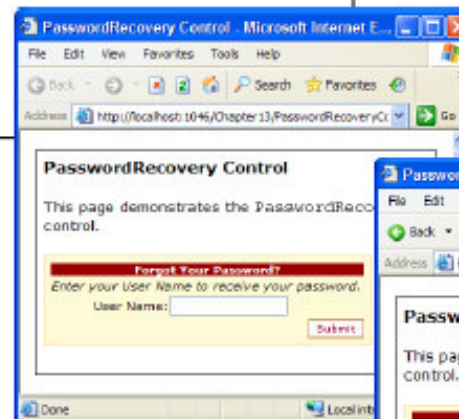
PasswordRecovery Control

```
<asp:PasswordRecovery ID="passRec" runat="server"
    CssClass="passRecovStyle">

    <InstructionTextStyle CssClass="instructionStyle" />
    <SuccessTextStyle CssClass="instructionStyle" />
    <TextBoxStyle CssClass="textboxStyle" />
    <TitleTextStyle CssClass="titleStyle" />
    <SubmitButtonStyle CssClass="buttonStyle" />

    <MailDefinition From="abc@abc.net"
        Subject="Password Recovery" />

</asp:PasswordRecovery>
```



Cấu hình Mail Server (SMTP)

Configure SMTP Settings

Server Name:

Server Port:

From:

Authentication:

☐ None

☒ Basic

Choose this option if your e-mail server requires you to explicitly pass a user name and password when sending an e-mail message.

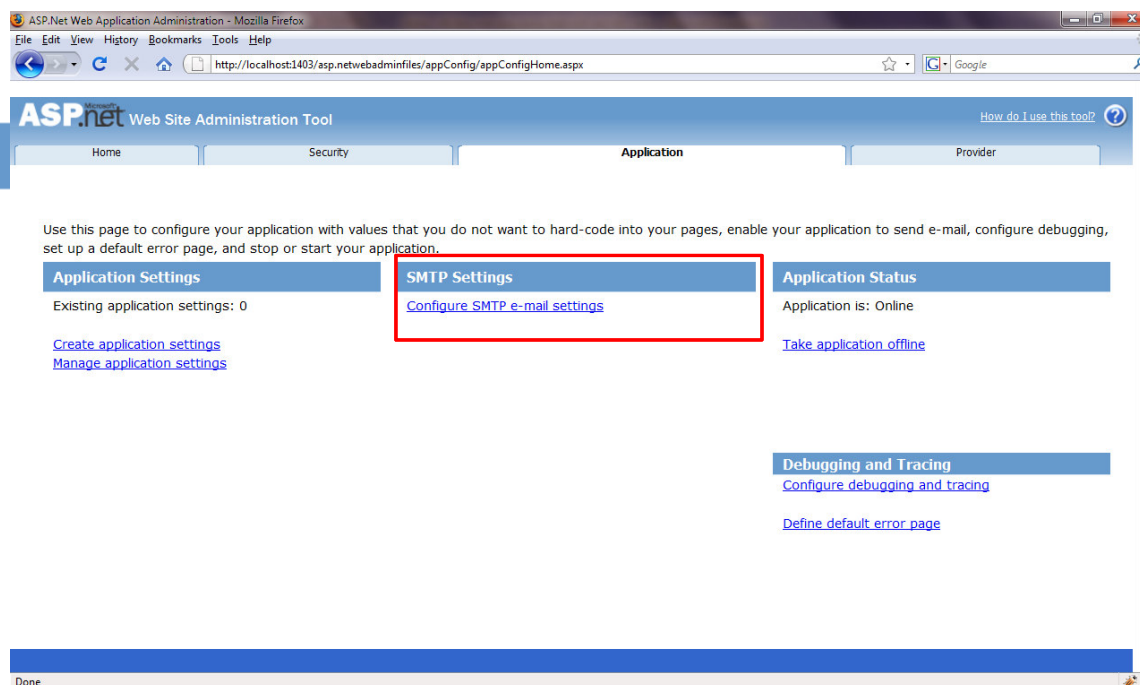
Sender's user name:

Sender's password:

☐ NTLM (Windows authentication)

Choose this option if your e-mail server is on a local area network and you connect to it using windows credentials.

Save



Cấu hình Mail Server (SMTP)

```
// Web.Config
<configuration>
  <system.net>
    <mailSettings>
      <smtp deliveryMethod="Network" from="yourmail@gmail.com">
        <network
          host="smtp.gmail.com" port="587"
          userName="yourmail@gmail.com" password="your password"
          defaultCredentials="true"/>
        </smtp>
      </mailSettings>
    </system.net>
    ...
  </configuration>
```

Xử lý Gửi mail lấy lại Password

```
using System.Net;
using System.Net.Mail;

protected void PasswordRecovery1_SendingMail(object sender,
    MailMessageEventArgs e) {
    try
    {
        SmtpClient smtpSender = new SmtpClient("smtp server", "smtp port");
        smtpSender.DeliveryMethod = SmtpDeliveryMethod.Network;
        smtpSender.Credentials = new NetworkCredential("username", "password");
        smtpSender.EnableSsl = true;
        smtpSender.Send(e.Message);
    } catch (Exception ex) {
        Response.Write("There was a problem sending the email. " + ex);
    }
    e.Cancel = true;
}
```

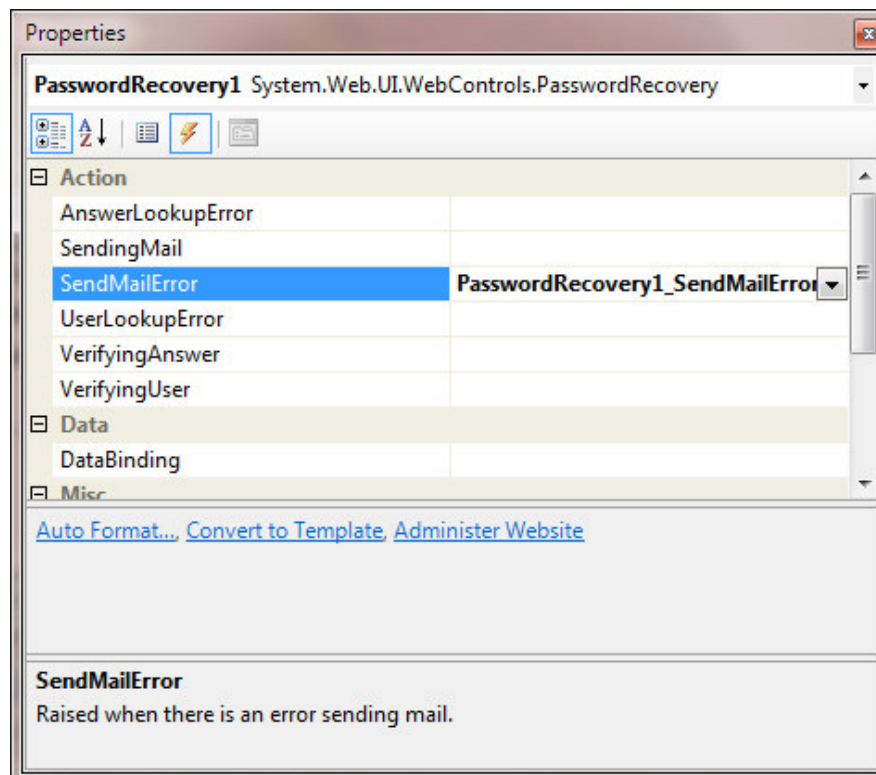
Lấy thông tin cấu hình Mail Server trong Web.config

```
using System.Web.Configuration;
using System.Net.Configuration;

Configuration config =
    WebConfigurationManager.OpenWebConfiguration(HttpContext.Current.Request.ApplicationPath);
MailSettingsSectionGroup settings =
    (MailSettingsSectionGroup)config.GetSectionGroup("system.net/mailSettings");

// settings.Smtp.Network.Host
// settings.Smtp.Network.Port
// settings.Smtp.Network.Username
// settings.Smtp.Network.Password
```

Xử lý lỗi Gửi mail



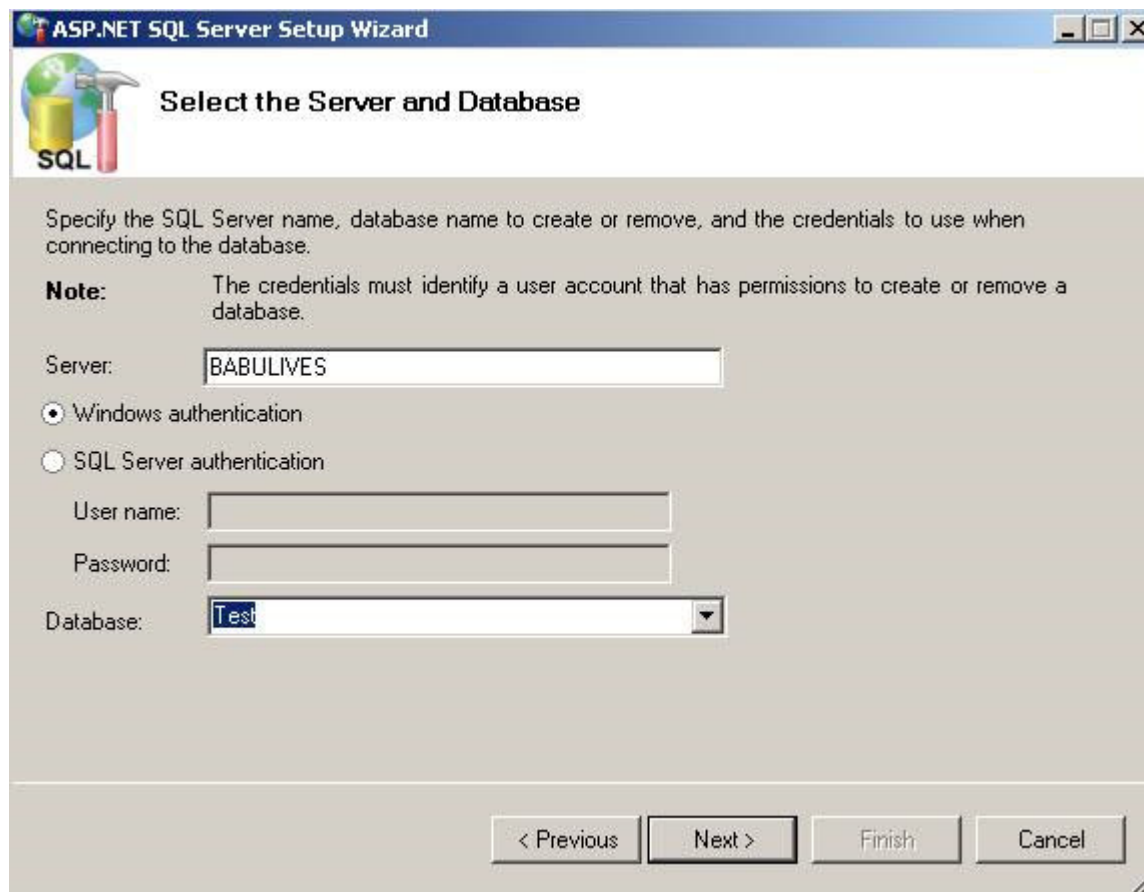
```
protected void PasswordRecovery1_SendMailError(object sender,  
    SendMailErrorEventArgs e)  
{  
  
    e.Handled = true;  
  
    PasswordRecovery1.SuccessText = e.Exception.Message;  
  
}
```

Cấu hình sử dụng Database riêng cho Membership & Role

- Bước 1: Thực thi **ASP.NET Sql Server Registration Tool** để tạo CSDL
 - WINDOWS\Microsoft.NET\Framework\2.0.xxxx**aspnet_regsql.exe**
- Bước 2: Cấu hình **ConnectionString, Membership Provider & Role Provider** trong **Web.Config**
- Bước 3: Sử dụng **Web Site Administration Tool** để cấu hình phân quyền
 - Menu > **Website > ASP.NET Configuration**

Cấu hình sử dụng Database riêng cho Membership & Role

■ Bước 1



The screenshot shows the 'ASP.NET SQL Server Setup Wizard' window. The title bar reads 'ASP.NET SQL Server Setup Wizard'. The main heading is 'Select the Server and Database'. Below this, there is a note: 'Specify the SQL Server name, database name to create or remove, and the credentials to use when connecting to the database.' A sub-note states: 'Note: The credentials must identify a user account that has permissions to create or remove a database.' The form contains the following fields: 'Server:' with the text 'BABULIVES'; 'Authentication' section with 'Windows authentication' selected (radio button) and 'SQL Server authentication' unselected; 'User name:' and 'Password:' text boxes; and 'Database:' dropdown menu with 'Test' selected. At the bottom, there are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

- <http://www.codedigest.com/FAQ/16-How-to-Configure-ASP-Net-Membership-Providers-to-Use-Our-Own-Database-.aspx>

Cấu hình sử dụng Database riêng cho Membership & Role

■ Bước 2

```
<!-- Set the connection string for SQL Server -->  
<connectionStrings>  
  <clear />  
  <add name="SqlConn"  
    connectionString="Data Source=localhost;Integrated Security=SSPI;Initial Catalog=Test;"  
  />  
</connectionStrings>
```

- <http://help.maximumasp.com/SmarterTicket/Customer/KBArticle.aspx?articleid=878>

Cấu hình sử dụng Database riêng cho Membership & Role

■ Bước 2 (tt)

```
<system.web>

  <!-- Configure the Sql Membership Provider -->
  <membership defaultProvider="MySqlMembershipProvider" userIsOnlineTimeWindow="15">
    <providers>
      <clear />
      <add
        name="MySqlMembershipProvider"
        type="System.Web.Security.SqlMembershipProvider"
        connectionStringName="SqlConn"
        applicationName="/"
        enablePasswordRetrieval="false"
        enablePasswordReset="false"
        requiresQuestionAndAnswer="false"
        requiresUniqueEmail="true"
        passwordFormat="Hashed" />
    </providers>
  </membership>
</system.web>
```

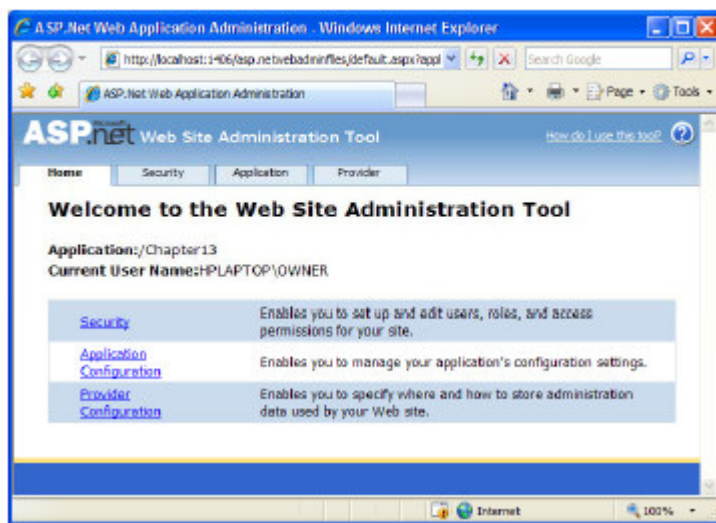
Cấu hình sử dụng Database riêng cho Membership & Role

■ Bước 2 (tt)

```
<system.web>
  <!-- Configure the Sql Role Provider -->
  <roleManager enabled="true"
    defaultProvider="MySQLRoleProvider" >
    <providers>
      <clear />
      <add name="MySQLRoleProvider"
        type="System.Web.Security.SqlRoleProvider"
        connectionStringName="SqlConn"
        applicationName="/" />
    </providers>
  </roleManager>
</system.web>
```

Cấu hình sử dụng Database riêng cho Membership & Role

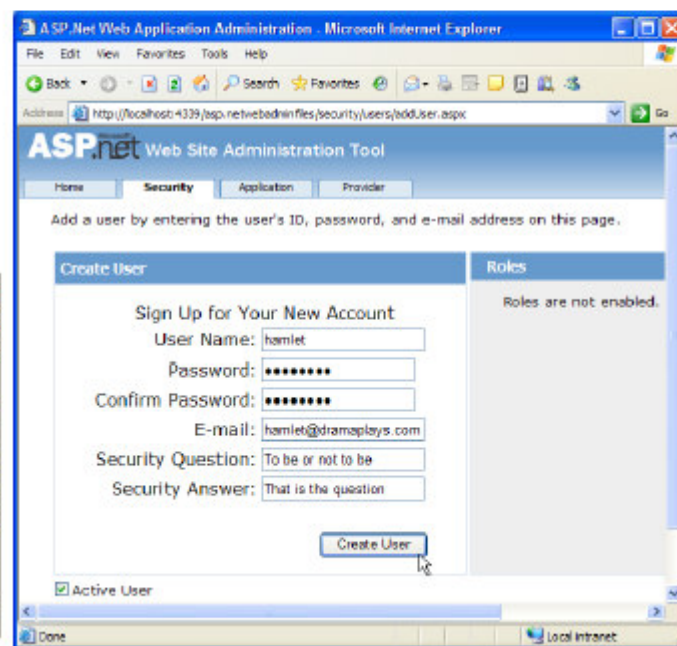
■ Bước 3: Website Administration Tool



The screenshot shows two SQL Server tables. The first table is 'aspnet_Users' from the 'ASPNETDB' database. The second table is 'aspnet_Membership' from the 'ASPNETDB' database.

ApplicationId	UserId	UserName	LoweredUserName	MobileAlias	IsAnonymous	LastActive
6744f6d4d4200d5	239b1231-566a-...	hamlet	hamlet	NULL	False	29/06/200...
7fc5e7bb-2559-...	7e55e1af-7fbb-...	plato	plato	NULL	False	29/06/200...
NULL	NULL	NULL	NULL	NULL	NULL	NULL

ApplicationId	UserId	Password	P...	PasswordSalt	M...	Email	Lower...	PasswordQue...	PasswordAnswer
6744f6d4d4200d5	239b12...	gfh95T...	1	YPSV/QY6...	NULL	hamlet@dram...	hamlet...	To be or not to be	8P93GhinoQn...
7fc5e7bb-2...	7e55e4...	eng0J3b...	1	ACS0KosKZ...	NULL	plato@phils...	plato...	what is the goo...	g5K6fpup8t0v...
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL



Membership API

Membership.Method

CreateUser

DeleteUser

FindUsersByEmail

FindUsersByName

GeneratePassword

GetAllUsers

GetNumberOfUsersOnline

GetUser

GetUserNameByEmail

UpdateUser

ValidateUser

```
protected void btnLogin_Click(object s, EventArgs e)
{
    string usr = txtUser.Text;
    string pwd = txtPassword.Text;

    // Use the membership system to authenticate user
    if ( Membership.ValidateUser(usr, pwd) )
        FormsAuthentication.RedirectFromLoginPage(usr,true);
    else
        labError.Text = "User not found, try again";
}
```

MembershipUser API

MembershipUser.Method	MembershipUser.Property
ChangePassword	Comment
ChangePasswordQuestionAndAnswer	CreationDate
GetPassword	Email
ResetPassword	IsApproved
UnLockUser	IsLockedOut
	IsOnline
	LastActivityDate
	LastLockoutDate
	LastLoginDate
	LastPasswordChangedDate
	PasswordQuestion
	UserName

Ví dụ - Quản lý danh sách User trong GridView

```
<asp:ObjectDataSource ID="odsUsers"
    runat="server"

    TypeName="System.Web.Security.Membership"

    SelectMethod="GetAllUsers"

    DeleteMethod="DeleteUser">
    <DeleteParameters>

        <asp:ControlParameter
            ControlID="grdUsers" Type="string"

            PropertyName="SelectedDataKey.Values[0]"
                Name="username" />

    </DeleteParameters>
</asp:ObjectDataSource>
```

	Name	Email	Create Date	Last Login
Delete Select	test	ttbhanh@gmail.com	5/5/2009 8:12:47 AM	5/5/2009 8:12:47 AM
Delete Select	ttbhanh	ttbhanh@fit.hcmuns.edu.vn	5/5/2009 8:13:27 AM	5/5/2009 8:13:27 AM

```
<asp:GridView ID="grdUsers" runat="server"

    DataSourceID="odsUsers"

    AutoGenerateColumns="false"

    AutoGenerateDeleteButton="true"

    AutoGenerateSelectButton="true"

    CellPadding="5"

    DataKeyNames="UserName">

    <Columns>

        <asp:BoundField HeaderText="Name"
            DataField="UserName" />

        <asp:BoundField HeaderText="Email"
            DataField="Email"/>

        <asp:BoundField HeaderText="Create
            Date" DataField="CreationDate" />

        <asp:BoundField HeaderText="Last
            Login" DataField="LastLoginDate" />

    </Columns>
</asp:GridView>
```

Roles API

Roles.Method	Roles.Method
AddUsersToRole	GetAllRoles
AddUsersToRoles	GetRolesForUser
AddUserToRole	GetUsersInRole
AddUserToRoles	RemoveUserFromRole
CreateRole	RemoveUserFromRoles
DeleteCookie	RemoveUsersFromRole
DeleteCookie	RemoveUsersFromRoles
FindUsersInRole	RoleExists
IsUserInRole	

Ví dụ - Hiển thị danh sách Roles trong CheckBoxList

```
<asp:ObjectDataSource ID="odsRoles" runat="server"
    TypeName="System.Web.Security.Roles"
    SelectMethod="GetAllRoles" />
```

Select user roles:


```
<asp:CheckBoxList ID="chkRoles" runat="server"
    DataSourceID="odsRoles" />
```

Select user roles:

☒ administrator

☒ guest

☒ member

Tổng kết

- IIS Security
- ASP.NET Security
- Membership & Role