**<https://pumascan.com/rules/>**

<https://www.c-sharpcorner.com/article/xml-manipulation-in-c-sharp/>

**Debug Build Enabled**

**Insecure Configuration:** The default value for the debug attribute is false.

<system.web>

...

<compilation debug="true" targetFramework="4.5"/>

...

</system.web>

**Secure Configuration:** Remove the debug attribute, or explicitly set the value to false.

<system.web>

...

<compilation debug="false" targetFramework="4.5"/>

...

</system.web>

## Custom Errors Disabled

**nsecure Configuration:** The default value for the mode attribute is RemoteOnly.

<system.web>

...

<customErrors mode="Off" defaultRedirect="/home/error"/>

...

</system.web>

**Secure Configuration:** Explicitly set the mode value to RemoteOnly or On, or simply remove the mode attribute.

<system.web>

...

<customErrors mode="RemoteOnly|On" defaultRedirect="/home/error"/>

...

</system.web>

## Forms Authentication: Insecure Cookie

**Insecure Configuration:** The default value for the requireSSL attribute is false.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" timeout="30" />

</authentication>

...

</system.web>

**Secure Configuration:** Explicitly set the requireSSL value to true.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" requireSSL="true"/>

</authentication>

...

</system.web>

## Forms Authentication: Cookieless Mode

**Insecure Configuration:** The default value for the cookieless attribute is UseDeviceProfile, which can allow URL-based authentication tokens.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" />

</authentication>

...

</system.web>

**Secure Configuration:** Explicitly set the cookieless attribute to UseCookies.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" cookieless="UseCookies" />

</authentication>

...

</system.web>

## Forms Authentication: Cross App Redirects

**Insecure Configuration:** The following example shows the enableCrossAppRedirects attribute set to true.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" enableCrossAppRedirects="true" />

</authentication>

...

</system.web>

**Secure Configuration:** Explicitly set the enableCrossAppRedirects attribute to false, or simply remove the insecure configuration. The default value for enableCrossAppRedirects is false.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" enableCrossAppRedirects="false" />

</authentication>

...

</system.web>

## Forms Authentication: Weak Cookie Protection

**Insecure Configuration:** The default value for the protection attribute is All. Setting the value to any of the options below weakens the authentication cookie protections.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" protection="None|Encryption|Validation" />

</authentication>

...

</system.web>

**Secure Configuration:** Explicitly set the protection attribute to All, or simply remove the insecure configuration.

<system.web>

...

<authentication mode="Forms">

<forms loginUrl="~/Account/Login.aspx" protection="All" />

</authentication>

...

</system.web>

*Vulnerable configuration:*

<configuration>

<system.web>

<trace enabled="true" localOnly="false">

*Secure configuration:*

<configuration>

<system.web>

<trace enabled="false" localOnly="true">

*Vulnerable configuration:*

<configuration>

<system.web>

<sessionState cookieless="UseUri">

*Secure configuration:*

<configuration>

<system.web>

<sessionState cookieless="UseCookies">

*Vulnerable configuration:*

<configuration>

<system.web>

<customErrors mode="Off">

*Secure configuration:*

<configuration>

<system.web>

<customErrors mode="RemoteOnly">

<customErrors mode="On" defaultRedirect="YourErrorPage.htm" />