**SQL Injection:**

To test enter below string in search box. It will drop UserData table. Below is given query to re-create table

Live';drop table UserData;--

CREATE TABLE [dbo].[UserData](

[UserId] [int] NOT NULL,

[Name] [varchar](50) NULL,

[Address] [varchar](500) NULL,

[EmailId] [varchar](100) NULL

) ON [PRIMARY]

GO

SET ANSI\_PADDING OFF

GO

INSERT [dbo].[UserData] ([UserId], [Name], [Address], [EmailId]) VALUES (1, N'John', N'Banglore', N'john@gmail.com')

INSERT [dbo].[UserData] ([UserId], [Name], [Address], [EmailId]) VALUES (2, N'Martin', N'Pune', N'martin@gmail.com')

**HttpForbiddenHandler:**

Exclude unnecessary unused file extension. In our example we have excluded xml file. But allowed csv file. Below URL can be used to verify the same..

Allowed

<http://localhost:26641//Data/UserData.csv>

Not Allowed

<http://localhost:26641/Data/UserData.xml>

This configuration need to be specified for all file extension required to be blocked.

<system.web>

<httpHandlers>

<add verb="\*" path="\*.xml" type="System.Web.HttpForbiddenHandler" />

</httpHandlers>

</system.web>

<system.webServer>

<handlers>

<add verb="\*" path="\*.xml" type="System.Web.HttpForbiddenHandler" name="XML"/>

</handlers>

</system.webServer>

The httpHandlers element is used on sites running on IIS 5 – 6, or IIS 7.x in Classic mode (IIS 6 compatibility mode). The handlers element is used on sites running on IIS 7.x (Integrated mode).

**Cross Site Scripting:**

In write Review text area enter below text and save it. After that whenever page get loaded it will execute script in below text and open new window.

This product is good.Checkout some more<script>window.open('http://www.w3schools.com/', '\_blank');</script>