[Web安全相关（四）：过多发布(Over Posting)](http://www.cnblogs.com/Erik_Xu/p/5497501.html)

**简介**

　　过多发布的内容相对比较简单，因此，我只打算把原文中的一些关键信息翻译一下。原文链接如下：

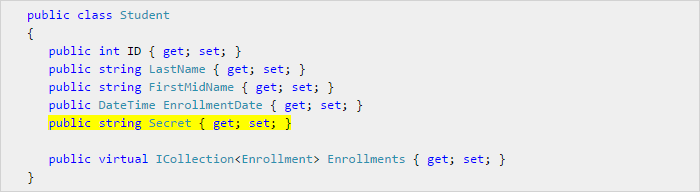
<http://www.asp.net/mvc/overview/getting-started/getting-started-with-ef-using-mvc/implementing-basic-crud-functionality-with-the-entity-framework-in-asp-net-mvc-application#overpost>

　　示例代码下载：

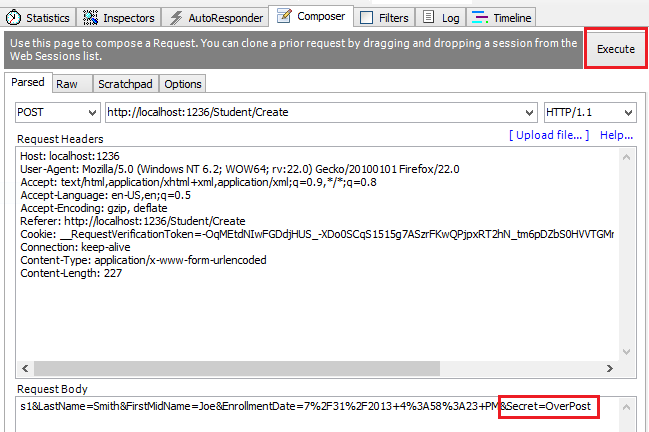
<https://code.msdn.microsoft.com/ASPNET-MVC-Application-b01a9fe8>

**分析**

　　假设有一个类Student，它用于和数据库建立映射，而且Student中的一个字段Secret你不想在页面上修改它的值。



　　即使界面上没有Secret对应的字段，hacker可以通过一些工具（如fildder）或者编写js去发送请求来修改Secret的值。



　　如上图，Secret的值会被修改为OverPost。

**防止**

　　在ASP.NET中，防止过多发布的方法大概有以下几种：

　　1. 使用BindAttribute中的Include属性，把需要映射的字段加到白名单。

　　public ActionResult Create([Bind(Include = "LastName, FirstMidName, EnrollmentDate")]Student student)

　　2. 使用BindAttribute中的Exclude属性，把不允许映射的字段加到黑名单。

　　public ActionResult Create([Bind(Exclude = "Secret")]Student student)

　　3. 使用TryUpdateModel方法，验证Model的时候，制定需要映射的字段。

　　if (TryUpdateModel(student, "", new string[] { "LastName", "FirstMidName", "EnrollmentDate" }))

　　{

　　}

　　4. 定义一个新的类作为输入参数

　  public class StudentForm

    {

         public string LastName { get; set; }

         public string FirstMidName { get; set; }

         public DateTime EnrollmentDate { get; set; }

    }