安全策略

1. 验证

Web安全处理的第一步便是“验证（Authentication）”，即对于请求信息的用户验证身份，用户使用其证件来表明身份。证件的种类各种各样，最常用的是用户名和密码。

ASP.NET验证是通过验证提供程序（Authentication Provider）来实现的，此提供程序是通过webconfig配置文件使用（Authentication）进行控制。

ASP.NET提供了三种验证用户的模式，每一种验证方法都是通过一个独立的验证提供程序来实现的。3种模式分别为windows、forms和Passport。Windows验证时通过IIS实现的；Forms验证是通过在开发人员自己的服务器上实现的；Passport验证是通过微软公司的订阅服务实现的。

1. 几种常见的验证方法

Web.config文件中可配置的身份验证方式有Windows、Forms、PassPort、None。

Web.config文件中<authentication>节点，身份验证方式取决于该节点“mode”属性的设置。  
**1．None**  
None表示不执行身份验证。  
**2．Windows**  
IIS根据应用程序的设置执行身份验证，其中包含匿名身份验证、NTLM身份验证、base64编码身份验证等。此外，NTFS在文件和目录上的权限（访问控制列表）将决定对目录中资源的访问。  
**3．Forms**  
编程者创建一个用于登录的WEB窗体，然后在应用程序中用于验证所有浏览用户的身份。用户第一次访问程序中任何窗体都将被重定向到这个登录窗体，当用户登录成功后，其登录信息被存储在Cookie中，并转向所访问过的其他窗体。  
**4．Passport**  
Passport身份验证是通过Microsoft的集中身份验证服务执行的，它为成员站点提供单独登录和核心配置文件服务。

默认情况下，Web.config文件中<authentication>节点采用Windows身份验证。如果需要使用Forms验证方式，并指定登录窗体为项目根目录下的Login.aspx，修改<authentication>节点如以下代码所示。  
<authentication mode="Forms">  
<forms loginUrl="lg.aspx" name=".cookiename"></forms>  
</authentication>  
<authorization>  
<deny users="?" />  
</authorization>  
在<authentication>节点下添加<forms>子节点即可设置Forms验证的各种细节，如“loginUrl”用于指定登录页面路径，“name”属性用于指定登录信息所存储Cookie的名称。为了使验证生效，必须配合<authorization>节点一起设置，在该节点下添加<deny>子节点，通过“users”属性设置拒绝所有非法用户。

1. 通配符\*在<allow>或<deny>中表示允许或拒绝任何人访问

②通配符?在<allow>中表示拒绝未授权的用户访问(允许匿名用户访问)，在<deny>中表示允许匿名用户访问（拒绝未授权的用户访问）

首先，在应用程序的配置文件(web.config)中配置程序。具体如下：   
    配置authentication 节点，表示使用Forms验证模式，forms 节点的具体意义大家可以上网搜搜  
    <authentication mode="Forms">   
      <forms name=".user" loginUrl="Login.aspx" timeout="1" />   
    </authentication>    
     配置authorization节点，拒绝匿名访问   
    <authorization>   
        <deny users="?" />    
    </authorization>   
然后，可以在Login.aspx页面和数据库连接起来验证用户，我用的方法是：   
    if (ValidateLogin(uid,pwd))     //此方法根据传过去的uid，pwd查找数据库中的记录，如有返回true   
    {   
        FormsAuthentication.SetAuthCookie(uid, false);     
         //设置Cookie，也可以用RedirectFromLoginPage（uid，false）直接到默认页面   
        Response.Redirect("index.aspx");    //重定向   
    }   
这样，如果用户未经验证，想访问受限资源，就会被定向到login.aspx页面。

说明：ASP.NET应用程序下每个子目录都可以有继承于根目录配置文件的Web.config文件，但一个应用程序只能有一个身份验证登录页面，即以上代码中<forms>子节点“loginUrl”属性所指定的页面。如果在子目录的Web.config文件中出现了<authentication>节点的配置，程序将出错，除非将此目录配置为虚拟目录进行访问。