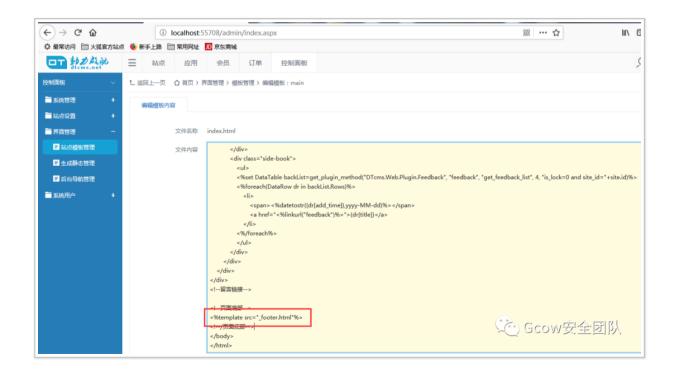
代码审计之 DTCMS V5.0 后台漏洞两枚

漏洞一 后台文件读取漏洞

漏洞一 后台文件读取漏洞

漏洞分析: 该漏洞主要是由于模板引擎解析未过滤导致的。

登录后台 - 模板管理 - 编辑模板



模板文件相互引用是十分常见的,这里我们可否将模板文件引用改为其他关键文件呢?

譬如: web.config



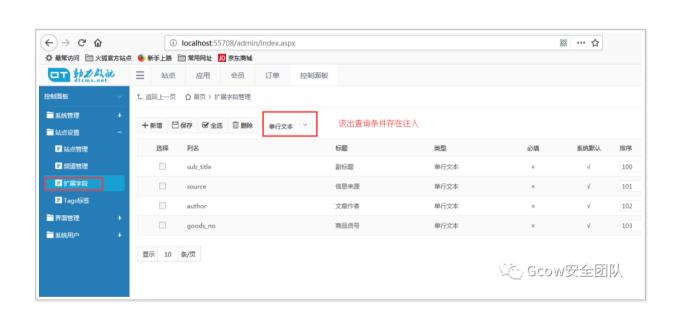
修改完成后, 生成页面。我们查看下前台页面的情况

```
< → C ↔
                           i view-source:http://localhost:55708/index.aspx
                                                                                                                        ... ☆
☆ 最常访问 🗎 火狐官方站点 🌑 新手上路 🗎 常用网址 🔟 京东商城
   <?xml version="1.0" encoding="utf-8"?>
877 <configuration>
     <!-- appSettings网站信息配置-->
     <appSettings>
      <add key="Configpath" value="~/xmlconfig/sys.config" />
       <add key="Urlspath" value="~/xmlconfig/urls.config" />
       <add key="Userpath" value="~/xmlconfig/user.config" />
       <add key="Orderpath" value="~/xmlconfig/order.config" />
     </appSettings>
      <!-- 数据库连接字符串-
     <connectionStrings>
       <add name="ConnectionString" connectionString="server=.;uid=sa;pwd=2100206;database=DTcmsdb5;" />
      </connectionStrings>
      (system. web)
       <compilation debug="true" targetFramework="4.0" />
       <customErrors mode="0ff"/>
       <httpModules>
         <add type="DTcms.Web.UI.HttpModule, DTcms.Web.UI" name="HttpModule" />
       </http///dules>
       <httpHandlers>
         <add verb="*" path="templates/main/*.html" type="System.Web.HttpForbiddenHandler" />
       </httpHandlers>
       <!-- 文件上传大小KB-->
       <a href="httpRuntime">httpRuntime</a> requestValidationMode="2.0" maxRequestLength="2097151" executionTimeout="36000" />
      </system.web>
      <system.webServer>
       <validation validateIntegratedModeConfiguration="false"/>
       <modules runAllManagedModulesForAllRequests="true">
                                                                                                       Cow安全团队
         <add type="DTcms.Web.UI.HttpModule, DTcms.Web.UI" name="HttpModule" />
       </modules>
        (cocurity)
```

数据库关键信息都读取出来了,同理可以查看其他重要文件。

漏洞二 SQL 注入漏洞

在审计源代码的时候发现了这一处。



我们查找下源代码:

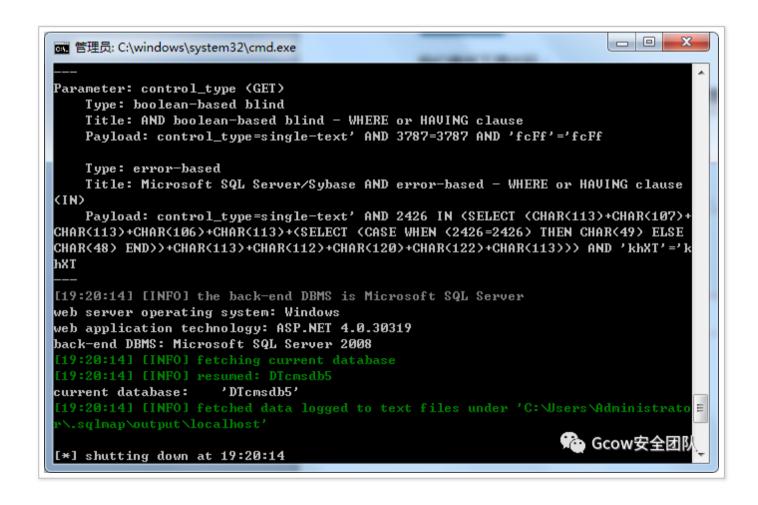
- 1 7 1 WOLL WESTERNIS (2007) 200 (C. 100)

```
解决方案资源管理器
Web.config DTRequest.cs attribute_field_list.aspx.cs × attribute_field_list.aspx article_attribute_field.cs
                                                                                                                                        🛅 😭 👩 🛭 🗃 🙈 🛙
SDTcms.Web.admin.channel.attribute_field_list
                                                                 → Page_Load(object sender, EventArgs e)
                                                                                                                                         DTcms.Common
           protected string control_type = string.Empty;
                                                                                                                                         DTcms.DAL
          protected string keywords = string. Empty;
                                                                                                                                        DTcms.DBUtility
           protected void Page_Load(object sender, EventArgs e)
                                                                                                                                       DTcms.Model
                                                                                                                                       this.control_type = DTRequest.GetQueryString("control_type"); 直接读取的参数
                                                                                                                                         ▶ ■ Properties
              this.keywords = DTRequest.GetQueryString("keywords");
                                                                                                                                         ▷ 🔄 引用
              this.pageSize = GetPageSize(10); //每页数里
                                                                                                                                         a admin
              if (!Page.IsPostBack)
                                                                                                                                            image: a channel
                  ChkAdminLevel("sys_channel_field", DTEnums.ActionEnum.View.ToString()): //检查权限
                                                                                                                                              attribute_fi
                  RptBind("id')0" + CombSqlTxt(this.control_type, this.keywords), "is_sys desc, sort_id asc, id desc");
                                                                                                                                              attribut
```

```
b E channel ec
b E channel lis
protected string CombSqlTxt(string _control_type, string _keywords)
                                                                                                                             StringBuilder strTemp = new StringBuilder();
                                                                                                                             b ☐ tags edit.a
   if (|string.IsNullOrEmpty(_control_type))
                                                                                                                             tags_list.as
      strTemp. Append(" and control_type='" + _control_type + __); control_type忘记过滤了吗?
                                                                                                                          ⊳ 🚞 js
   _keywords = _keywords.Replace("'", "");

if (!string.IsNullUrbmpty( keywords))
                                       对 kevwords 进行了过滤
                                                                                                                          ▶ manage
                                                                                                                          order
       strTemp.Append(" and (name like '%" + _keywords + "%" or title like '%" + _keywords + "%")");
                                                                                                                          settings
                                                                                                                          return strTemp. ToString();
                                                                                                                             ie6update.htm
```

果然,应该是忘记过滤了,直接上 SQLMAP 测试下:布尔的盲注



本文简短,简单明了,适人群广泛