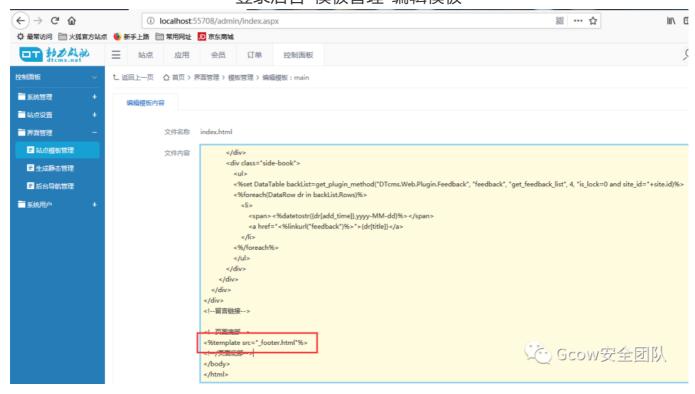
## 代码审计之DTCMS V5.0后台漏洞两枚

原创 复眼小组 Gcow安全团队 前天

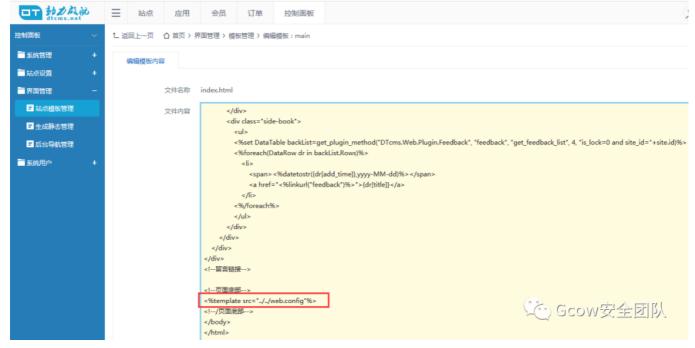
## 漏洞一 后台文件读取漏洞

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?





修改完成后, 生成页面。我们查看下前台页面的情况

```
(-) → C 0
                                  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
                       "1.0" encoding="utf-8"?>
     <?xml version=</pre>
     <configuration>
         !-- appSettings网站信息配置-->
       <appSettings>
         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" />
<add key="Orderpath" value="~/xmlconfig/order.config" /></a>
       </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" />
         </httpModules>
         <httpHandlers>
<add verb="*" path="templates/main/*.html" type="System.Web.HttpForbiddenHandler" />
         </httpHandlers>
          <!-- 文件上传大小KB-->
         httpRuntime requestValidationMode="2.0" maxRequestLength="2097151" executionTimeout="36000" />
       </system.web>
          <validation validateIntegratedModeConfiguration="false"/>
         (企) Grow安全团队
         </modules>
```

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。



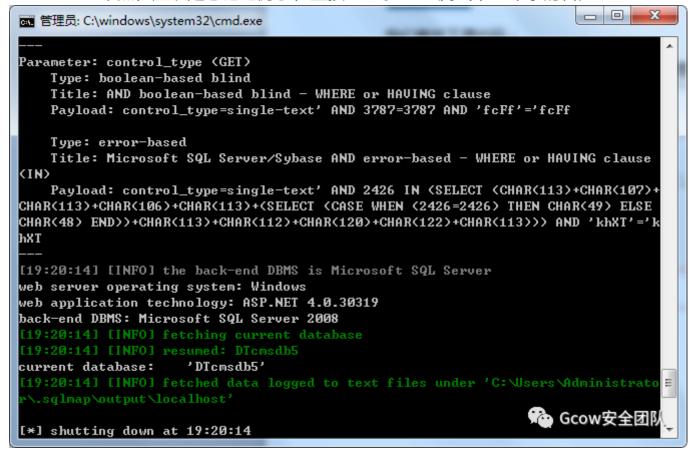
我们查找下源代码:

```
attribute_field_list.aspx.cs × attribute_field_list.aspx
                                                                                                                                                     解决方案资源管理器
                                                                                                                                                      🛅 👔 🗗 🖫 📆 👔
🕏 DTcms.Web.admin.channel.attribute_field_list
                                                                       ▼ Page_Load(object sender, EventArgs e)
                                                                                                                                                        DTcms.Commo
           protected string control_type = string.Empty;
protected string keywords = string.Empty;
                                                                                                                                                        DTcms.DAL
                                                                                                                                                        DTcms.DBUtility
           protected void Page_Load(object sender, EventArgs e)
                                                                                                                                                        DTcms.Model
                                                                                                                                                     DTcms.Web
               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
                                                                                                                                                        admin
               if (!Page.IsPostBack)

■ Channel

                   ChkàdminLevel("sys_channel_field", DTEnums.åctionEnum.View.ToString()): //檢查权限
RptBind("id')0" + CombSqlTxt(this.control_type, this.keywords), "is_sys desc,sort_id asc,id desc"):
                                                                                                                                                                attribute fi
                                                                                                                                                              a attribute fi
           }
                                                                                                                                                                   attribut
                                                                                                                                                                   attribut
           数据绑定======
                                                                                                                                                             channel_ec
           #region 组合SQL查询语句============
                                                                                                                                                             protected string CombSqlTxt(string _control_type, string _keywords)
                                                                                                                                                             site list.ası
               StringBuilder strTemp = new StringBuilder();
if (!string.IsNullOrEmpty(_control_type))
                                                                                                                                                             tags_edit.a
                                                                                                                                                                tags_list.as
                   strTemp.Append(" and control_type='" + _control_type + __); control_type忘记过滤了吗?
                                                                                                                                                           ,
_keywords = _keywords.Replace("", "");
ri (!string.IsNullUrEmpty(_keywords))
                                                                                                                                                          b 🛅 js
                                                                                                                                                          manager
                                                                                                                                                           ▶ i order
                   strTemp.Append(" and (name like '%" + _keywords + "%" or title like '%" + _keywords + "%')");
                                                                                                                                                           settings
                                                                                                                                                             i skin
                                                                                                                                  COW安全景景。
               return strTemp. ToString();
           #endregion
                                                                                                                                                              ■ 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 更多技术文章 请关注公众号

Gcow安全团队

仅供学习,违法必究!

Gcow安全团队致力于网络安全发展 开设有免费公开课

B站搜索: Gcow安全团队

即可观看往期公开课视频!