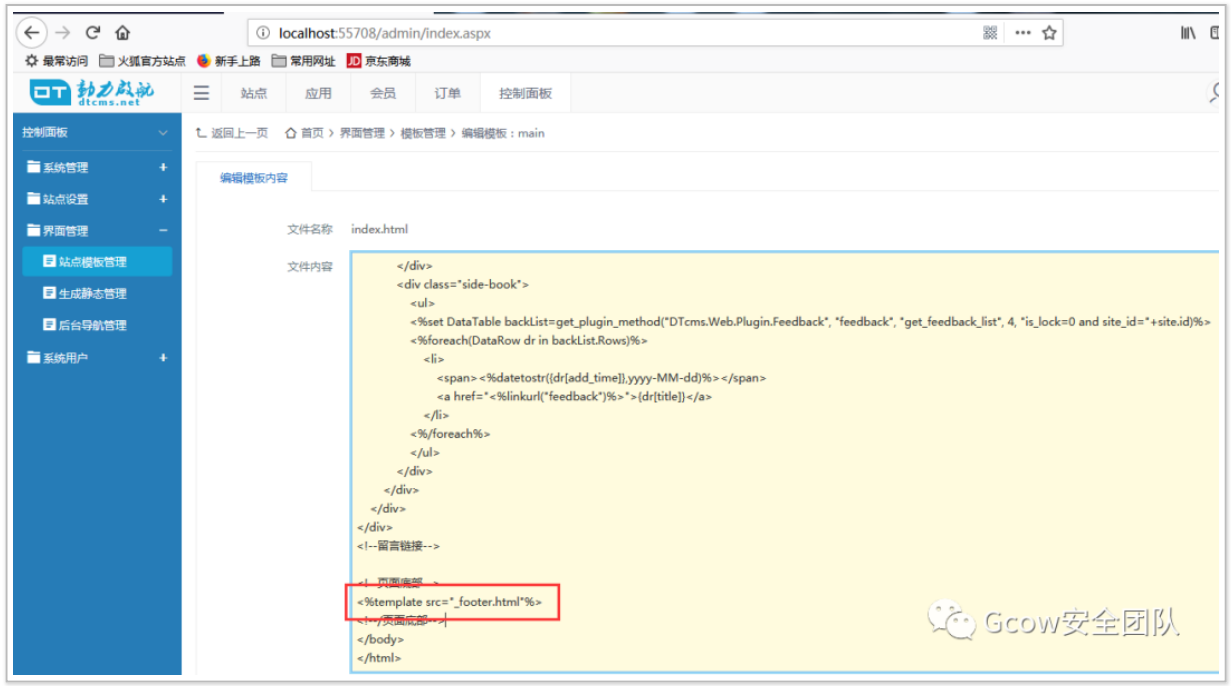
代码审计之 DTCMS V5.0 后台漏洞两枚

> 漏洞一 后台文件读取漏洞

漏洞一 后台文件读取漏洞

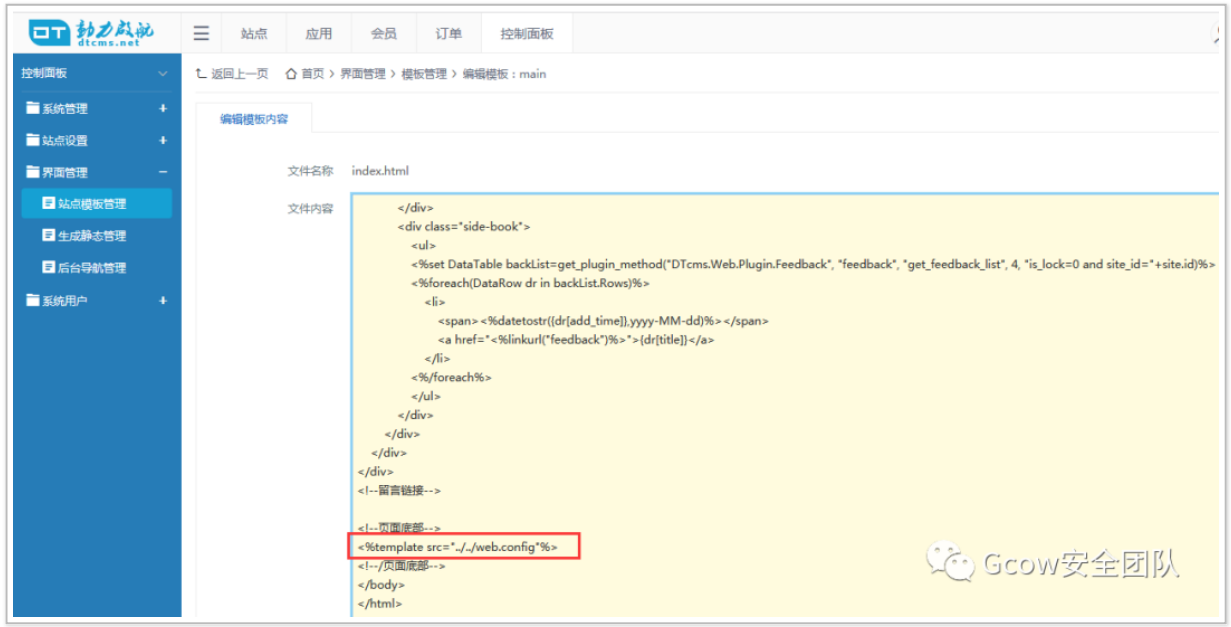
漏洞分析：该漏洞主要是由于模板引擎解析未过滤导致的。

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

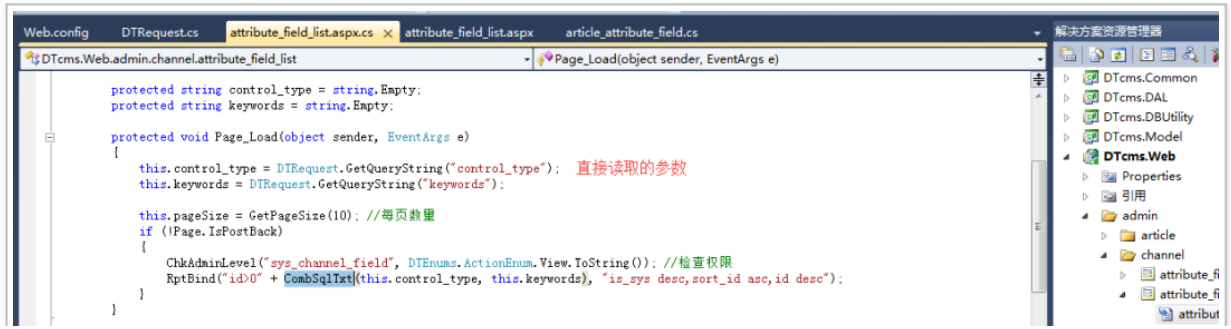
数据库关键信息都读取出来了，同理可以查看其他重要文件。

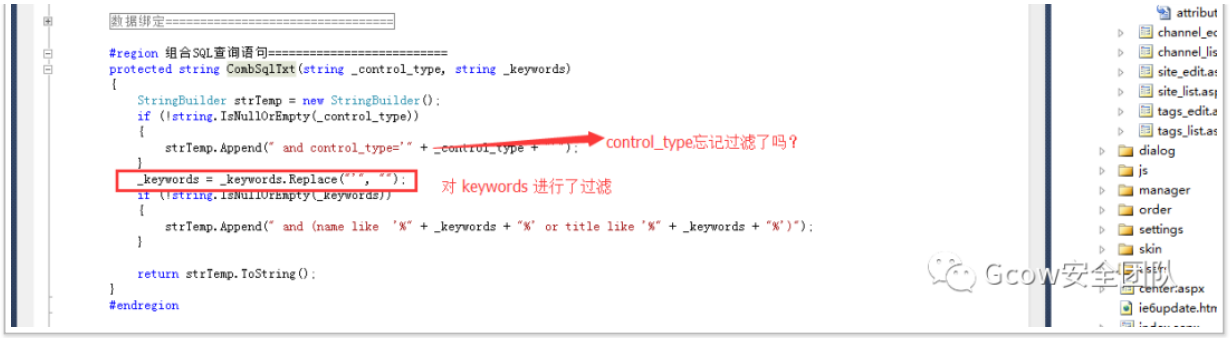
漏洞二 SQL 注入漏洞

在审计源代码的时候发现了这一处。

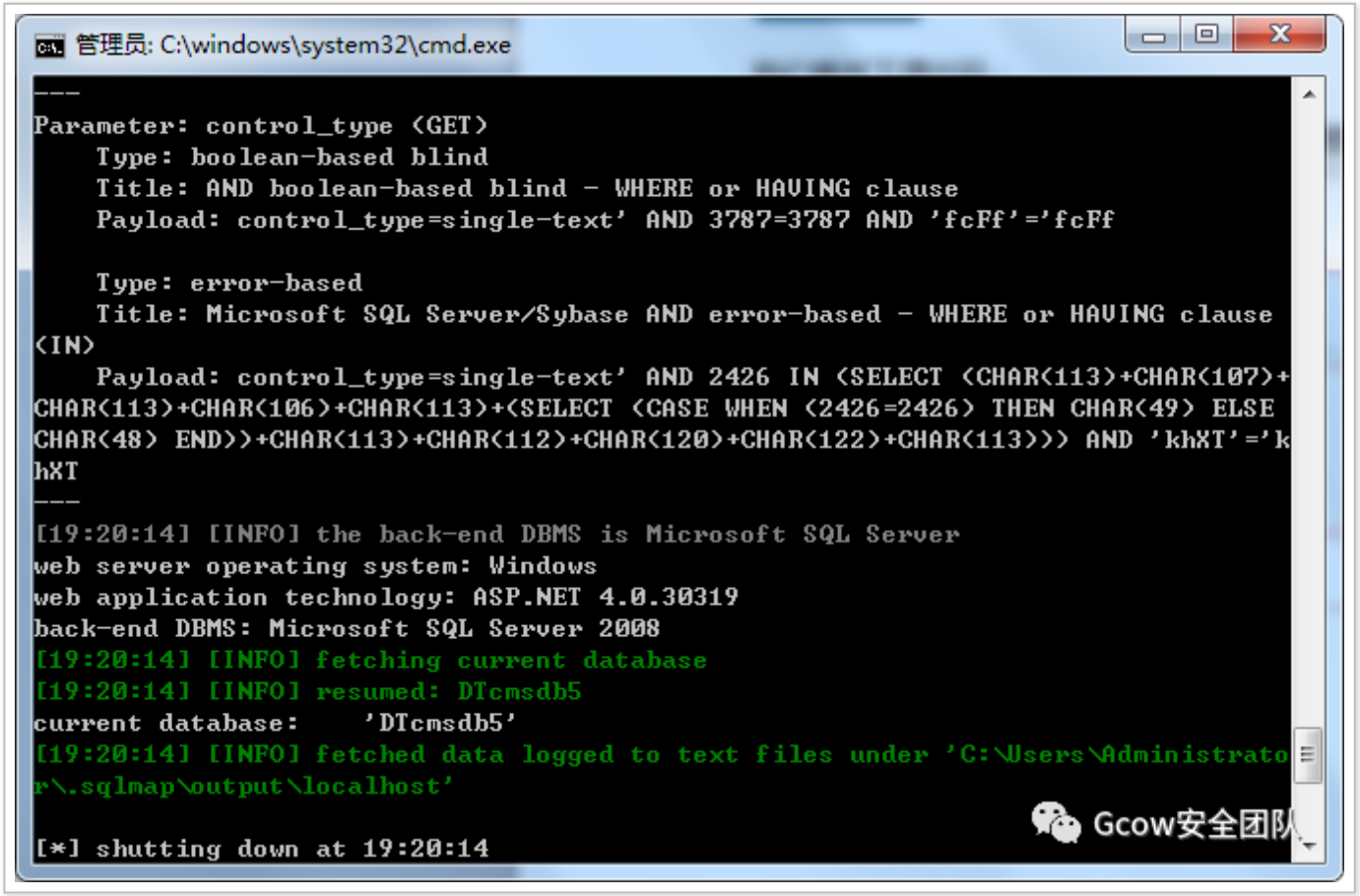

localhost:55708/admin/index.aspx
站点
应用
会员
订单
控制面板
控制面板
系统管理
站点设置
站点管理
频道管理
扩展字段
Tags标签
界面管理
系统用户
返回上一页
首页 › 扩展字段管理
+新增
保存
全选
删除
单行文本
该出查询条件存在注入
选择
列名
标题
类型
必填
系统默认
排序
sub_title
副标题
单行文本
source
信息来源
单行文本
author
文章作者
单行文本
goods_no
商品货号
单行文本
显示
10
条/页
Gcow安全团队

我们查找下源代码：


Web.config
DTRequest.cs
attribute_field_list.aspx.cs
attribute_field_list.aspx
article_attribute_field.cs
DTcms.Web.admin.channel.attribute_field_list
Page_Load(object sender, EventArgs e)
protected string control_type = string.Empty;
protected string keywords = string.Empty;
protected void Page_Load(object sender, EventArgs e)
{
this.control_type = DTRequest.GetQueryString("control_type");
直接读取的参数
this.keywords = DTRequest.GetQueryString("keywords");
this.pageSize = GetPageSize(10); //每页数量
if (!Page.IsPostBack)
{
ChkAdminLevel("sys_channel_field", DTEnums.ActionEnum.View.ToString()); //检查权限
RptBind("id>0" + CombSqlTxt(this.control_type, this.keywords), "is_sys desc,sort_id asc,id desc");
}
}
解决方案资源管理器
DTcms.Common
DTcms.DAL
DTcms.DBUtility
DTcms.Model
DTcms.Web
Properties
引用
admin
article
channel
attribute_fi
attribute_fi
attribut



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

/