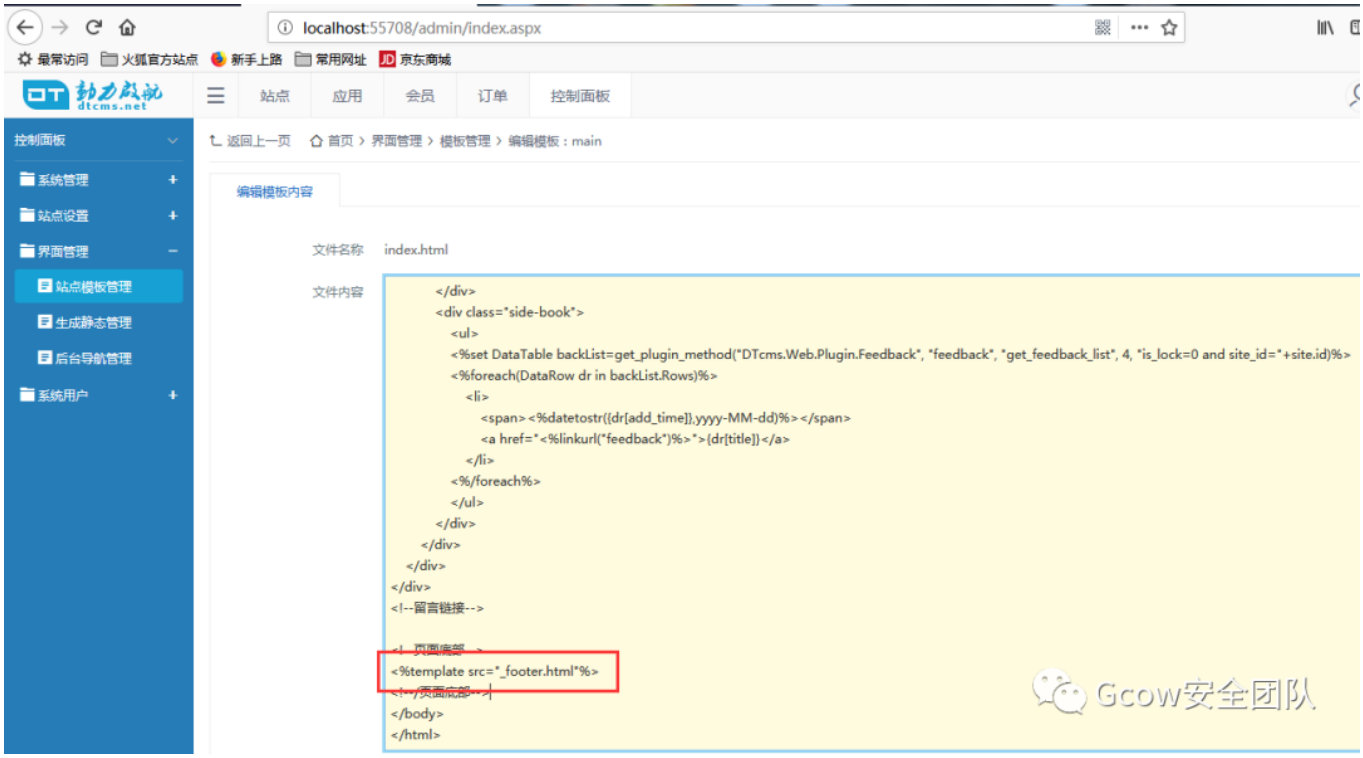
代码审计之DTCMS V5.0后台漏洞两枚

原创 复眼小组 Gcow安全团队 前天

漏洞一 后台文件读取漏洞

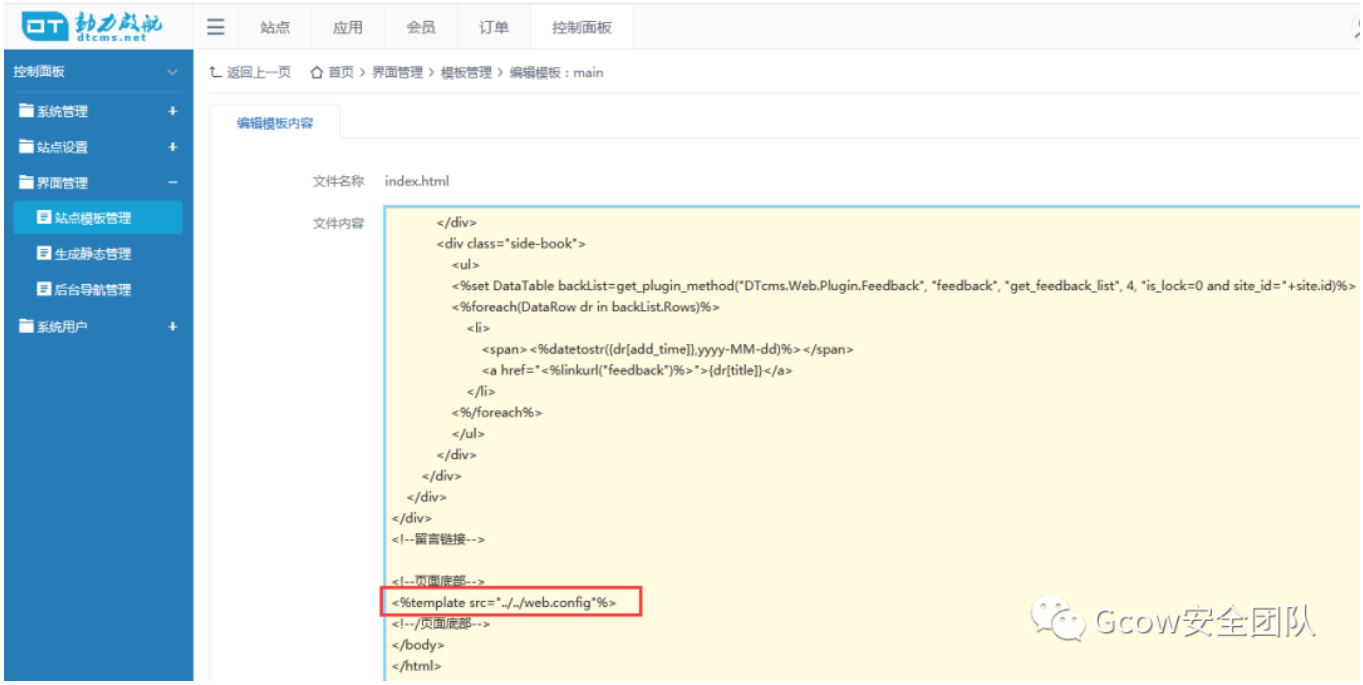
漏洞分析：该漏洞主要是由于模板引擎解析未过滤导致的。

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



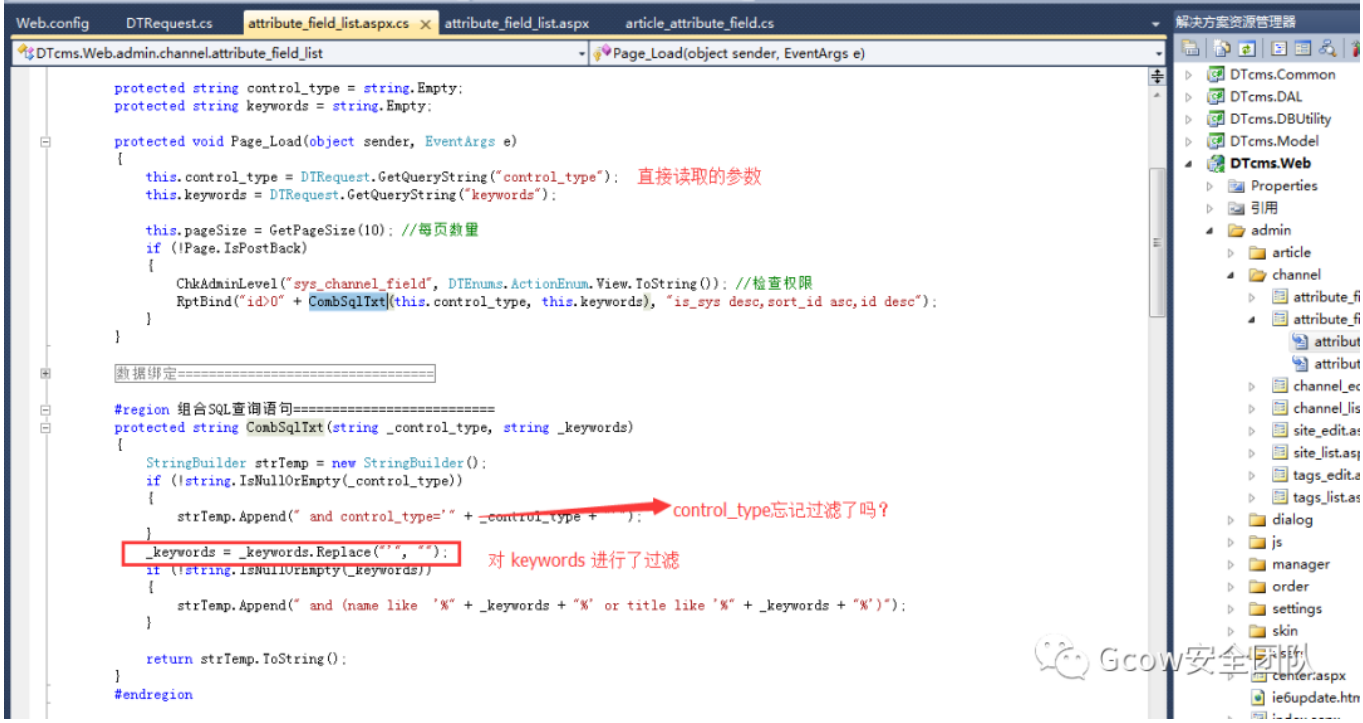
修改完成后，生成页面。我们查看下前台页面的情况

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。

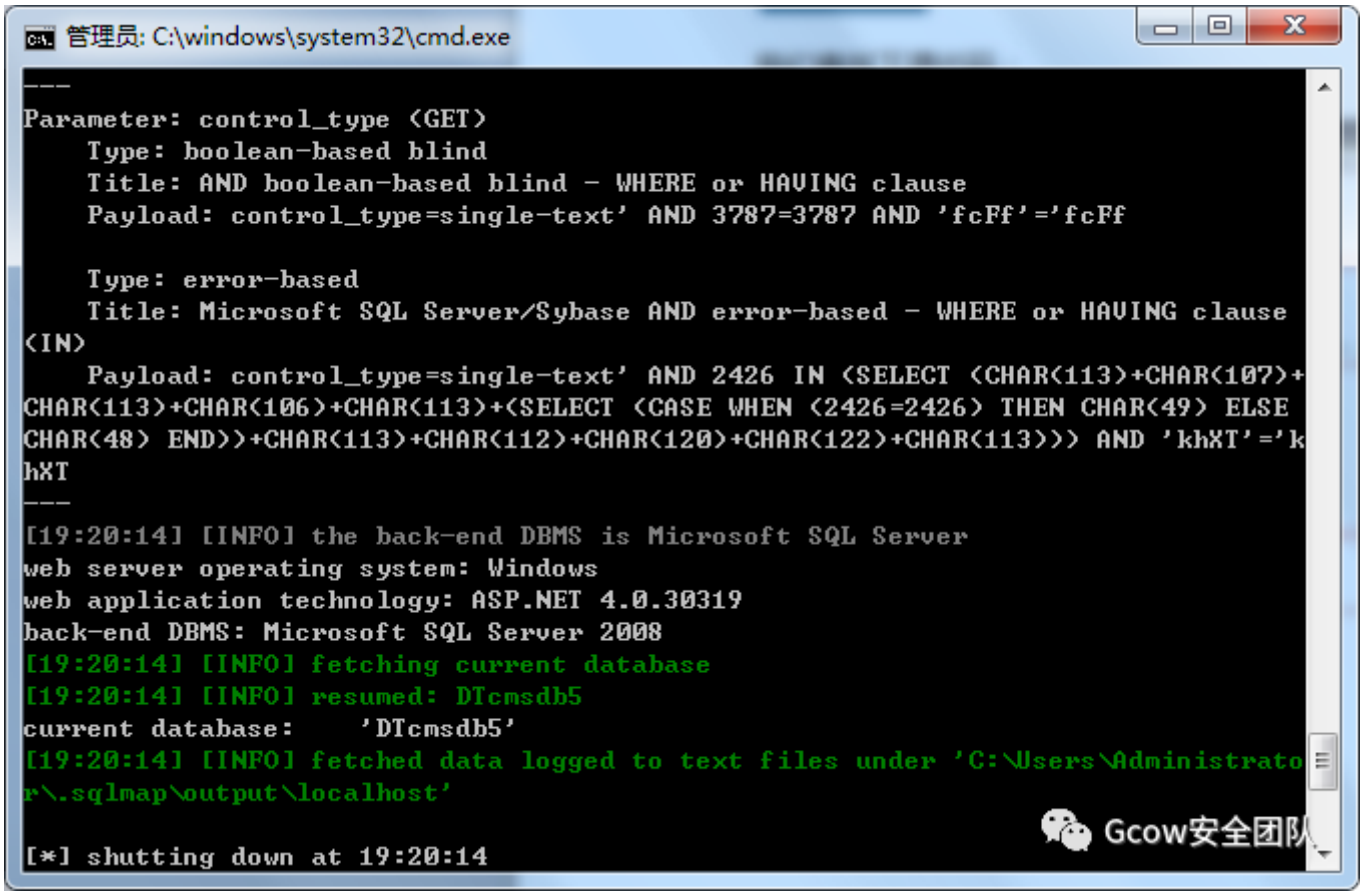
漏洞二 SQL注入漏洞

在审计源代码的时候发现了这一处。

我们查找下源代码：



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！