New issue　　Jump to bottom

这里有几处没有换成预编译，但个人建议修复 #4127

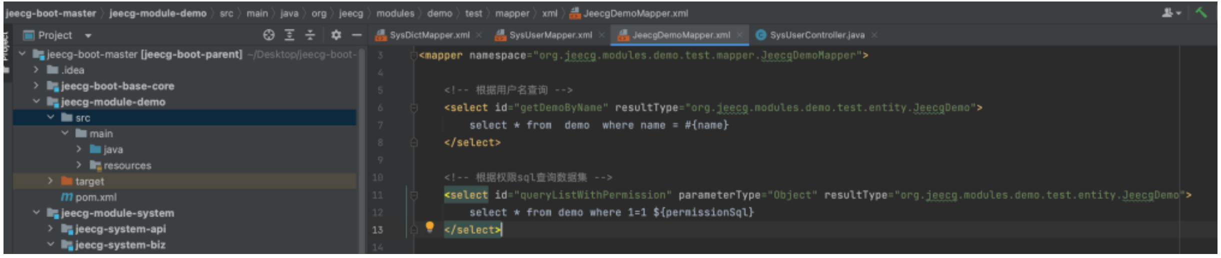
Closed　**azraelxuemo** opened this issue on Oct 25 · 6 comments

azraelxuemo commented on Oct 25 • edited

java提供了原生的预编译sql语句，这样可以防止sql注入问题

queryListWithPermission

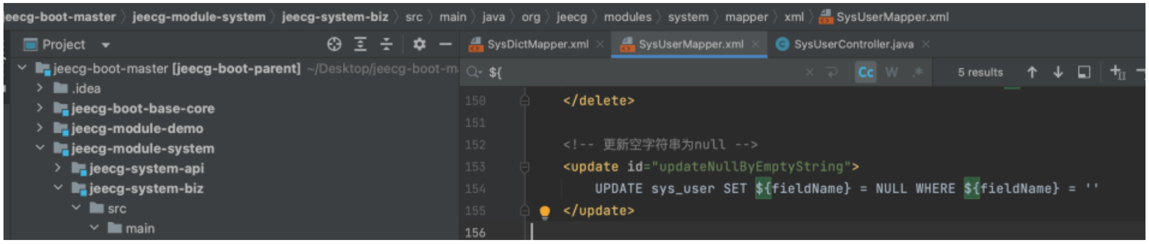
下图没有进行预编译处理，建议换成#{},虽然项目现在没有使用这条语句，但不排除以后的可能，建议修复



```
<mapper namespace="org.jeecg.modules.demo.test.mapper.JeecgDemoMapper">

    <!-- 根据用户名查询 -->
    <select id="getDemoByName" resultType="org.jeecg.modules.demo.test.entity.JeecgDemo">
        select * from  demo  where name = #{name}
    </select>

    <!-- 根据权限sql查询数据集 -->
    <select id="queryListWithPermission" parameterType="Object" resultType="org.jeecg.modules.demo.test.entity.JeecgDemo">
        select * from demo where 1=1 ${permissionSql}
    </select>
```

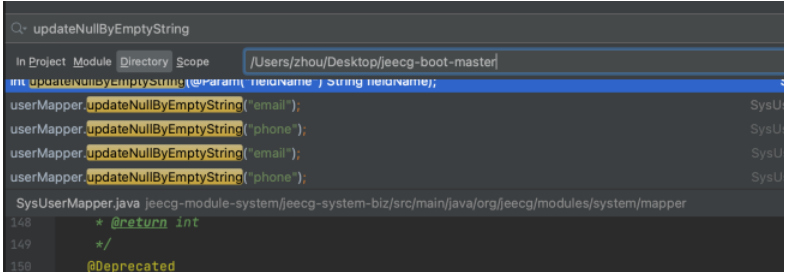
updateNullByEmptyString

下图也使用的是${}


eecg-boot-master 〉 jeecg-module-system 〉 jeecg-system-biz 〉 src 〉 main 〉 java 〉 org 〉 jeecg 〉 modules 〉 system 〉 mapper 〉 xml 〉 SysUserMapper.xml
Project
SysDictMapper.xml
SysUserMapper.xml
SysUserController.java
${
Cc W .*
5 results
jeecg-boot-master [jeecg-boot-parent] ~/Desktop/jeecg-boot-m
.idea
jeecg-boot-base-core
jeecg-module-demo
jeecg-module-system
jeecg-system-api
jeecg-system-biz
src
main

```
    </delete>

    <!-- 更新空字符串为null -->
    <update id="updateNullByEmptyString">
        UPDATE sys_user SET ${fieldName} = NULL WHERE ${fieldName} = ''
    </update>
```

但实际上是写死的，但为了安全考虑，建议也换乘#{}

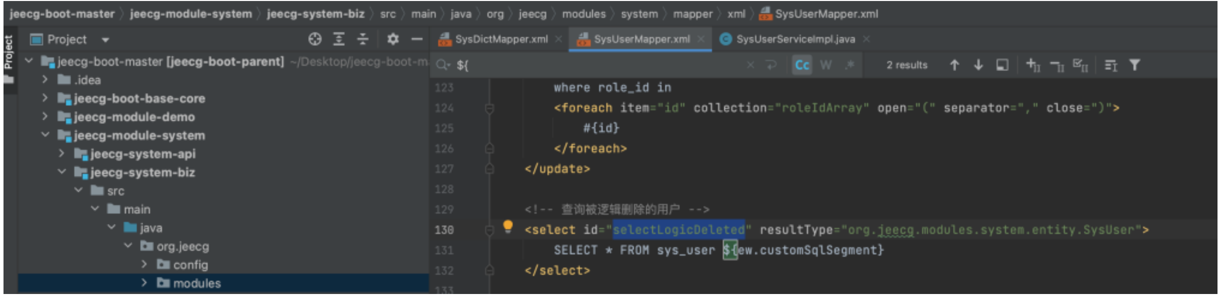

updateNullByEmptyString
In Project　Module　Directory　Scope
/Users/zhou/Desktop/jeecg-boot-master
SysU
SysU
SysU
SysU
SysUserMapper.java jeecg-module-system/jeecg-system-biz/src/main/java/org/jeecg/modules/system/mapper

```
int updateNullByEmptyString(@Param("fieldName") String fieldName);
userMapper.updateNullByEmptyString("email");
userMapper.updateNullByEmptyString("phone");
userMapper.updateNullByEmptyString("email");
userMapper.updateNullByEmptyString("phone");
```

```
     * @return int
     */
    @Deprecated
```

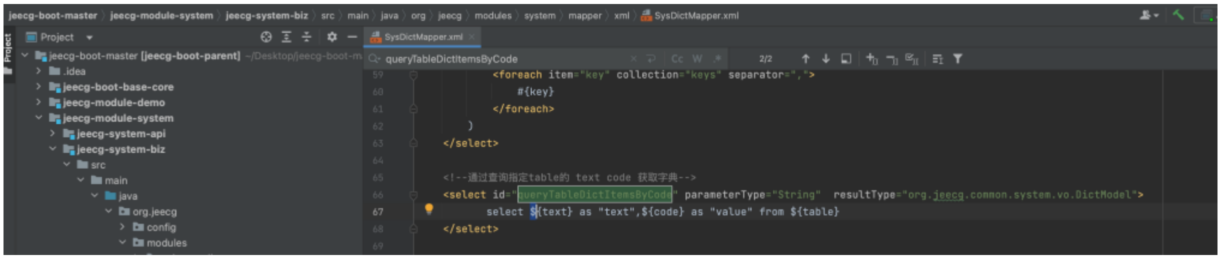
selectLogicDeleted

这里也建议换乘#{}



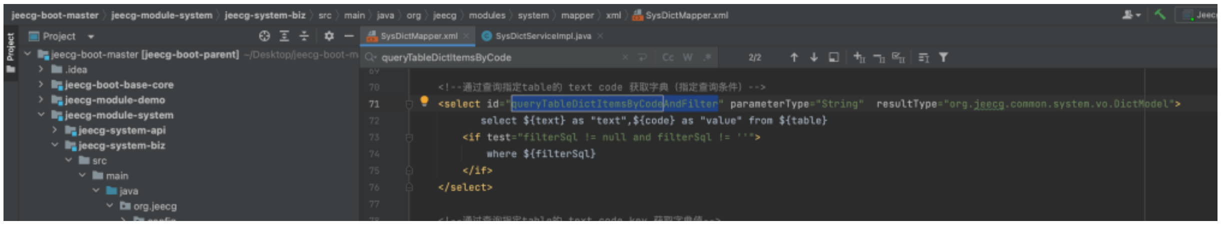
```
        where role_id in
        <foreach item="id" collection="roleIdArray" open="(" separator="," close=")">
            #{id}
        </foreach>
    </update>

    <!-- 查询被逻辑删除的用户 -->
    <select id="selectLogicDeleted" resultType="org.jeecg.modules.system.entity.SysUser">
        SELECT * FROM sys_user ${ew.customSqlSegment}
    </select>
```

queryFilterTableDictInfo


jeecg-boot-master 〉 jeecg-module-system 〉 jeecg-system-biz 〉 src 〉 main 〉 java 〉 org 〉 jeecg 〉 modules 〉 system 〉 mapper 〉 xml 〉 SysDictMapper.xml
Project
jeecg-boot-master [jeecg-boot-parent] ~/Desktop/jeecg-boot-m
.idea
jeecg-boot-base-core
jeecg-module-demo
jeecg-module-system
jeecg-system-api
jeecg-system-biz
src
main
java
org.jeecg
config
modules
SysDictMapper.xml
queryTableDictItemsByCode
2/2

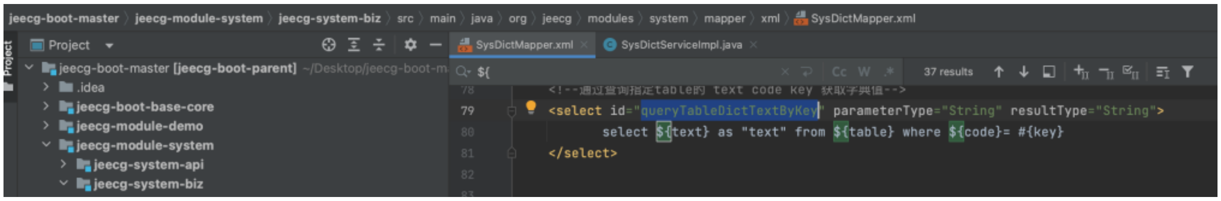
```xml
            <foreach item="key" collection="keys" separator=",">
                #{key}
            </foreach>
        )
    </select>

    <!--通过查询指定table的 text code 获取字典-->
    <select id="queryTableDictItemsByCode" parameterType="String"  resultType="org.jeecg.common.system.vo.DictModel">
           select ${text} as "text",${code} as "value" from ${table}
    </select>
```

queryTableDictItemsByCodeAndFilter


jeecg-boot-master 〉 jeecg-module-system 〉 jeecg-system-biz 〉 src 〉 main 〉 java 〉 org 〉 jeecg 〉 modules 〉 system 〉 mapper 〉 xml 〉 SysDictMapper.xml
Project
jeecg-boot-master [jeecg-boot-parent] ~/Desktop/jeecg-boot-m
.idea
jeecg-boot-base-core
jeecg-module-demo
jeecg-module-system
jeecg-system-api
jeecg-system-biz
src
main
java
org.jeecg
SysDictMapper.xml
SysDictServiceImpl.java
queryTableDictItemsByCode
2/2

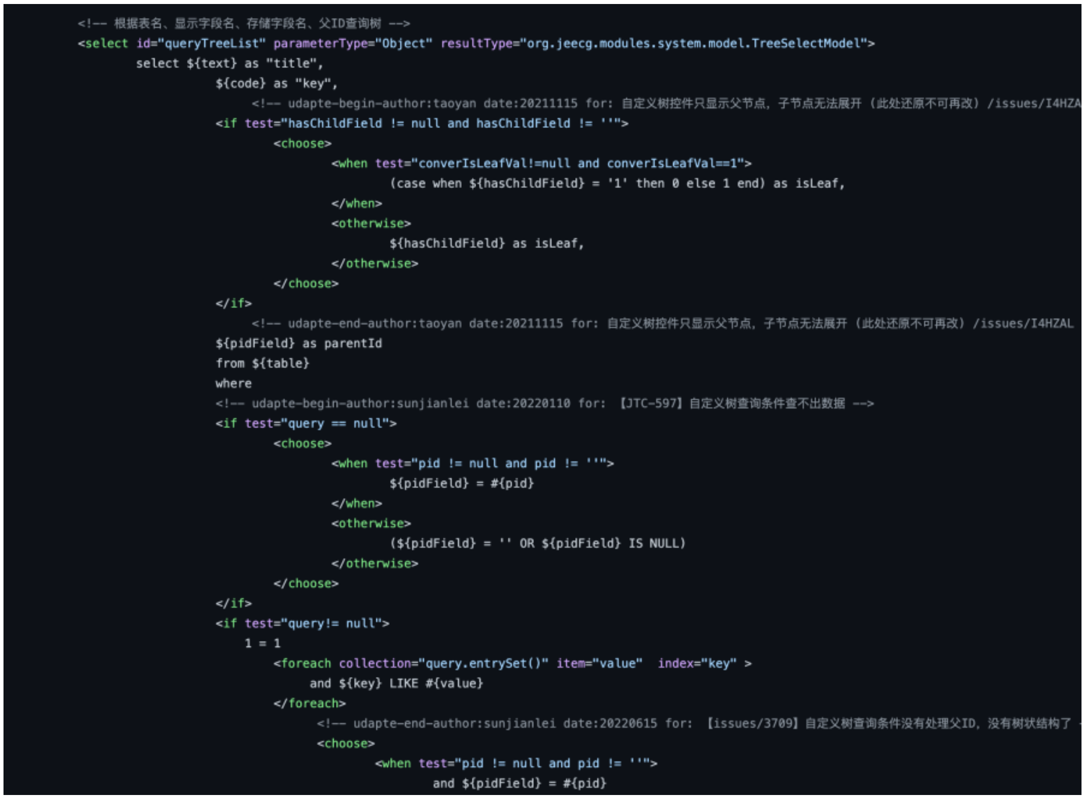
```xml
    <!--通过查询指定table的 text code 获取字典（指定查询条件）-->
    <select id="queryTableDictItemsByCodeAndFilter" parameterType="String"  resultType="org.jeecg.common.system.vo.DictModel">
           select ${text} as "text",${code} as "value" from ${table}
        <if test="filterSql != null and filterSql != ''">
            where ${filterSql}
        </if>
    </select>
```

queryTableDictTextByKey


jeecg-boot-master 〉 jeecg-module-system 〉 jeecg-system-biz 〉 src 〉 main 〉 java 〉 org 〉 jeecg 〉 modules 〉 system 〉 mapper 〉 xml 〉 SysDictMapper.xml
Project
jeecg-boot-master [jeecg-boot-parent] ~/Desktop/jeecg-boot-m
.idea
jeecg-boot-base-core
jeecg-module-demo
jeecg-module-system
jeecg-system-api
jeecg-system-biz
SysDictMapper.xml
SysDictServiceImpl.java
${
37 results

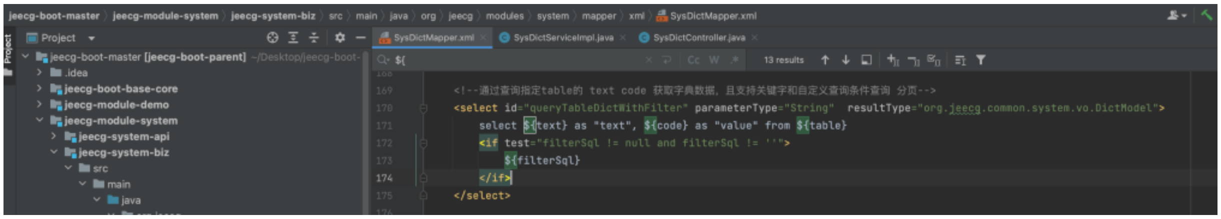
```xml
    <!--通过查询指定table的 text code key 获取字典值-->
    <select id="queryTableDictTextByKey" parameterType="String" resultType="String">
           select ${text} as "text" from ${table} where ${code}= #{key}
    </select>
```

queryTreeList



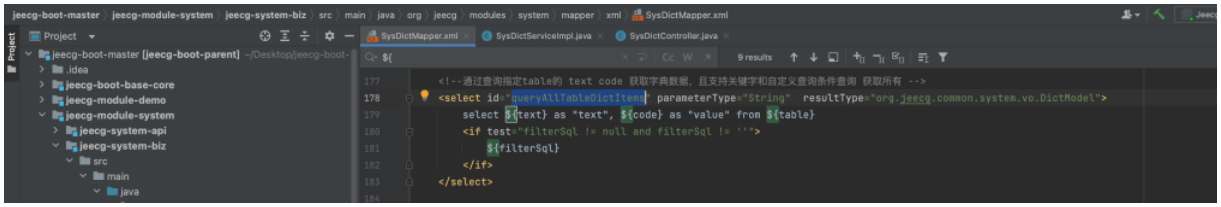
```xml
    <!-- 根据表名、显示字段名、存储字段名、父ID查询树 -->
    <select id="queryTreeList" parameterType="Object" resultType="org.jeecg.modules.system.model.TreeSelectModel">
        select ${text} as "title",
               ${code} as "key",
                 <!-- udapte-begin-author:taoyan date:20211115 for: 自定义树控件只显示父节点，子节点无法展开 （此处还原不可再改） /issues/I4HZA
               <if test="hasChildField != null and hasChildField != ''">
                   <choose>
                       <when test="converIsLeafVal!=null and converIsLeafVal==1">
                           (case when ${hasChildField} = '1' then 0 else 1 end) as isLeaf,
                       </when>
                       <otherwise>
                           ${hasChildField} as isLeaf,
                       </otherwise>
                   </choose>
               </if>
                 <!-- udapte-end-author:taoyan date:20211115 for: 自定义树控件只显示父节点，子节点无法展开 （此处还原不可再改） /issues/I4HZAL
               ${pidField} as parentId
               from ${table}
               where
               <!-- udapte-begin-author:sunjianlei date:20220110 for: 【JTC-597】自定义树查询条件查不出数据 -->
               <if test="query == null">
                   <choose>
                       <when test="pid != null and pid != ''">
                           ${pidField} = #{pid}
                       </when>
                       <otherwise>
                           (${pidField} = '' OR ${pidField} IS NULL)
                       </otherwise>
                   </choose>
               </if>
               <if test="query!= null">
                 1 = 1
                   <foreach collection="query.entrySet()" item="value"  index="key" >
                        and ${key} LIKE #{value}
                   </foreach>
                      <!-- udapte-end-author:sunjianlei date:20220615 for: 【issues/3709】自定义树查询条件没有处理父ID，没有树状结构了
                      <choose>
                          <when test="pid != null and pid != ''">
                              and ${pidField} = #{pid}
```

queryTableDictWithFilter



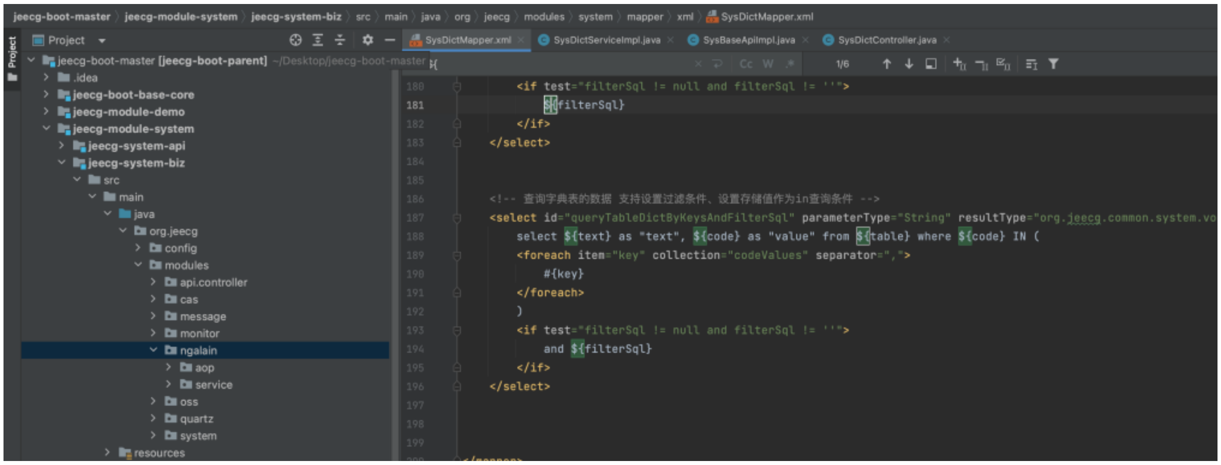
```
<!--通过查询指定table的 text code 获取字典数据，且支持关键字和自定义查询条件查询 分页-->
<select id="queryTableDictWithFilter" parameterType="String"  resultType="org.jeecg.common.system.vo.DictModel">
    select ${text} as "text", ${code} as "value" from ${table}
    <if test="filterSql != null and filterSql != ''">
        ${filterSql}
    </if>
</select>
```

queryAllTableDictItems



```
<!--通过查询指定table的 text code 获取字典数据，且支持关键字和自定义查询条件查询 获取所有 -->
<select id="queryAllTableDictItems" parameterType="String"  resultType="org.jeecg.common.system.vo.DictModel">
    select ${text} as "text", ${code} as "value" from ${table}
    <if test="filterSql != null and filterSql != ''">
        ${filterSql}
    </if>
</select>
```

queryTableDictByKeysAndFilterSql



```
        <if test="filterSql != null and filterSql != ''">
            ${filterSql}
        </if>
    </select>


    <!-- 查询字典表的数据 支持设置过滤条件、设置存储值作为in查询条件 -->
    <select id="queryTableDictByKeysAndFilterSql" parameterType="String" resultType="org.jeecg.common.system.vo
        select ${text} as "text", ${code} as "value" from ${table} where ${code} IN (
        <foreach item="key" collection="codeValues" separator=",">
            #{key}
        </foreach>
        )
        <if test="filterSql != null and filterSql != ''">
            and ${filterSql}
        </if>
    </select>
```

zhangdaiscott commented on Oct 29 Member

这里面有一些是必须这么写的，比如字典动态查询，虽然写法存在漏洞安全。我们在方法调用的地方已经加入了checksql注入逻辑。
针对一些可以优化的我们会处理

azraelxuemo commented on Oct 30 Author

您好，我理解你的考虑，所以最开始我以为单纯是预编译问题，直到看到了in ()这种，但您看我其他的一个issuse，您的checksql可以被easy bypass，然后我也提供了修复建议，希望可以采纳
这个issuse里面的几个sql因为我看到有x-sign的check，我暂时不知道怎么构造，所以我就没有poc，只是单纯提出来，希望可以帮助到您
…

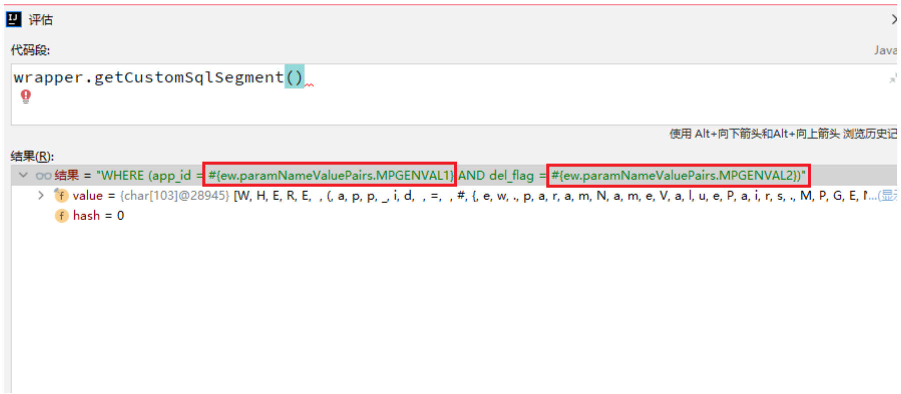
zhangdaiscott commented on Oct 30 Member

updateNullByEmptyString
selectLogicDeleted

sjlei commented on Nov 2

selectLogicDeleted

selectLogicDeleted里写的 `${ew.customSqlSegment}` 是MyBatisPlus提供的构造器，实际输出的就是带 `#` 的参数，不存在注入风险，可放心使用。



```
wrapper.getCustomSqlSegment()
```

```
结果 = "WHERE (app_id = #{ew.paramNameValuePairs.MPGENVAL1} AND del_flag = #{ew.paramNameValuePairs.MPGENVAL2})"
  value = {char[103]@28945} [W, H, E, R, E,  , (, a, p, p, _, i, d,  , =,  , #, {, e, w, ., p, a, r, a, m, N, a, m, e, V, a, l, u, e, P, a, i, r, s, ., M, P, G, E, N...(显
  hash = 0
```

azraelxuemo commented on Nov 2 Author

okok,了解嘞

zhangdaiscott added a commit that referenced this issue 27 days ago

【#4127】sql漏洞写法修复 958cf01

zhangdaiscott added a commit that referenced this issue 27 days ago

【#4127】sql漏洞写法修复 8632a83

zhangdaiscott commented 27 days ago Member

可以改的，已经提交

zhangdaiscott closed this as completed 27 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants