New issue

Jump to bottom

Mingsoft MCMS v5.2.8 SQL注入【后台】 #97

Closed **thunder-sec** opened this issue on Jul 17 · 1 comment

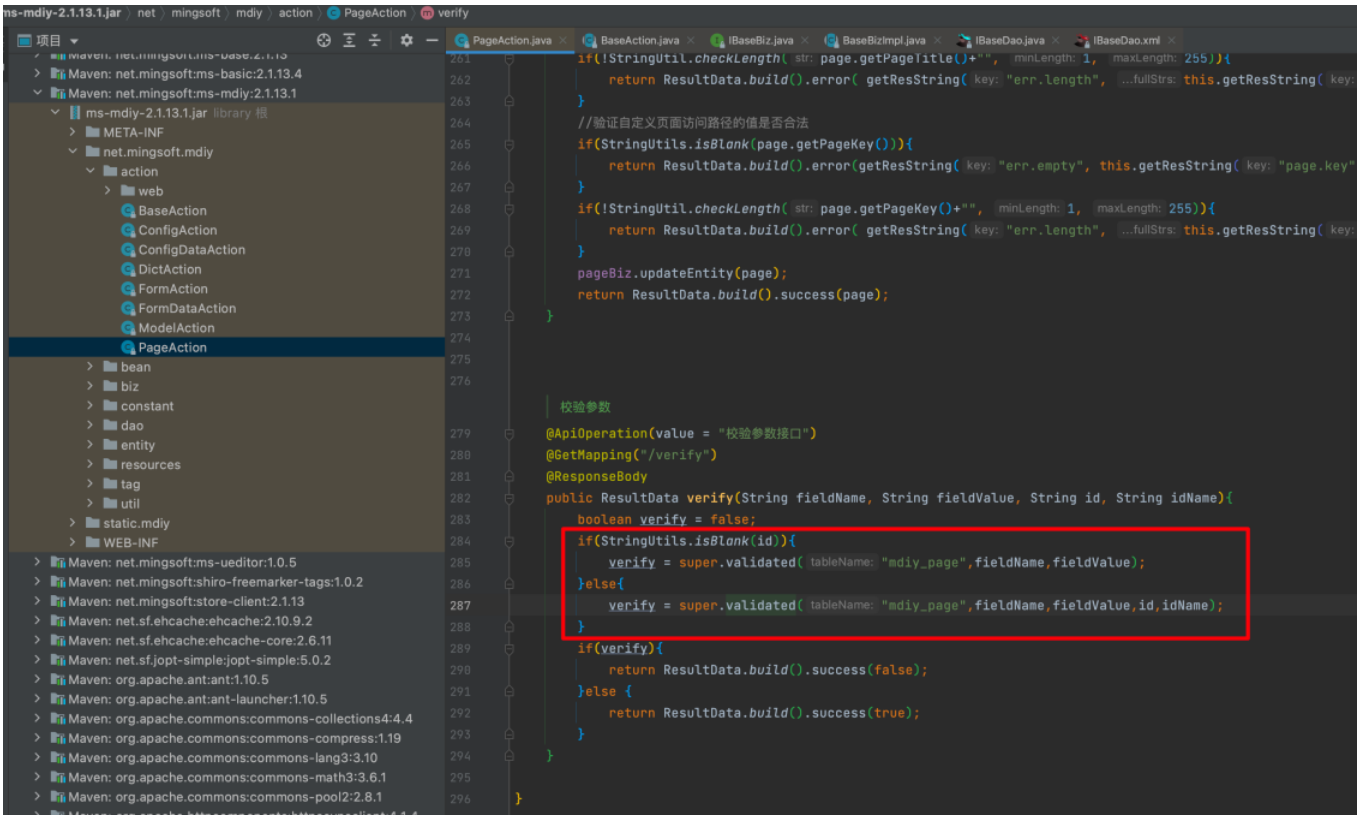
Assignees

Labels bug

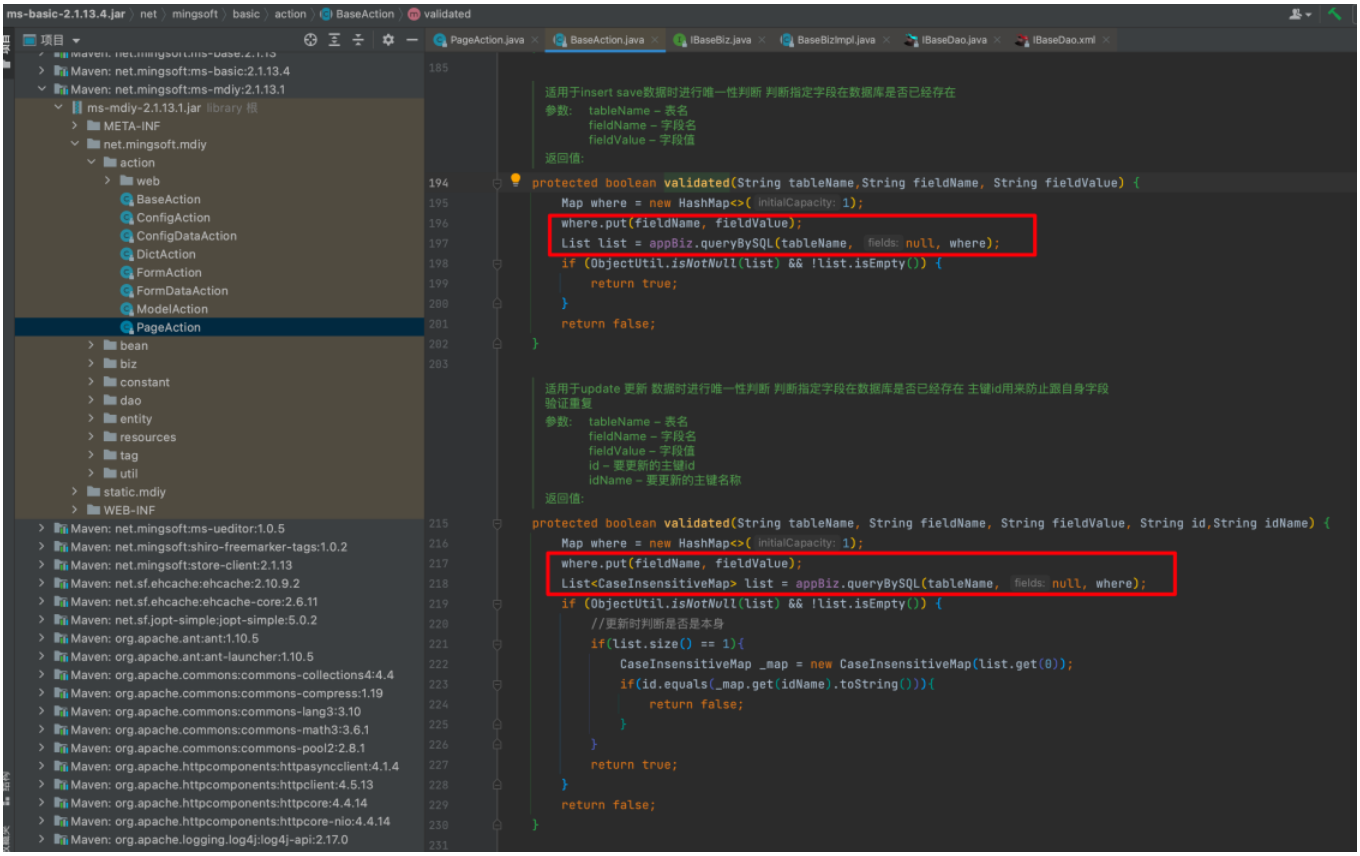
thunder-sec commented on Jul 17

漏洞分析

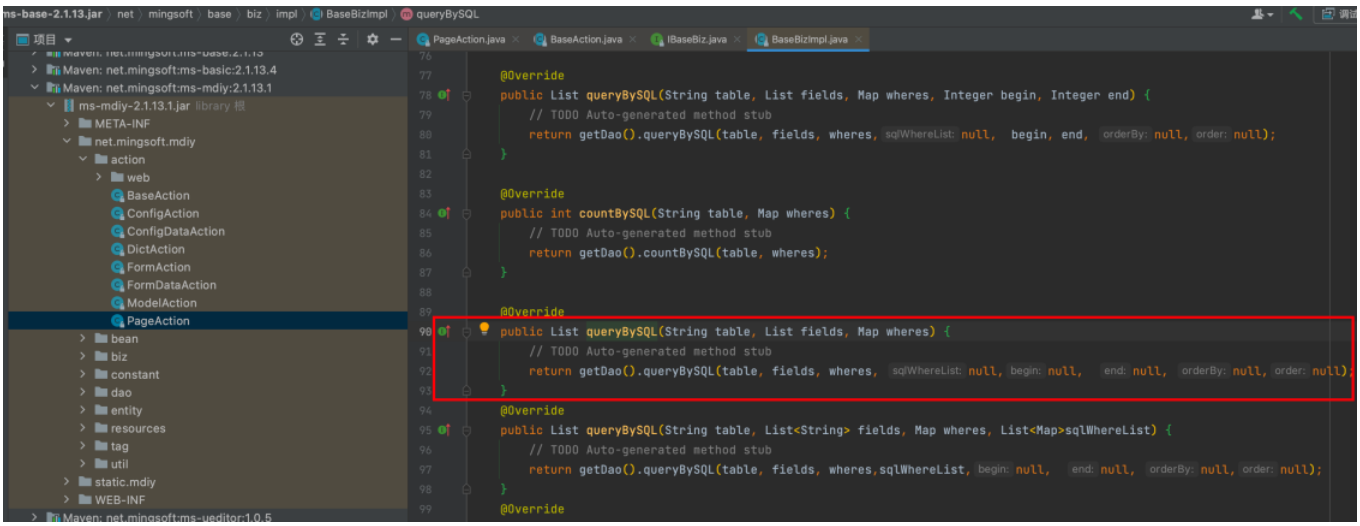
漏洞路由位置/${ms.manager.path}/mdiy/page/verify，漏洞点在如下方法，if...else两个条件中的validated方法均存在问题。

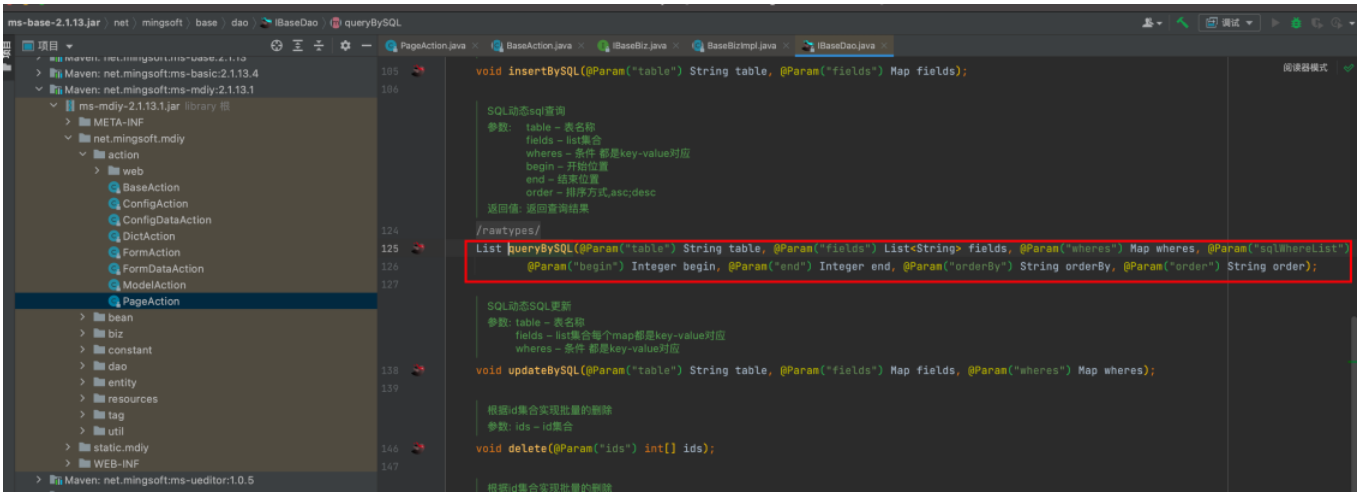


调用了父类的 `validated` 方法，validated方法中将传入的fieldName和fieldValue复制where对象中，并调用了 `appBiz.queryBySQL` 方法。

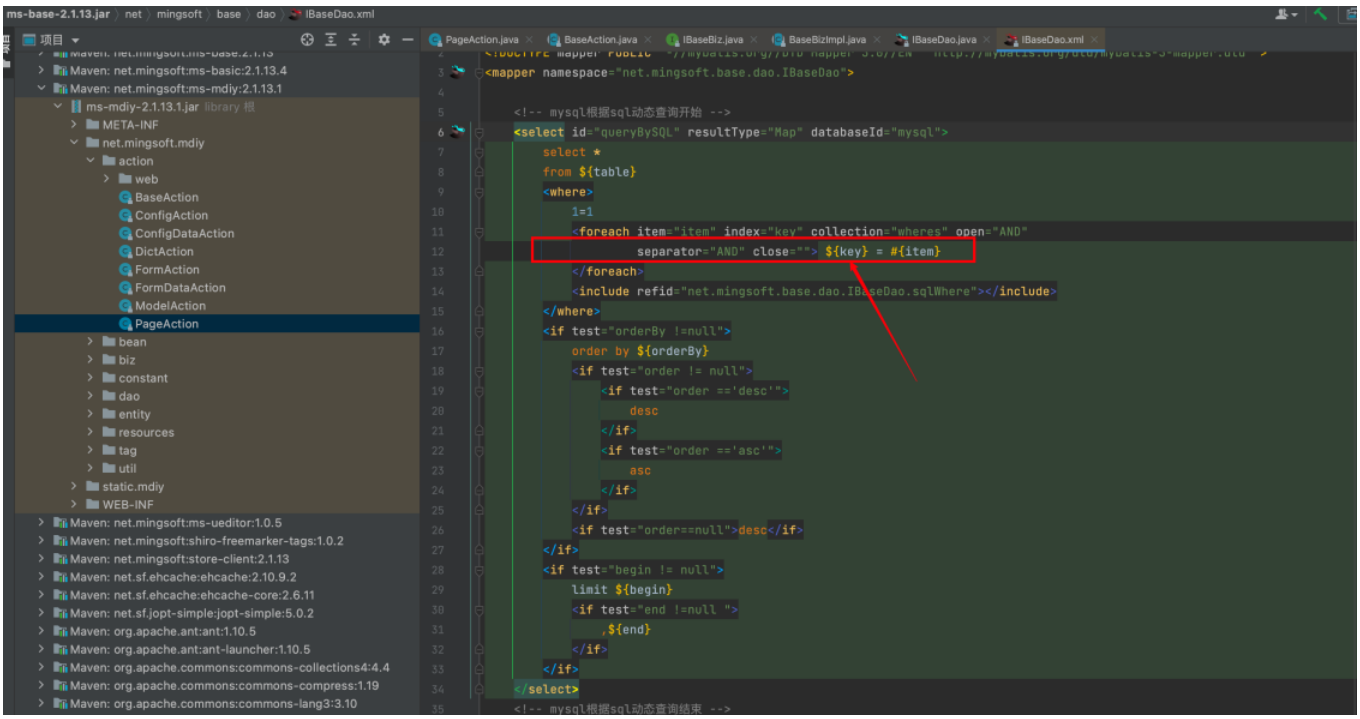


queryBySQL的实现方法如下调用了 `getDao().queryBySQL(table, fields, wheres, null,null, null, null,null);`



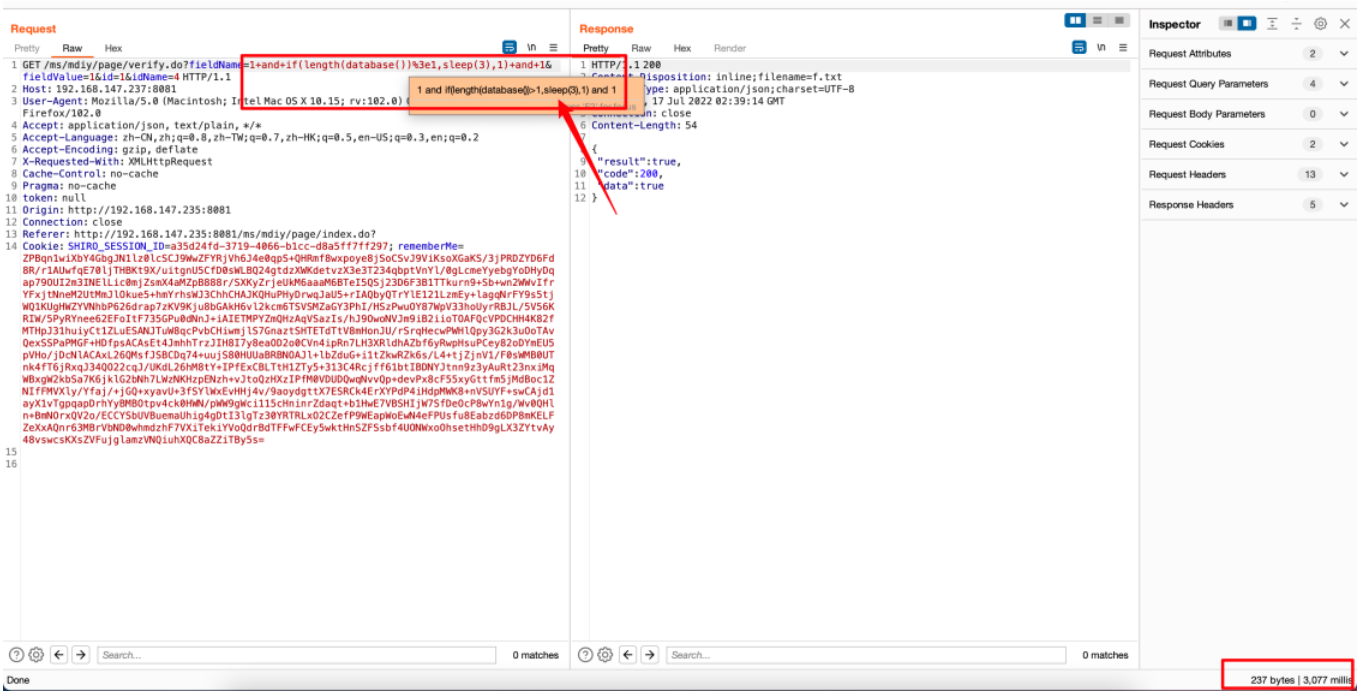


getDao().queryBySQL调用的具体SQL语句如下，其中key值对应的Map类型对象where，也就是前端传进来的fieldName

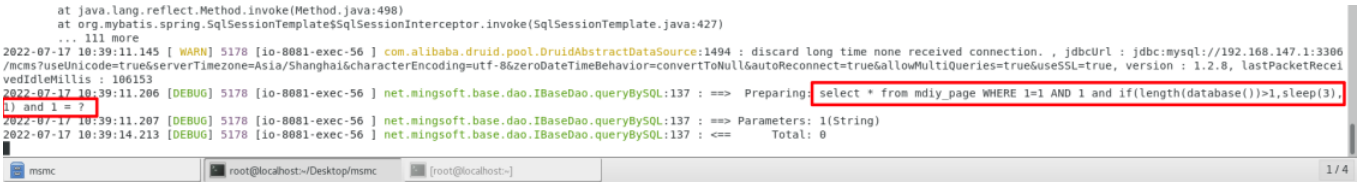


漏洞验证

构造如下请求包，如果数据库长度大于1，即成功睡眠3秒。



debug输出sql语句



killfen added the bug label on Sep 8

killfen self-assigned this on Sep 8

killfen commented on Sep 8 — Contributor

5.2.9 fix it

killfen closed this as completed on Sep 8

Assignees

killfen

Labels

bug

bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants