

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

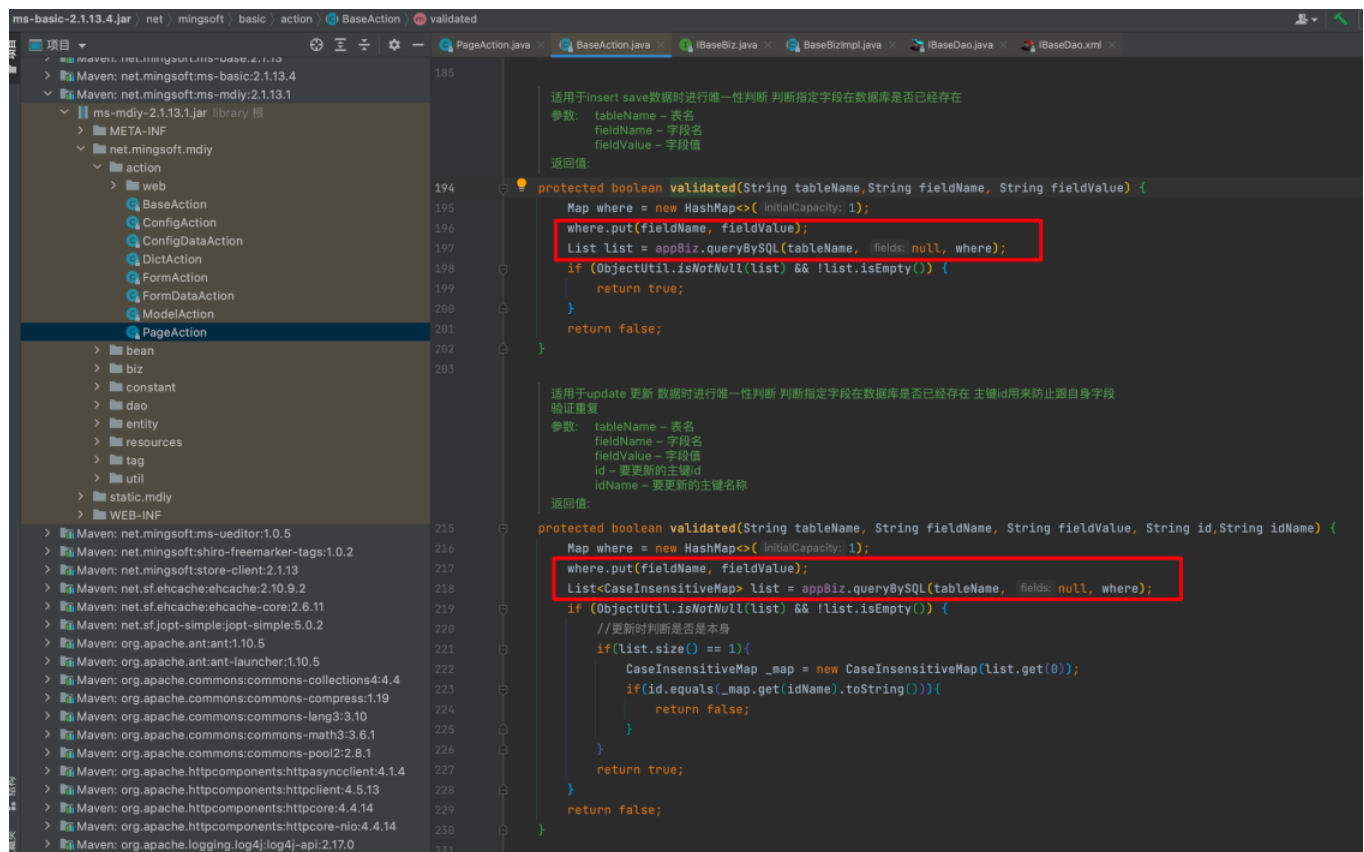
thunder-sec commented on Jul 17

漏洞分析

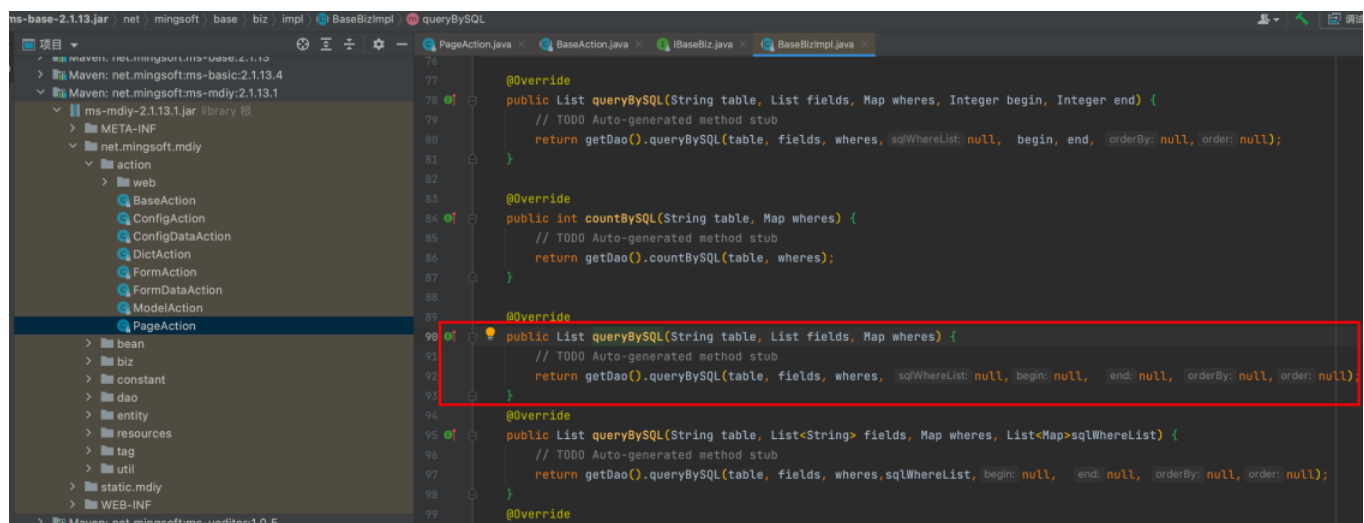
漏洞路由位置/\${ms.manager.path}/mdiy/page/verify，漏洞点在如下方法，if...else两个条件中的validated方法均存在问题。

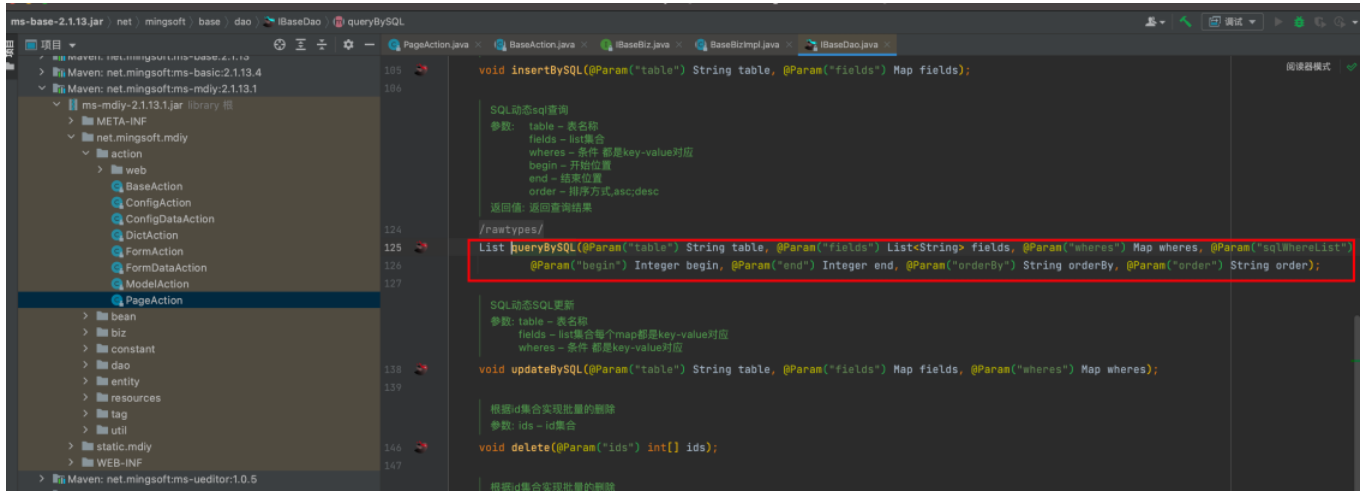
```
261 public ResultData verify(String fieldName, String fieldValue, String id, String idName) {
262     if (!StringUtil.checkLength(str: page.getPageTitle(), minLength: 1, maxLength: 255)) {
263         return ResultData.build().error(getResString(key: "err.length", ...fullStrs: this.getResString(key:
264     })
265     //验证自定义页面访问路径的值是否合法
266     if (StringUtil.isBlank(page.getPageKey())) {
267         return ResultData.build().error(getResString(key: "err.empty", this.getResString(key: "page.key"
268     })
269     if (!StringUtil.checkLength(str: page.getPageKey(), minLength: 1, maxLength: 255)) {
270         return ResultData.build().error(getResString(key: "err.length", ...fullStrs: this.getResString(key:
271     })
272     pageBiz.updateEntity(page);
273     return ResultData.build().success(page);
274 }
275
276
277
278
279 校验参数
280 @ApiOperation(value = "校验参数接口")
281 @GetMapping("/verify")
282 @ResponseBody
283 public ResultData verify(String fieldName, String fieldValue, String id, String idName) {
284     boolean verify = false;
285     if (StringUtil.isBlank(id)) {
286         verify = super.validated(tableName: "mdiy_page", fieldName, fieldValue);
287     } else {
288         verify = super.validated(tableName: "mdiy_page", fieldName, fieldValue, id, idName);
289     }
290     if (verify) {
291         return ResultData.build().success(false);
292     } else {
293         return ResultData.build().success(true);
294     }
295 }
296 }
```

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。

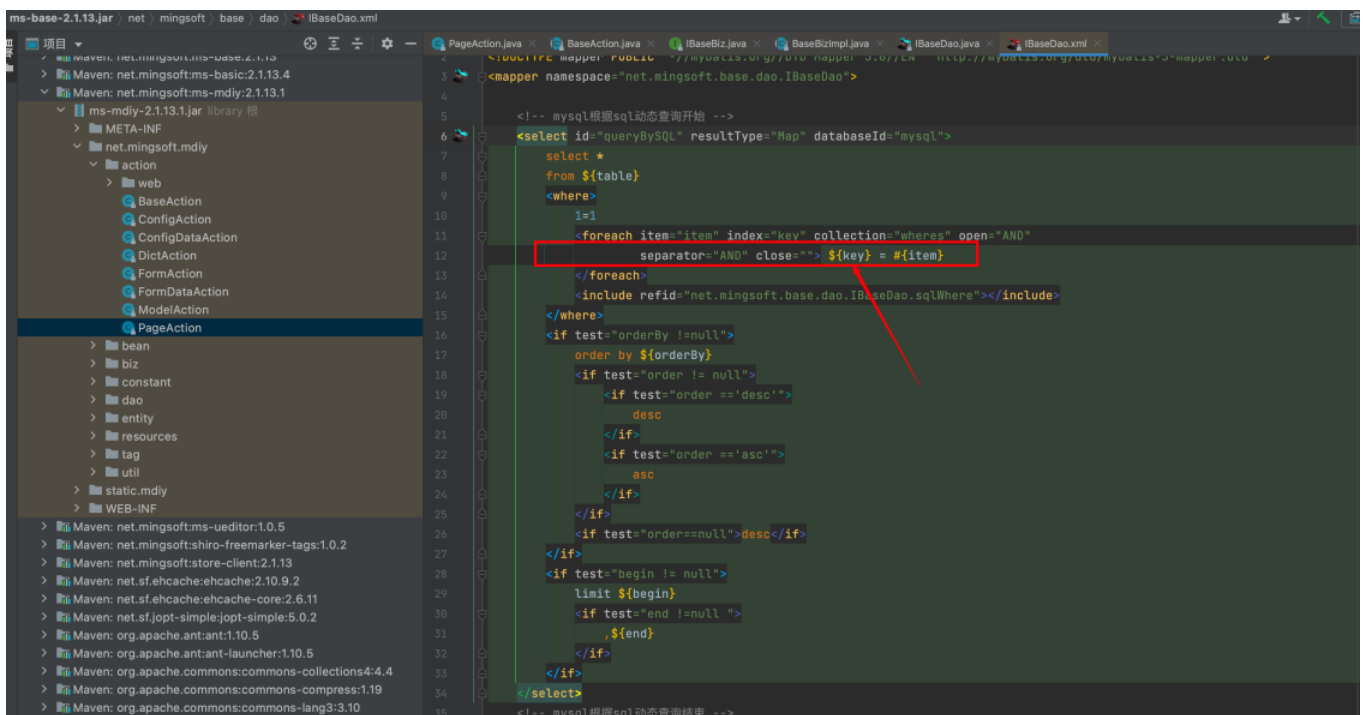


queryBySQL的实现方法如下调用了 getDao().queryBySQL(table, fields, wheres, null,null, null, null,null);





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。

dug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

