

Code

Issues 2

Pull requests

Actions

Projects

Security

Insights

New issue



A fatal error that can access the background without authorization #1

Open



haioudelibaiyi opened 3 weeks ago

...

There are no login restrictions :

```

NoNeedLoginController.java
public class NoNeedLoginController extends BaseAbstractController {
    /**
     * 登陆的具体操作
     * @return
     */
    @RequestMapping({"/", "/login"})
    public String login(HttpServletRequest request) { return "admin/login"; }

    /**
     * 登陆次数+1
     */
    @RequestMapping({"/toLogin"})
    @MethodLog(type = "登陆")
    public @ResponseBody Object toLogin(String account, String password, HttpServletRequest request) {
        UserVO vo = systemDao.login(account, password);
        getClientENV(request.getSession()).setCurUser(vo);
        // 登陆次数+1
        systemDao.upLastLogin(UserAgentUtil.getRemoteAddr(request), vo.getUserId());
        return getReturnJsonMap();
    }

    /**
     * 刷新静态化页面
     */
    @RequestMapping(values = {"flushPage"})
    public @ResponseBody Object flushPage(String url, HttpServletRequest request) {
        StaticPageUtils.flushPage(url);
        return getReturnJsonMap();
    }
}

```

The routes in the background can be accessed directly:

```

public class CommonController extends BaseAbstractController {
    private SystemDao systemDao;

    /**
     * @param request
     * @return
     */
    @RequestMapping({@"/admin"})
    public String admin(HttpServletRequest request) {
        // 根据用户角色获取权限 获取用户拥有的菜单、页面、按钮
        UserVO user = getCurUser(request.getSession());
        List<AdminPageMenuVO> menus = AdminPageUtils.getHasAdminPageMenus(user.getRole());
        request.setAttribute("menus", menus);
        getClientENV(request.getSession()).setAdminPageMenus(menus);
        request.setAttribute("mustPsChange", getMustPsChange(user));
        return "admin/index";
    }

    /**
     * 查看是否需要修改密码
     * @param user
     * @return
     */
    private boolean getMustPsChange(UserVO user) { 1个用法
        String PSCHANGE_MONTH = Commons.getConfigValue(code: "PSCHANGE_MONTH", defvalue: "-1");
        if(StringUtil.isNotBlank(user.getPsChangeTime()) || "-1".equals(PSCHANGE_MONTH)) return false;
        String ts = DateTimeUtil.getLastMonthTime(Integer.parseInt(PSCHANGE_MONTH));
    }
}

```

Access the background to obtain super administrator privileges : <http://127.0.0.1:8999/admin>

The screenshot shows the JAdmin backend development framework's user management interface. The left sidebar includes '用户管理' and '系统管理' sections. The main content area displays a user profile (username: 系统管理员, role: 超级管理员, login count: 1, last login IP: 127.0.0.1, last login time: 2018-11-26 08:35:41). Below this is a '常见问题' section with links like '系统推荐使用哪款浏览器?' and '忘记密码如何找回?'. To the right is a '实用小工具' section with icons for clock, calculator, image, Chinese input method, and others. At the bottom right is a calendar for April 2025.

Add users, view logs, etc

The screenshot shows the JAdmin backend development framework's user management interface. The left sidebar includes '用户管理' and '系统管理' sections. The main content area shows a '添加' (Add) dialog for a new user. The fields are: 账号: test1, 姓名: test1, 性别: 男, 所属角色: 超级管理员, 所属部门: 管理部, 联系: 123456, 状态: 启用. On the right, there is a log table with one entry: 1-21 08:21:34 | admin.

Request

```

1 POST /user/edit?nrTab= HTTP/1.1
2 Host: 127.0.0.1:8999
3 Content-Length: 1218
4 Cache-Control: max-age=0
5 sec-ch-ua: "Google Chrome";v="135", "Not-A-Brand";v="8", "Chromium";v="135"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Origin: http://127.0.0.1:8999
9 Content-Type: multipart/form-data;
  boundary=====WebKitFormBoundaryqAXJersUHU17Xdhz
10
11 =====WebKitFormBoundaryqAXJersUHU17Xdhz
12 Content-Disposition: form-data; name="primaryKey"
13
14
15 =====WebKitFormBoundaryqAXJersUHU17Xdhz
16 Content-Disposition: form-data; name="baseHere"
17
18
19 =====WebKitFormBoundaryqAXJersUHU17Xdhz
20 Content-Disposition: form-data; name="hideReturn"
21
22
23 =====WebKitFormBoundaryqAXJersUHU17Xdhz
24 Content-Disposition: form-data; name="hideTitle"
25
26 true
27 =====WebKitFormBoundaryqAXJersUHU17Xdhz

```

Response

```

1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=280C65B02D94267047BFF85B47332D97; Path=/; HttpOnly
3 Content-Type: text/html;charset=UTF-8
4 Content-Language: zh-CN
5 Content-Length: 223
6 Date: Fri, 18 Apr 2025 07:32:38 GMT
7
8
9 <!DOCTYPE HTML>
10 <html>
11   <head>
12     </head>
13   <body>
14     <script type="text/javascript">
15       parent.parent.layer0.show('操作成功，正在刷新页面……');
16       parent.layer.closeAll();
17     </script>
18   </body>
19 </html>

```

The screenshot shows a web-based administration interface. On the left, there's a sidebar with '用户管理' (User Management) and '系统管理' (System Management) sections. The main area has tabs for '我的桌面' (My Desktop), '接口中心' (API Center), '国度管理' (Country Management), '搜索字典' (Search Dictionary), and '系统设置' (System Settings). A search bar at the top right contains the placeholder 'Search...'. Below the search bar are two buttons: '0 matches' and '0 matches'.

This screenshot shows a detailed log table under the '系统日志' (System Log) section. The table has columns for '操作人' (Operator), 'IP', and '时间' (Time). Each row contains a checkbox, the operator name, IP address, and timestamp. To the right of the table, there's a '详细内容' (Detailed Content) column displaying log entries. At the bottom right of the table, it says '共有数据: 14' (Total data: 14).

	操作人	IP	时间	详细内容
test1	127.0.0.1	2025-04-18 15:20:40		操作: 退出登录: {status: true, errorMsg: ''}
管理员	127.0.0.1	2025-04-18 15:25:16		用户管理->用户管理->删除: 返回结果: public/del-layer, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 15:31:06		用户管理->用户管理->删除: 返回结果: public/del-layer, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 15:32:44		用户管理->用户管理->删除成功: 返回结果: success, 数据: {}
管理员	127.0.0.1	2025-04-18 11:44:48		用户管理->用户管理->删除: errorMsg: 该角色存在, 无法删除!, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 11:46:12		用户管理->用户管理->删除: errorMsg: 该角色存在, 无法删除!, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 11:51:45		用户管理->用户管理->删除: errorMsg: 该角色存在, 无法删除!, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 11:25:22		用户管理->用户管理->删除成功: 返回结果: public/del-layer, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 11:19:49		用户管理->用户管理->删除: errorMsg: 该角色存在, 无法删除!, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}
管理员	127.0.0.1	2025-04-18 11:19:12		用户管理->用户管理->删除成功: 返回结果: public/del-layer, 数据: {"role":0,"msg":1,"isDelete":1,"sex":1}

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

 Code with Copilot Agent Mode

No branches or pull requests

Participants

