

New issue

[Jump to bottom](#)

Your source code has a SQL injection vulnerability #92

🕒 Open

CNXWHAT opened this issue on Jun 30 · 0 comments

CNXWHAT commented on Jun 30

Hello, this vulnerability allows the user to trigger before logging in.

File path: [novel-front/src/main/java/com/java2nb/novel/service/impl/BookServiceImpl.java](#)

```
@Override
public PageBean<?> searchByPage(BookSpVO params, int page, int pageSize) {

    if (params.getUpdatePeriod() != null) {
        long cur = System.currentTimeMillis();
        long period = params.getUpdatePeriod() * 24 * 3600 * 1000;
        long time = cur - period;
        params.setUpdateTimeMin(new Date(time));
    }

    if (esEnable == 1) {

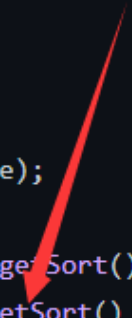
        try {
            return searchService.searchBook(params, page, pageSize);

        } catch (Exception e) {
            log.error(e.getMessage(), e);
        }

    }
    PageHelper.startPage(page, pageSize);

    if (StringUtil.isNotBlank(params.getSort())) {
        OrderByHelper.orderBy(params.getSort() + " desc");
    }

    return PageBuilder.build(bookMapper.searchByPage(params));
}
```



Vulnerability is only triggered when at least one piece of data can be queried. The "keyword" parameter can be set to % (urlencode:%25)

Example:

 CNXWHAT changed the title ~~There are two sql injection vulnerabilities in your source code~~ Your source code has a **SQL injection vulnerability** on Jun 30

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant



