

liyupi / yu-picture Public

<> Code Issues 1 Pull requests 3 Actions Projects Security and quality

fix: prevent SQL injection via sortField parameter in PageRequest #3

Open jackieya wants to merge 2 commits into liyupi:master from jackieya:master

Conversation Commits 2 Checks Files changed



jackieya commented 3 weeks ago

漏洞描述

`PageRequest.sortField` 参数未经校验直接拼接到 MyBatis-Plus 的 `orderBy` 方法中，导致多个分页查询接口存在 ORDER BY 子句 SQL 注入。

受影响接口：

- POST `/api/picture/list/page/vo` (无需认证)
 - POST `/api/space/list/page/vo` (无需认证)
 - POST `/api/user/list/page/vo` (需管理员权限)
- 攻击者可利用 time-based 盲注提取数据库中的任意数据。

修复方案

在 `PageRequest.setSortField()` 中添加正则白名单校验 `^[a-zA-Z][a-zA-Z0-9]*$`，仅允许合法列名格式（字母开头，仅含字母和数字）。

- 复用项目已有的 `ThrowUtils` + `ErrorCode.PARAMS_ERROR`
- 所有继承 `PageRequest` 的子类自动受到保护
- 正常排序请求不受影响

漏洞复现

```
bash curl -w "\nTime: %{time_total}s\n" -X POST http://TARGET/api/picture/list/page/vo \ -H "Content-Type: application/json" \ -d '{"sortField":"(SELECT 1 FROM (SELECT SLEEP(3)) t)","sortOrder":"ascend","current":1,"pageSize":10}'
```

fix: prevent SQL injection via sortField parameter in PageRequest de57bef

Copilot AI review requested due to automatic review settings [3 weeks ago](#)

Copilot started reviewing on behalf of **jackieya** [3 weeks ago](#)

[View session](#)

jackieya mentioned this pull request [3 weeks ago](#)

[Security] SQL Injection via sortField parameter in multiple unauthenticated endpoints

#4

[Open](#)

Copilot AI reviewed [3 weeks ago](#)

[View reviewed changes](#)

Copilot AI left a comment

Pull request overview

This PR mitigates an ORDER BY SQL injection risk by validating `PageRequest.sortField` before it is used to build MyBatis-Plus `orderBy` clauses.

Changes:

- Added whitelist validation in `PageRequest.setSortField()` to restrict sortable fields to a safe identifier pattern.
- Reused existing `ThrowUtils` + `ErrorCode.PARAMS_ERROR` for consistent parameter error handling.

[Add Copilot custom instructions](#) for smarter, more guided reviews. [Learn how to get started.](#)



```

yu-picture-backend/src/main/java/com/yupi/yupicturebackend/common/PageRequest.java
...
@@ -27,4 +29,12 @@ public class PageRequest {
27      29      * 排序顺序 (默认升序)
  
```

Outdated

**Copilot** AI 3 weeks ago

Javadoc/注释与实际默认值不一致：这里写“排序顺序（默认升序）”，但 sortOrder 默认值是“descend”（降序）。建议二选一：要么把默认值改成“ascend”，要么把注释改为“默认降序”，避免误导接口调用方。

Suggested change

-	* 排序顺序 (默认升序)
+	* 排序顺序 (默认降序)

[Copilot](#) uses AI. Check for mistakes.

yu-picture-backend/src/main/java/com/yupi/yupicturebackend/common/PageRequest.java

Comment on lines +33 to +37

```
33 + public void setSortField(String sortField) {
34 +     if (sortField != null && !sortField.isEmpty()) {
35 +         ThrowUtils.throwIf(!sortField.matches("[a-zA-Z][a-zA-Z0-9]*$"),
36 +             ErrorCode.PARAMS_ERROR, "排序字段名称不合法");
37 +     }
```

**Copilot** AI 3 weeks ago

这里用 String#matches 每次调用都会重新编译正则，虽然调用频率不高但属于可避免的开销。建议将正则提取为 static final Pattern（或常量）并复用，既能减少重复编译，也更便于后续修改/复用该白名单规则。

[Copilot](#) uses AI. Check for mistakes.

refactor: extract regex to static final Pattern, fix sortOrder comment

6f4443a

Sign up for free to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Reviewers

Copilot

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging this pull request may close these issues.

None yet

2 participants

