New issue

[Security] SQL Injection via sortField parameter in multiple unauthenticated endpoints #4

Open

jackieya opened 3 weeks ago

Vulnerability Type

SQL Injection (Time-based Blind)

Affected Version

All versions (up to current latest master branch)

Description

The `sortField` parameter in `PageRequest` is passed directly to MyBatis-Plus `orderBy()` method without any validation, resulting in ORDER BY clause SQL injection. The endpoints `POST /api/picture/list/page/vo` and `POST /api/space/list/page/vo` are **accessible without authentication**.

Affected Code

PictureServiceImpl.java (L336)

```
String sortField = pictureQueryRequest.getSortField();  // user-controlled
queryWrapper.orderBy(StrUtil.isNotEmpty(sortField), sortOrder.equals("ascend"), sortFie
// sortField is directly concatenated as column name, no parameterization, no whitelist
```

Same pattern exists in:

- **SpaceServiceImpl.java** (L224) — no auth required

- **UserServiceImpl.java** (L240) — admin role required

Steps to Reproduce

Send the following request and observe a ~3 second delay in response time:

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

- Normal request (`sortField: "id"`) responds in ~0.02s
- Injected request responds in **~3.0s**, confirming SLEEP execution

Impact

- Exploitable **without authentication** (Pre-Auth)
- Attacker can extract arbitrary data from the database via time-based blind SQL injection (user credentials, admin passwords, etc.)

Fix

PR: #3

Metadata

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants