

HiEventsDev / Hi.Events Public[Code](#) [Issues](#) 127 [Pull requests](#) 21 [Discussions](#) [Actions](#) [Projects](#)

fix: Validate sort_by parameter against allowlist in repositories #1128

Merged **daveearley** merged 1 commit into `develop` from `fix/validate-sort-by-parameters` 
last week

[Conversation](#) [Commits](#) 1 [Checks](#) [Files changed](#)



daveearley commented [last week](#) • edited ▾

Contributor

Summary

- Multiple repository classes were passing the user-supplied `sort_by` query parameter directly to Eloquent's `orderBy()` without validation, enabling SQL injection (PostgreSQL supports stacked queries, so this is particularly spicy)
- Added `validateSortColumn()` and `validateSortDirection()` helpers to `BaseRepository` that check against each domain object's existing `getAllowedSorts()` whitelist
- Applied validation across all 11 affected repository files — invalid values silently fall back to defaults
- Added `IsSortable` to `ProductCategoryDomainObject` (the one domain object that was missing it)

The allowlist pattern was already used correctly in the admin endpoints (`getAllEventsForAdmin` , `getAllOrdersForAdmin`) — this just applies the same approach everywhere else.

Test plan

- All 350 unit tests pass
- Verify sorting still works on attendees, orders, events, promo codes, etc.
- Confirm invalid `sort_by` values fall back to defaults instead of erroring

Reported by [@tikket1](#)





[fix: Validate sort_by parameter against allowlist in all repositories](#)

✓ [cdd5485](#)



daveearley changed the base branch from `main` to `develop` [last week](#)



daveearley merged commit `01e1aee` into `develop` [last week](#)

4 checks passed

[View details](#)



daveearley deleted the `fix/validate-sort-by-parameters` branch [last week](#)



github-actions `bot` locked and limited conversation to collaborators [last week](#)

[Sign up for free](#)

to subscribe to this conversation on **GitHub**. Already have an account? [Sign](#)

[in.](#)

Reviewers

No reviews

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

1 participant

