New issue

Jump to bottom

SQL Injection in Reactive project #18269

Closed **appkr** opened this issue on Apr 3 · 35 comments · Fixed by #18294

Labels area: bug $$ bug-bounty $$ theme: reactive theme: security $500

Milestone 7.8.1

appkr commented on Apr 3

I don't know whether this is the right place to ask this though...

In a reactive spring project with r2dbc, I found that SQL injection is actually possible. This may happen because of me, lacking knowledge on how to use r2dbc correctly. If it is case please let me know the correct usage.

Setup

- Jhipster 7.7.0
- reactive with Spring WebFlux? Yes
- type of database? SQL

JDL

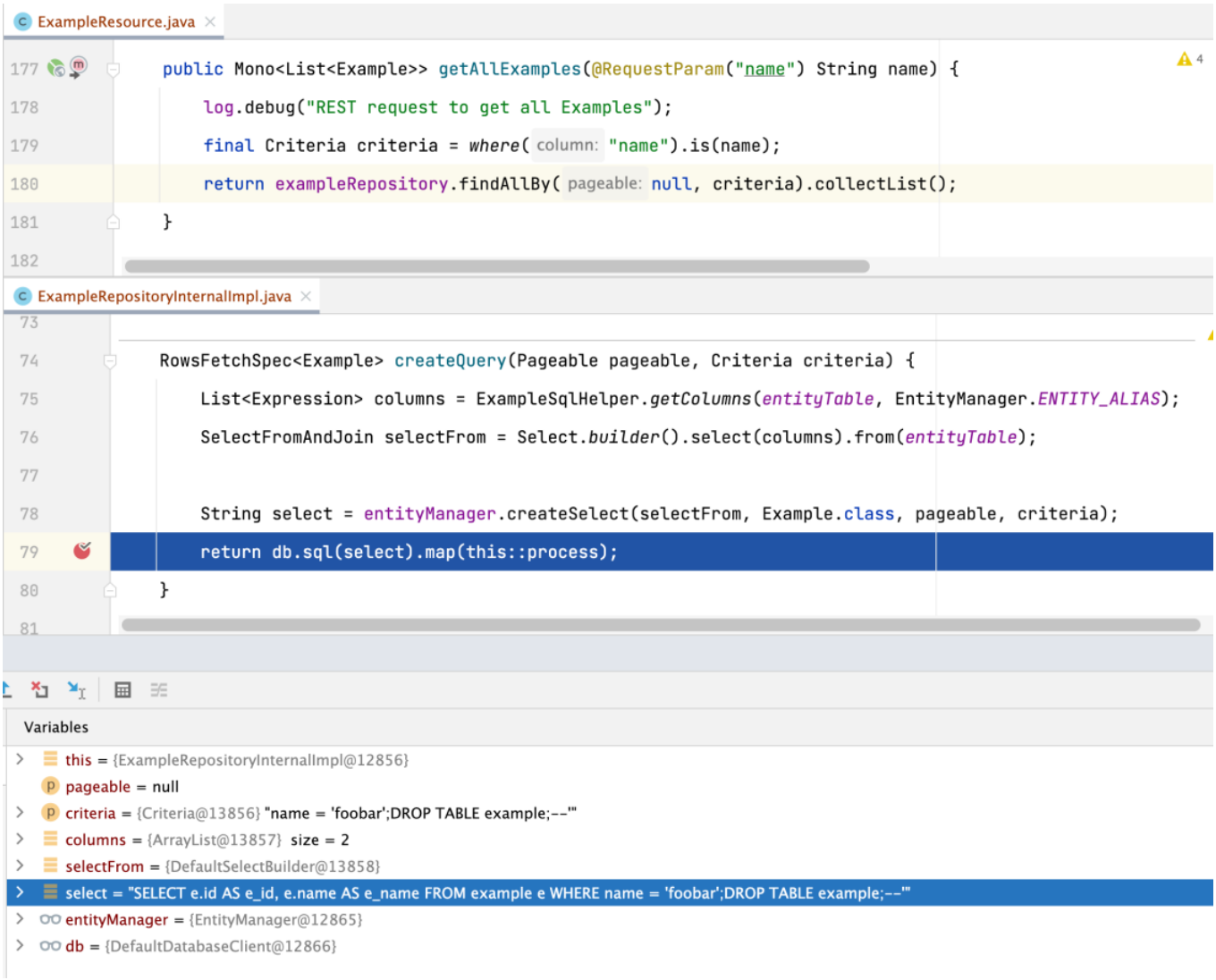
```
entity Example {
        id String
  name String
}
```

Change I made

- Make /api/** be accessible without authorization header
- Make GET /api/examples accept query parameter of `name`, and bind the parameter to the `findAllBy(Pageable pageable, Criteria criteria)` repository method
- Make a request to `GET /api/examples?name=foobar';DROP TABLE example;--`

Result

- The sql rendered was `SELECT e.id AS e_id, e.name AS e_name FROM example e WHERE name = 'foobar';DROP TABLE example;--'`
- That actually dropped the table



github-actions bot added area: triage theme: undefined labels on Apr 3

pascalgrimaud added area: needs-reproduction theme: security theme: reactive and removed area: triage theme: undefined labels on Apr 4

pascalgrimaud commented on Apr 4 — Member

Cc @jhipster/developers

atomfrede commented on Apr 4 — Member

Didn't expect that. Is it the same for non reactive/hibernate?

pascalgrimaud commented on Apr 4 — Member

I think it's important to try and check

👍 2 ❤️ 2

jdubois commented on Apr 4 — Member

On non-reactive, at least when I worked on it a few years ago, we were using Hibernate's criteria API, which would prevent this.

👍 1

 **pascalgrimaud** added area: bug $$ bug-bounty $$ $500 and removed area: needs-reproduction labels on Apr 4

deepu105 commented on Apr 4 — Member

For non reactive i'll be extremely surprised if its the case since we don't do any direct SQL and everything goes via Spring Data and hibernate

👍 1

atomfrede commented on Apr 4 — Member

Yes me too. Maybe thats also the reason why we didn't check it for reactive part in detail. Spoiled by hibernate's power 😄

deepu105 commented on Apr 4 • edited — Member

we should be using named parameters isn't it? seems like here its generating with value instead

OmarHawk commented on Apr 4 • edited — Contributor

Probably, the Conditions.just taking a literal sql here allowing an arbitrary WHERE clause, but also being vulnerable for injection:

generator-jhipster/generators/server/templates/src/main/java/package/repository/EntityManager.java.ejs
Line 122 in 85aa8dd

```
122     return createSelectImpl(selectFrom.limitOffset(pageable.getPageSize(), pageable.getOffset()
```

and here:

generator-jhipster/generators/server/templates/src/main/java/package/repository/EntityManager.java.ejs
Line 128 in 85aa8dd

```
128     return createSelectImpl(selectFrom.where(Conditions.just(criteria.toString())), entityType,
```

OmarHawk commented on Apr 4 — Contributor

Probably came out of the following PR #13515

deepu105 commented on Apr 4 — Member

@atomfrede are you working on this? else I can try to find a fix?

atomfrede commented on Apr 4 — Member

Wanted to start now.

👍 1

deepu105 commented on Apr 4 — Member

I have a CVE drafted for this ready to go once we have a fix in place. Let me know if you need any help

👍 1

atomfrede commented on Apr 4 — Member

At least I can reproduce it too pretty easy :(

atomfrede commented on Apr 4 • edited ▾ Member

When mapping the criteria manually to a condition it is not vulnerable, but somehow this seems to me as not the intended way to use spring datas criteria. But using `.just(VALUE)` instead of `.just(WHOLE CRITERIA)` seems to do the trick. But creating the custom mapping will be a lot of code and most likely quite error prone.

@mraible Maybe you have come across this?

```
//Criteria.where("name").is("foobar';DROP TABLE example;--");
//-->toString -->'foobar';DROP TABLE example;--'
//name=foobar';DROP TABLE example;--
Comparison equal = Conditions.isEqual(
Column.create(criteria.getColumn(), Table.create("example")),
                    Conditions.just(criteria.getValue().toString()));
```

atomfrede commented on Apr 4 Member

I have created a reproducer here https://github.com/atomfrede/reactive-sql-jhipster-reproducer which has a potential hand coded fix. Try it via `http://localhost:8080/api/examples?name=foobar';DROP TABLE example;--` . Without the changes it will indeed delete the table while with the hand coded condition it works correctly.

deepu105 commented on Apr 4 Member

@atomfrede how important is the where clause mapping? can we remove the feature for the time being if it only affects searching in Get queries? so that we can publish a fix and then look for a proper solution?

atomfrede commented on Apr 4 Member

As far as I can tell the generated application does not need it by default I think. All crud operations should work without the custom criteria (need to check). So yes we might remove it for the time being.

deepu105 commented on Apr 4 • edited ▾ Member

In that case, I vote to remove it and publish a patch and CVE. Then we can create a new issue to add the feature in a secure and scalable way (if it's important). **@jdubois @pascalgrimaud @mraible @DanielFran @jhipster/developers** WDYAT?

pascalgrimaud commented on Apr 5 Member

Agree with this fix. We can see later if we can do better

1

atomfrede commented on Apr 5 Member

So basically we will ignore the `Criteria` provided to `EntityManager.createSelect` right?

deepu105 commented on Apr 5 Member

yes, and maybe change signature in generated code, if possible, to not take the criteria and add a comment so that users don't end up adding the same manually

1

pascalgrimaud added this to the **7.8.1** milestone on Apr 5

DanielFran commented on Apr 5 Member

Yes, I agree too with this fix.

atomfrede added a commit to atomfrede/generator-jhipster that referenced this issue on Apr 5

`use conditions instead of criteria as workaround` ... `5a37a9f`

atomfrede mentioned this issue on Apr 5

use conditions instead of criteria as workaround #18294

Merged

6 tasks

deepu105 closed this as completed in `c220a21` on Apr 6

deepu105 closed this as completed in #18294 on Apr 6

deepu105 mentioned this issue on Apr 6

Bump jhipster-bom version to 7.8.1 #18305

Merged

6 tasks

deepu105 commented on Apr 7 — Member

Thanks to everyone involved **@appkr** **@OmarHawk** we have decided to award each of you a 300$ bounty so please claim it via open collective. **@atomfrede** for you, we (me, Julien, Pascal) think you deserve more than 500$ so I'll send a mail in the public group to discuss that.

👍 2 ❤️ 2

appkr commented on Apr 7 — Author

@deepu105 Thanks, the claim was filed at https://opencollective.com/generator-jhipster/expenses/71638

deepu105 commented on Apr 7 — Member

@appkr it's approved. Next time please do report security issues to project maintainers privately first so we can disclose it responsibly after fixing them.

appkr commented on Apr 7 — Author

@deepu105 My bad, sorry. Yes I will If I have any.

OmarHawk commented on Apr 7 — Contributor

> Thanks to everyone involved **@appkr** **@OmarHawk** we have decided to award each of you a 300$ bounty so please claim it via open collective. **@atomfrede** for you, we (me, Julien, Pascal) think you deserve more than 500$ so I'll send a mail in the public group to discuss that.

Thanks :-). Filed it at https://opencollective.com/generator-jhipster/expenses/71657

mshima commented on Apr 7 — Member

@deepu105 it's missing to tag the release at GitHub https://github.com/jhipster/generator-jhipster/releases.

mraible commented on Apr 7 • edited ▾ Contributor

I noticed there are two draft releases on the releases page. We should fix that and remove all the dependabot updates. As a developer, I like to quickly skim release notes, not scroll through automated patch updates from dependabot.

deepu105 commented on Apr 7 Member

I'll clean those up once I have power back. Hopefully tonight or tomorrow morning
...

deepu105 commented on Apr 7 Member

@mshima **@mraible** I dont think the release page is used at all, since I see a lot of drafts. **@pascalgrimaud** do you know who set up the release drafter? there are too many drafts and the date is wrong as well

pascalgrimaud commented on Apr 7 Member

@deepu105 : there was a bug 1 month ago in GitHub, that's why there are a lot of duplicated drafts. All these drafts need to be deleted manually, then release-drafter can work normally

deepu105 commented on Apr 7 Member

there are like pages and pages of them :P so that's gonna be some long task

Thanks & Regards,
Deepu
...

pascalgrimaud commented on Apr 7 Member

I know, I spent a lot lot lot of time to delete it in jhipster-lite project, but didn't have motivation to do it for generator-jhipster...

deepu105 commented on Apr 7 Member

I created a ticket and assigned bounty lets see if someone is motivated

Thanks & Regards,
Deepu
...

 **rjbgaspar** mentioned this issue on Jun 2

Bad SQL grammar is thrown for all entities with string ID types #18804

Closed

Assignees

No one assigned

Labels

area: bug $$ bug-bounty $$ theme: reactive theme: security $500

Projects

None yet

Milestone

7.8.1

Development

Successfully merging a pull request may close this issue.

use conditions instead of criteria as workaround
atomfrede/generator-jhipster

9 participants