Foreman - Refactor #23300

Do not use string interpolation when composing SQL queries.

04/17/2018 02:27 PM - Martin Povolny

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Rails		
Target version:			
Difficulty:		**Fixed in Releases:**	3.2.0
Triaged:	No	**Found in Releases:**	
Bugzilla link:		**Red Hat JIRA:**	
Pull request:	https://github.com/theforeman/foreman/pull/8979		

Description

Using string interpolation when composing SQL queries is just one step away from creating a security issue. It's against the Rails best practices to do so. Doing so actually results into Brakeman complaining loudly.

Task: replace string interpolation with use of parameterization of queries and/or AREL.

Related issues:

Related to Foreman - Tracker #21834: Rails 5.2 upgrade tasks	**Closed**
Related to Foreman - Refactor #23234: remove friendly_id <5.0 workarounds	**Closed**
Related to Foreman - Tracker #24837: Rails 6.0 Tracker	**Closed**
Related to Foreman - Refactor #29520: Wrap sql in Arel.sql() where needed	**Closed**
Blocks Foreman - Tracker #28570: Rails 6.1 Tracker	**Closed**

Associated revisions

Revision 09c865a3 - 01/10/2022 10:43 AM - Leos Stejskal

Fixes #23300 - Brakeman SQL injections

Fix all foundings of SQL injections by
Brakeman: "brakeman --test SQL"

History

#1 - 04/18/2018 05:40 AM - Marek Hulán

- Status changed from New to Need more information

Could you share the list of such places? Or is that based on brakeman scan only? Was it just Foreman core or also some plugins that you've scanned?

#2 - 04/18/2018 08:22 PM - Anonymous

Brakeman is there: http://ci.theforeman.org/job/test_brakeman (although that's going to be deleted soon). The Rails 5.2 warnings can be seen in the new deprecations in https://github.com/theforeman/foreman/pull/5428

#3 - 04/19/2018 01:19 PM - Martin Povolny

I started with Brakeman scan and `grep` and with Foreman only and did not spend much time on this yet.

I think that basic checking should be done on regular basis possibly as part of the CI and also for plugins. Brakeman can be used and/or services such as Hakiri (https://hakiri.io/).

I don't have a list of issues. Initial one can be obtained by running Brakeman.

In my opinion as a starting point all issues reported by Brakeman should be fixed or marked as false positives in the Brakeman config file (to be included with Foreman).

#4 - 04/22/2018 01:03 PM - Anonymous

- Related to Tracker #21834: Rails 5.2 upgrade tasks added

#5 - 04/22/2018 01:04 PM - Anonymous

- Tracker changed from Bug to Refactor

#6 - 04/22/2018 01:10 PM - Anonymous

- Related to Refactor #23234: remove friendly_id <5.0 workarounds added

#7 - 04/22/2018 01:11 PM - Anonymous

- Pull request https://github.com/theforeman/foreman/pull/5367 added

#8 - 09/06/2018 08:13 PM - Anonymous

- Blocks Tracker #24837: Rails 6.0 Tracker added

#9 - 03/19/2019 03:53 PM - Anonymous

- Status changed from Need more information to New

- Pull request deleted (https://github.com/theforeman/foreman/pull/5367)

#10 - 04/28/2019 08:32 PM - Anonymous

- Related to Bug #26414: Api error when querying LDAP users added

#11 - 12/25/2019 03:40 PM - Anonymous

- Related to deleted (Bug #26414: Api error when querying LDAP users)

#12 - 12/25/2019 03:40 PM - Anonymous

- Blocks deleted (Tracker #24837: Rails 6.0 Tracker)

#13 - 12/25/2019 03:41 PM - Anonymous

- Blocks Tracker #28570: Rails 6.1 Tracker added

#14 - 12/25/2019 03:41 PM - Anonymous

- Related to Tracker #24837: Rails 6.0 Tracker added

#15 - 04/13/2020 03:26 PM - Anonymous

- Related to Refactor #29520: Wrap sql in Arel.sql() where needed added

#16 - 12/08/2021 07:59 AM - The Foreman Bot

- Status changed from New to Ready For Testing

- Pull request https://github.com/theforeman/foreman/pull/8979 added

#17 - 01/10/2022 10:43 AM - The Foreman Bot

- Fixed in Releases 3.2.0 added

#18 - 01/10/2022 11:01 AM - Leos Stejskal

- Status changed from Ready For Testing to Closed

Applied in changeset foreman|09c865a37172d422564afbf7c8d6467e882e3ad5.

#19 - 02/15/2022 01:34 PM - Amit Upadhye

- Category set to Rails