QGIS Application - Bug report #11071
SQL injection on PostGIS layer filtering

2014-08-18 09:09 AM - Carlos Ruiz

Status:	Closed		
Priority:	Normal		
Assignee:			
Category:	Data Provider/PostGIS		
Affected QGIS version:	master	**Regression?:**	No
Operating System:		**Easy fix?:**	No
Pull Request or Patch supplied:	No	**Resolution:**	wontfix
Crashes QGIS or corrupts data:	No	**Copied to github as #:**	19405

Description

Hi to all,

When the version 1.8 was released, I did some tests to inject SQL while filtering a PostGIS layer. I thought that the following releases will fix it, but this issue is still with 2.0, 2.2 and 2.4.

Using QGIS 2.4 I did the following:

1. I've connected to my PostgreSQL database to get a PostGIS layer named rutas_afectacion.
2. I chose to filter the features and entered TRUE; DROP TABLE rutas_afectacion (because I know that the SQL command built will be SELECT * FROM rutas_afectacion WHERE <CONDITION> | [<LOGICAL_OP> | <CONDITION> ...)
3. QGIS throws an error message saying: Sintax error ... LINE 1: ...afectacion" WHERE TRUE; DROP TABLE rutas_afectacion LIMIT 0 .
4. Then it was clear for me that I just have to inject TRUE; DROP TABLE rutas_afectacion; SELECT 1 (I could be more mischievous and try DROP DATABASE instead).
5. Once executed by clicking the "Test" button, QGIS throws an error message saying: relation rutas_afectacion does not exist.

I think security is an important issue when accessing to a database server, so I suggest to evaluate the SQL string with a regular expression which accepts just a query command (SELECT ... FROM ... WHERE ... LIMIT 0 or SELECT ... FROM ... WHERE ...) before testing or executing it, rejecting some DDL commands like ALTER, DROP, GRANT, REVOKE and TRUNCATE.

Cheers

History

#1 - 2014-08-20 02:47 AM - Matthias Kuhn

- Status changed from Open to Feedback

You will have access to the user/password anyway when you are using QGIS to access data. With these credentials you will be able to perform malicious code on the database anyway as far as user permissions allow.

- Is there a situation/possible setup where a user might be able to change the subset string without having access to user credentials?
- Is this an issue on QGIS server (where a user normally does not have access to the user credentials and it can therefore be considered a severe security issue)?

The meaning of this comment is not to say that this should not be fixed, but that with this fix security will most likely not be considerably improved.

#2 - 2014-10-05 09:58 AM - Giovanni Manghi

- Status changed from Feedback to Open
- Affected QGIS version changed from 2.4.0 to master

#3 - 2014-10-07 04:26 AM - Matthias Kuhn
- Status changed from Open to Feedback

Was there a reason to change the state to open?

I think there are two possibilities to change the state from Feedback to something else:

- Feedback provided => Open
- No feedback in a long time => Close

Having something in the state Open with missing information does not help to fix it but makes it harder to close it due to lack of information.

#4 - 2014-10-12 02:06 AM - Giovanni Manghi

Matthias Kuhn wrote:

> *Was there a reason to change the state to open?*
>
> *I think there are two possibilities to change the state from Feedback to something else:*
> - *Feedback provided => Open*
> - *No feedback in a long time => Close*
>
> *Having something in the state Open with missing information does not help to fix it but makes it harder to close it due to lack of information.*

I Matthias, I change the status because I have tested what is described and confirmed that it is indeed an issue.

Then you (developers) can argue that it not worth fixing it, for the reasons you describe, and then close this ticket. Otherwise there is no need for further feedback but then the ticket should stay open, to remind us about it.

#5 - 2014-10-12 08:02 AM - Jürgen Fischer
- Assignee deleted (Jürgen Fischer)
- Target version deleted (Future Release - High Priority)
- Category changed from Data Provider/PostGIS to Data Provider

Giovanni Manghi wrote:

> *I Matthias, I change the status because I have tested what is described and confirmed that it is indeed an issue.*

But the question was why this is an issue. You can only execute statements that you're allowed to and you can't execute anything more via sql injection as you can via db manager or any other connection using the available credentials.

#6 - 2014-10-12 08:07 AM - Giovanni Manghi

> *But the question was why this is an issue. You can only execute statements that you're allowed to and you can't execute anything more via sql injection as you can via db manager or any other connection using the available credentials.*

Yes I understand (and agree) 100%, but the point is that the feedback tag was not necessary because there is nothing more to add or to know. If the developers consider this an issue then it should be left open, if not then it should be closed as won't fix.

#7 - 2014-10-12 08:09 AM - Jürgen Fischer

Giovanni Manghi wrote:

> *Yes I understand (and agree) 100%, but the point is that the feedback tag was not necessary because there is nothing more to add or to know. If the developers consider this an issue then it should be left open, if not then it should be closed as won't fix.*

Um, but both questions Matthias raised were not answered.

#8 - 2014-10-26 03:36 PM - Jürgen Fischer

- Category changed from Data Provider to Data Provider/PostGIS

#9 - 2015-05-22 12:55 AM - Giovanni Manghi

- Resolution set to wontfix

- Status changed from Feedback to Closed

closing for lack of feedback.