

# ✓ SQL injection in SemanticDrilldown (CVE-2022-29904)

[Actions](#)

✓ Closed, Resolved

🌐 Public

SECURITY

## Assigned To

Yaron\_Koren

## Authored By

Seb35

2022-04-19 19:08:17 (UTC+0)

## Tags

🔒 Security

📁 MediaWiki-extensions-SemanticDrilldown (Backlog)

🔒 Vuln-Inject (Tracked)

🔒 SecTeam-Processed (Completed)

## Referenced Files

None

## Subscribers

Aklapper

NavidBoyWiki

Seb35

Yaron\_Koren

## Description

In SemanticDrilldown current master **044614d** there is a SQL injection through:

- the GET parameter "\_cat" in the special page Special:BrowseData
- read in class `SDBrowseData` [here](#), passed to the object `SDBrowseDataPage` [here](#)
- saved in property `category` in object `SDBrowseDataPage` [here](#)
- transmitted in `SDBrowseData::printAppliedFilterLine()` to `SDAppliedFilter::getAllOrValues()` [here](#)
- injected in the SQL request in `SDAppliedFilter::getAllOrValues()` [here](#)

The method `DBrowseData::printAppliedFilterLine()` is used to display the SMW values when a SMW property value is selected.

An example of URL is `/Special:BrowseData?SomeProperty=SomeValue&_cat=SomeCategory'_OR_'='`. The category `SomeCategory'_OR_'='` has to exist on the wiki and the result is that the WHERE is bypassed and more values than requested are displayed.

Possibly more harmful SQL queries could be created, but it is limited by existing escaping `'_'`  $\rightarrow$  `' '` (preventing use of all columns and tables containing an underscore) and the two remaining lines in the original SQL query (preventing easy use of SQL comments `--` since these two lines must be integrated in some SQL request to avoid a global SQL error).

I found this SQLi with [phan-taint-check-plugin](#).

Affiliation: Wiki Valley






## Details

### Risk Rating

Low

### Author Affiliation

Wikimedia Communities

Project	Subject
 <a href="#">mediawiki/extensions/SemanticDrilldown</a>	<a href="#">Improve quoting in DB query</a>
 <a href="#">mediawiki/extensions/SemanticDrilldown</a>	<a href="#">Improve quoting in DB query</a>
 <a href="#">mediawiki/extensions/SemanticDrilldown</a>	<a href="#">Improve quoting in DB query</a>
 <a href="#">mediawiki/extensions/SemanticDrilldown</a>	<a href="#">Improve quoting in DB query</a>
 <a href="#">mediawiki/extensions/SemanticDrilldown</a>	<a href="#">Improve quoting in DB query</a>
<a href="#">Customize query in gerit</a>	

## Related Objects


### Mentions

#### Mentioned In

~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2)~~

#### Mentioned Here

[rESDD044614d60c30: Localisation updates from https://translatewiki.net.](#)

 **Seb35** created this task. 2022-04-19 19:08:17 (UTC+0)

  Restricted Application added a subscriber: **Aklapper**. · View Herald Transcript 2022-04-19 19:08:18 (UTC+0)

 **Seb35** added a project: **MediaWiki-extensions-SemanticDrilldown**. 2022-04-19 19:08:51 (UTC+0)

Seb35 added a comment. 2022-04-19 19:14:56 (UTC+0)

Here is a patch as a Git commit:

```
commit dda8ac5ca2d8f6ff595f1a2e641bda4c2057bfc4
tree 7492d30ceab679b68d72c026ecbdc7987085202
parent 044614d60c30cbbd7d3882f836905796bc1ade06
author Sébastien Beyou <sebastien.beyou@wiki-valley.com> 1650395410 +0200
committer Sébastien Beyou <sebastien.beyou@wiki-valley.com> 1650395410 +0200
```

SECURITY: SQL injection

Through the URL GET parameter `_cat`. The exploitation is limited by:

- \* the fact it must be a category title: in particular `_` are replaced by spaces, preventing use of most SQL tables and columns having a `_`;
- \* the category title must exist, hence limited to editors;
- \* there are next lines in the SQL request, preventing comment-type SQLi.

Bug: T306463

Change-Id: Ia4d588b91e71d41e594e23684b1ec24ba1f1db0c

```
diff --git includes/SDAppliedFilter.php includes/SDAppliedFilter.php
index dc7c7c5..689fdc6 100644
--- includes/SDAppliedFilter.php
+++ includes/SDAppliedFilter.php
@@ -197,6 +197,7 @@ class SDAppliedFilter {
     $property_value = $this->filter->escaped_property;
     $dbr = wfGetDB( DB_REPLICA );
     $property_table_name = $dbr->tableName( $this->filter->getTableName() );
+    $category = $dbr->addQuotes( $category );
     if ( $this->filter->property_type != 'date' ) {
         $value_field = $this->filter->getValueField();
     } else {
@@ -226,7 +227,7 @@ class SDAppliedFilter {
     JOIN $smwIDs cat_ids ON insts.o_id = cat_ids.smw_id
     WHERE p_ids.smw_title = '$property_value'
     AND cat_ids.smw_namespace = $cat_ns
-    AND cat_ids.smw_title = '$category'
+    AND cat_ids.smw_title = $category
     GROUP BY $value_field
     ORDER BY $value_field";
     $res = $dbr->query( $sql );
```

Aklapper added a project: **Vuln-Inject**. 2022-04-20 07:25:05 (UTC+0)







Yaron\_Koren closed this task as *Resolved*. 2022-04-22 15:03:51 (UTC+0)



Yaron\_Koren claimed this task.

Thanks for this patch. I added this in here, so I believe the problem is fixed now:

<https://gerrit.wikimedia.org/r/c/mediawiki/extensions/SemanticDrilldown/+785213>

sbassett triaged this task as *Low* priority. 2022-04-25 20:06:21 (UTC+0)



-  **sbassett** mentioned this in ~~T305209: Write and send supplementary release announcement for extensions and skins with security patches (1.35.7/1.37.3/1.38.2).~~
-  **sbassett** changed Author Affiliation from Other (Please specify in description) to Wikimedia Communities.
-  **sbassett** edited projects, added **SecTeam-Processed**; removed **Security-Team**.
-  **sbassett** changed the visibility from "**Custom Policy**" to "Public (No Login Required)".
-  **sbassett** changed the edit policy from "**Custom Policy**" to "All Users".
-  **sbassett** changed Risk Rating from N/A to Low.

 **gerritbot** added a comment. 2022-04-27 20:44:35 (UTC+0) 


Change 786425 had a related patch set uploaded (by RhinosF1; author: Yaron Koren):  
[mediawiki/extensions/SemanticDrilldown@REL1\_38] Improve quoting in DB query  
<https://gerrit.wikimedia.org/r/786425>

 **gerritbot** added a project: **Patch-For-Review**. 2022-04-27 20:44:36 (UTC+0) 

Change 787086 had a related patch set uploaded (by RhinosF1; author: Yaron Koren):  
[mediawiki/extensions/SemanticDrilldown@REL1\_37] Improve quoting in DB query  
<https://gerrit.wikimedia.org/r/787086>

 **gerritbot** added a comment. 2022-04-27 20:45:18 (UTC+0) 

Change 787087 had a related patch set uploaded (by RhinosF1; author: Yaron Koren):  
[mediawiki/extensions/SemanticDrilldown@REL1\_36] Improve quoting in DB query  
<https://gerrit.wikimedia.org/r/787087>

 **gerritbot** added a comment. 2022-04-27 20:54:38 (UTC+0) 



Change 787088 had a related patch set uploaded (by RhinosF1; author: Yaron Koren):  
[mediawiki/extensions/SemanticDrilldown@REL1\_35] Improve quoting in DB query  
<https://gerrit.wikimedia.org/r/787088>

 **gerritbot** added a comment. 2022-04-27 20:56:49 (UTC+0) 

Change 786425 **merged** by jenkins-bot:

[mediawiki/extensions/SemanticDrilldown@REL1\_38] Improve quoting in DB query



<https://gerrit.wikimedia.org/r/786425>

 **gerritbot** added a comment. 2022-04-27 20:57:59 (UTC+0) 

Change 787086 **merged** by jenkins-bot:

[mediawiki/extensions/SemanticDrilldown@REL1\_37] Improve quoting in DB query



<https://gerrit.wikimedia.org/r/787086>

 **gerritbot** added a comment. 2022-04-27 20:58:18 (UTC+0) 

Change 787087 **merged** by jenkins-bot:

[mediawiki/extensions/SemanticDrilldown@REL1\_36] Improve quoting in DB query

<https://gerrit.wikimedia.org/r/787087>


 **gerritbot** added a comment. 2022-04-27 20:59:53 (UTC+0) 

Change 787088 **merged** by jenkins-bot:

[mediawiki/extensions/SemanticDrilldown@REL1\_35] Improve quoting in DB query

<https://gerrit.wikimedia.org/r/787088>

 **Maintenance\_bot** removed a project: **Patch-For-Review**. 2022-04-27 21:31:35 (UTC+0)

 **Mstyles** renamed this task from *SQL injection in SemanticDrilldown* to *SQL injection in SemanticDrilldown (CVE-2022-29904)*. 2022-07-06 17:52:55 (UTC+0)