

📁 [beekeeper-studio](#) / [beekeeper-studio](#) Public

[Code](#)

[Issues](#) 444

[Pull requests](#) 4

[Discussions](#)

[Actions](#)

[Projects](#)

[Security](#)

[Insights](#)

BUG: Beekeeper Remote Code Execution via XSS #1393

New issue

[Jump to bottom](#)

🔒 Closed

[goseungduk](#) opened this issue Oct 8, 2022 · 2 comments · Fixed by [#1438](#)

[goseungduk](#) commented Oct 8, 2022 • edited ▾

...

Author: [bob11.devvranger@gmail.com](#)

Date: 2022-10-07

OS: Windows, Linux, MacOS

Beekeeper Studio Version: 3.6.6

DB Type&Version: MySQL 5.7 and 8.0 Also

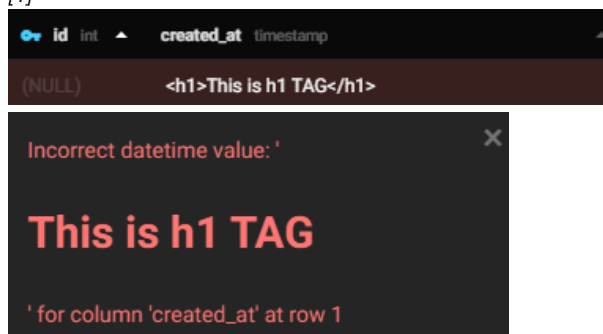
Summary

It has been possible to trigger remote code execution via Beekeeper's **Modal Container**.

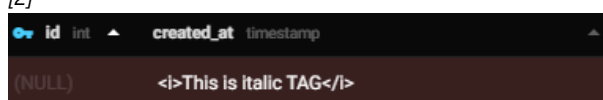
Description

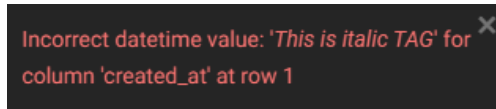
Beekeeper has the modal container which indicates the user's interaction is valid and due to a lack of sanitization of the modal contents, It has an XSS vulnerability like this:

[1]

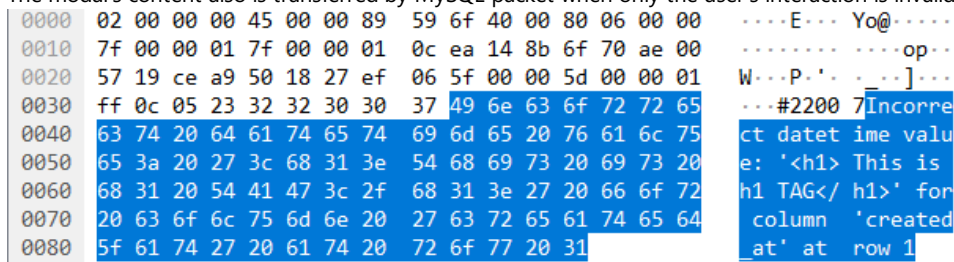


[2]





The modal's content also is transferred by MySQL packet when only the user's interaction is invalid like this:



So, Taking advantage of the report in [CVE-2022-26174](#), it has been possible Remote Code Execution via Modal Container.

In this case, I made the fake MySQL server which spoofs user's modal output when the user puts some data in a table.

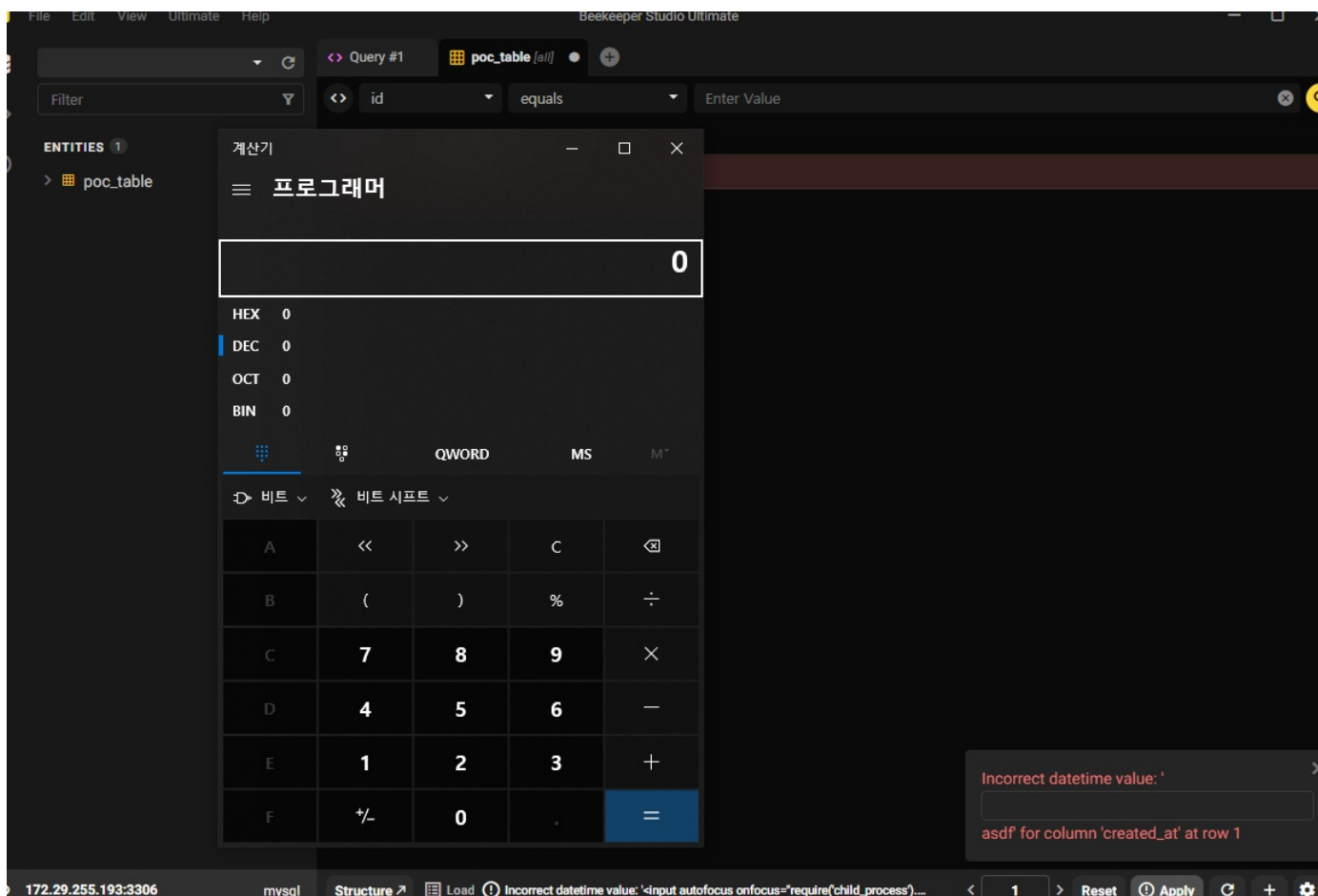
This is my sample fake SQL server : [poc.py](#)

You can see this poc video that fake SQL server triggers RCE via Beekeeper.

[PoC_Video](#)

In this video, I used this XSS script `<input type="text" onfocus="require('child_process').execSync('calc.exe')" autofocus />` for modal error output and any input that user passes is replaced by that XSS script and re-passed to the user.

Finally, Malicious Code is triggered in the user's PC and is continued until the modal is inactivated.



What's More?


- Not only data inserting functions but also any functions which use error modal(e.g. create table), It seems that we can trigger RCE too.

Temporary Fake SQL Server

146.56.129.188:3306

- You can do these poc in this fake SQL server with Beekeeper
- If you have any problems, contact me via a42873410@gmail.com or bob11.devrranger@gmail.com
- Thank You :)



 [goseungduk](#) changed the title ~~BUG: Beekeeper RCE via XSS~~ **BUG: Beekeeper Remote Code Execution via XSS** [Oct 25, 2022](#)
rathboma commented Nov 21, 2022 ...

Thanks. Looking into this. Will get fixed asap




[rathboma](#) added a commit that referenced this issue [Nov 21, 2022](#)



[Fix #1393 - XSS and code injection vulnerability](#) ...

d7cc5fd



 [rathboma](#) mentioned this issue [Nov 21, 2022](#)


[Fix #1393 3.7.10 hotfix with xss fix #1438](#)

🔗 Merged

rathboma commented Nov 21, 2022 ...

Fixed in 3.7.10



 [rathboma](#) closed this as [completed Nov 21, 2022](#)



[rathboma](#) added a commit that referenced this issue [Nov 21, 2022](#)



[Merge pull request #1438 from beekeeper-studio/3.7.9-hotfix](#) ...

219ec63

[Sign up for free](#)

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

🔗 [Fix #1393 3.7.10 hotfix with xss fix](#)
[beekeeper-studio/beekeeper-studio](#)

2 participants



[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact GitHub](#)

[Pricing](#)

[API](#)

[Training](#)

[Blog](#)

[About](#)