# File an Issue

If you have a question rather than an issue, please post it to the [Hangfire Stack

Overflow tag](http://stackoverflow.com/questions/tagged/hangfire). For non-security related bugs please log a new issue:

1. Search the [issue tracker](https://github.com/HangfireIO/Hangfire/issues) for similar issues.

2. Specify the \*\*version\*\* of `Hangfire.Core` package in which the bug was occurred.

3. Specify the \*\*storage\*\* package (e.g. `Hangfire.SqlServer`) you are using and its exact version.

4. Specify the \*\*configuration\*\* logic for Hangfire.

5. Specify all the custom job \*\*filters\*\* if any, and post their source code.

6. Describe the problem and your environment in detail (i.e. what happened and what you expected would happen).

ProTip!

\* Include screenshots from Dashboard UI, to allow us to see the same

problem. You can simply use <kbd>Print Screen</kbd>, then <kbd>Ctrl + V</kbd> directly

into the comment window on GitHub.

\* Include log messages, written by Hangfire when a problem occurred. Don't forget to tell your logger to dump all the exception details.

\* Include stack trace dump, if your background processing stucked. You can use

[`stdump`](https://github.com/odinserj/stdump) utility to get them either from a minidump file,

or from a running process without interrupting it: `stdump w3wp > stacktrace.txt`

Hints

\* Use [syntax highlighting](https://help.github.com/articles/creating-and-highlighting-code-blocks/#syntax-highlighting) for your C#, SQL, etc. code blocks.

\* Use [fenced code blocks](https://help.github.com/articles/creating-and-highlighting-code-blocks/#fenced-code-blocks) for exception details.

# Reporting security issues

In order to give the community time to respond and upgrade we strongly urge you report all security issues privately. Please email us at [security@hangfire.io](mailto:security@hangfire.io) with details and we will respond ASAP. Security issues always take precedence over bug fixes and feature work. We can and do mark releases as "urgent" if they contain serious security fixes.