Iframes

Host Iframe Control

By default BookStack will only allow itself to be embedded within iframes on the same domain as you're hosting on. This is done through a CSP: frame-ancestors header. You can add additional trusted hosts by setting a `ALLOWED_IFRAME_HOSTS` option in your `.env` file like the example below:

```
# Adding a single host
ALLOWED_IFRAME_HOSTS="https://example.com"

# Multiple hosts can be separated with a space
ALLOWED_IFRAME_HOSTS="https://a.example.com https://b.example.com"
```

Note: when this option is used, all cookies will served with `SameSite=None` (info) set so that a user session can persist within the iframe.

Iframe Source Control

By default BookStack will only allow certain other hosts to be used as `src` values for embedded iframe/frame content within the application. This is done through a CSP: frame-src header. You can configure the list of trusted sources by setting a `ALLOWED_IFRAME_SOURCES` option in your `.env` file like the examples below:

```
# Adding a single host
ALLOWED_IFRAME_SOURCES="https://example.com
"

# Multiple hosts can be separated with a
space
ALLOWED_IFRAME_SOURCES="https://a.example.c
om https://b.example.com"

# Allow all sources
# This opens vulnerability risk and should
only be done in secure & trusted
environments.
ALLOWED_IFRAME_SOURCES="*"
```

By default this option is configured as follows:

```
ALLOWED_IFRAME_SOURCES="https://*.draw.io
https://*.youtube.com https://*.youtube-
nocookie.com https://*.vimeo.com"
```

Note: The source of ‘self’ will always be automatically added to this CSP rule. In addition, the host used for the diagrams.net integration (If enabled) will be automatically appended to the lists of hosts.

Revision #1
Created 2025-07-19 20:29:30 UTC by Orientación
Updated 2025-07-19 20:32:14 UTC by Orientación