BookStack

Search site

Platform

Features

An overview of the core features of BookStack

Demo

Give BookStack a test drive on our demo instance

Documentation

Guidance for managing and using BookStack

Our Blog

Get the latest project news from our blog

Support

Documentation

Get support from our user and admin documentation

Support Plans

See our range of support plans for BookStack

Donate

Provide financial support to the project

Video Guides

Watch our video guides on YouTube

GitHub Issues

Find or report issues on the GitHub project

Community

GitHub

Star the project on GitHub and follow us

Discord

Chat with the development team and other users

Twitter

See updates and shout us out on Twitter

YouTube

Watch and comment on our YouTube videos

Reddit

Join our community on the BookStack subreddit

Beta Security Release v0.30.4

Dan Brown posted on the 31st of October 2020

XSS and user-injected auto-redirect vulnerabilities have been found within the page content & attachment components of BookStack which BookStack v0.30.4 looks to address. These are primarily a concern if untrusted users can edit content on your BookStack instance.

- Update instructions
- GitHub release page

Impact

1. A user with permissions to edit a page could insert JavaScript code through the use of `javascript:` URIs within a link or form which would run, within the context of the current page, when clicked or submitted.
2. A user with permissions to edit a page could insert a particular meta tag which could be used to silently redirect users to a alternative location upon visit of a page.
3. A user with permissions to edit a page could add an attached link which would execute untrusted JavaScript code when clicked by a viewer of the page.

Patches

The issues were addressed in BookStack v0.30.4.

Dangerous content may remain in the database. The in-page vulnerabilities will be removed before being displayed on a page but dangerous attachment content will remain if exploited. If you think this could have been exploited you can search for potential cases with the following SQL commands:

```
# XSS within page content:
select * from pages where html like '%javascript:%';

# Auto-redirect within page content:
select * from pages where html like '%<meta%';

# XSS in page link attachments:
select a.name as attachment_name, p.name as page_name, p.id as page_id from attachments a l
```

Workarounds

Page edit permissions could be limited to only those that are trusted until you can upgrade although this will not address existing exploitation of this vulnerability.

References

- BookStack Beta v0.30.4
- GitHub Security Page - XSS/Redirect in Page Content
- GitHub Security Page - XSS in Page Attachment

Attribution

- Thanks to @PercussiveElbow for the discovery, reporting, patching and testing of the page-content vulnerabilities.
- Thanks to Yassine ABOUKIR (https://twitter.com/yassineaboukir/) for the discovery and reporting of the page attachment vulnerability.

More Information

If you have any questions or comments about this advisory:

- Open an issue in the BookStack GitHub repository.
- Ask on the BookStack Discord chat.
- Follow the BookStack Security Advice to contact someone privately.

Header Image Credits: Photo by marcos mayer on Unsplash

Subscribe to Updates

There are two lists you can sign-up to for updates, A general news & updates list, sent on a weekly basis, and a security alerts list that's sent when new security updates are available.

News and Updates | Security Alerts

Want to let me know what you think of BookStack or this post?
You can find me on twitter @ssddanbrown or on the BookStack Discord server.
You can open a suggestion or issue on GitHub.

Latest Posts

BookStack Release v22.11
30 Nov 2022

BookStack Release v22.10
21 Oct 2022

Reaching 10k GitHub Stars & A look at first sharing BookStack
15 Sep 2022

BookStack Release v22.09
8 Sep 2022

A Look at Some Interesting Documentation Methods
25 Aug 2022

BookStack Security Release v22.07.3
11 Aug 2022

BookStack Release v22.07
28 Jul 2022

Seven Years of BookStack
12 Jul 2022

Documentation

Our Features

View the Demo

Read our Blog

Donate

Information

A Confluence Alternative

Open Source Documentation Software

Our Support Services

Github

Discord

Twitter

YouTube

Reddit