

Updating BookStack



- [Version Specific Instructions](#)
 - [Updating to v24.05.1 or higher](#)
 - [Updating to v24.05 or higher](#)
 - [Updating to v24.02 or higher](#)
 - [Updating to v23.12.3 or higher](#)
 - [Updating to v23.12 or higher](#)
 - [Updating to v23.10.3 or higher](#)
 - [Updating to v23.10 or higher](#)
 - [Updating to v23.08 or higher](#)
 - [Updating to v23.06.2 or higher](#)
 - [Updating to v23.06.1 or higher](#)
 - [Updating to v23.06 or higher](#)
 - [Updating to v23.05 or higher](#)
 - [Updating to v23.02 or higher](#)
 - [Updating to v23.01.1 or higher](#)
 - [Updating to v23.01 or higher](#)
 - [Updating to v22.10 or higher](#)
 - [Updating to v22.09 or higher](#)
 - [Updating to v22.07.3 or higher](#)
 - [Updating to v22.06 or higher](#)
 - [Updating to v22.04 or higher](#)
 - [Updating to v22.03 or higher](#)
 - [Updating to v22.02.3 or higher](#)
 - [Updating to v22.02 or higher](#)
 - [Updating to v21.12.3 or higher](#)
 - [Updating to v21.12.1 or higher](#)
 - [Updating to v21.11.3 or higher](#)
 - [Updating to v21.11.2 or higher](#)

- [Updating to v21.11 or higher](#)
- [Updating to v21.10.3 or higher](#)
- [Updating to v21.10.1/v21.10.2 or higher](#)
- [Updating to v21.08.5 or higher](#)
- [Updating to v21.08.2 or higher](#)
- [Updating to v21.08 or higher](#)
- [Updating to v21.04 or higher](#)
- [Updating to v0.31.0 or higher](#)
- [Updating to v0.30.6, v0.30.7 or higher](#)
- [Updating to v0.30.5 or higher](#)
- [Updating to v0.30.4 or higher](#)
- [Updating to v0.30 or higher](#)
- [Updating to v0.29.3 or higher](#)
- [Updating to v0.29.2 or higher](#)
- [Updating to v0.28 or higher](#)
- [Updating to v0.26 or higher](#)
- [Updating to v0.25.3 or higher](#)
- [Updating to v0.25.2 or higher](#)
- [Updating to v0.25 or higher](#)
- [Updating to v0.24 or higher](#)
- [Updating to v0.19 or higher](#)
- [Updating to v0.18 or higher](#)
- [Updating to v0.13 or higher](#)



BookStack is updated regularly. We try our best to keep the platform and upgrade path as stable as possible. The latest release can be found on [GitHub here](#) and detailed information on releases is posted on the [BookStack blog here](#).

Before updating you should back up the database and any file uploads to prevent potential data loss.

Backup and restore documentation can be found [here](#).

Updating is currently done via Git version control. To update BookStack you can run the three following commands in the root directory of the application:

```
git pull origin release
composer install --no-dev
php artisan migrate
```

This first command will update the repository that was created in the installation. The second will install the PHP dependencies using `composer`. The third will then update the database with any required changes.

In addition, Clearing the system caches is also recommended:

```
php artisan cache:clear
php artisan config:clear
php artisan view:clear
```

Check the below [Version Specific Instructions](#) list for the version you are updating to for any additional instructions.

When running update commands, your command line user will need permission to handle the required files and folders in the BookStack installation folder. You can find more details about [required filesystem permissions here](#).

Version Specific Instructions

The below lists things you may need to be aware of when upgrading to a newer version of BookStack. This is primarily a list of breaking changes & security notices. Details of updates can be found on [our blog](#) or via the [GitHub releases page](#).

Updating to v24.05.1 or higher

Security - v24.05.1 adds extra rate-limiting to some forms that are accessible without authentication, while also implementing changes to prevent methods that could be used to indicate if specific user emails exist in the system.

Updating to v24.05 or higher

PHP Version Requirement Change - The minimum supported PHP version has changed from PHP 8.0.2 to PHP 8.1 in this release. Please see our ["Updating PHP & Composer" documentation](#)

[page](#) for guidance on updating PHP.

Composer Version Requirement Change - The minimum supported composer version has changed from v2.0 to v2.2 in this release. Please see our ["Updating PHP & Composer" documentation page](#) for guidance on updating Composer.

Page Content - Text links in page content will now be underlined by default for accessibility. Refer to [the release blogpost](#) for an simple customization to override & revert this if desired.

PDF Exports - The `WKHTMLTOPDF` option is now considered deprecated, with the alternative being the newly added `EXPORT_PDF_COMMAND` which is detailed in [our documentation here](#). The `WKHTMLTOPDF` option will though remain supported for a number of feature releases though to avoid unexpected breaking changes.

OIDC Authentication - The OIDC "userinfo" endpoint may now be called in very rare scenarios where not all expected claims were being properly provided in the user ID Token, which could alter the details used for new users on access, and the groups obtained for user group/role sync, but only in edge case scenarios where functionality was not matching configuration before the update.

LDAP Authentication - The `LDAP_USER_FILTER` BookStack option now uses `{user}` as a placeholder instead of `${user}` by default. The older `${user}` placeholder format is still supported but you may want to use the new format instead. This should not cause any issues on existing instances, unless `{user}` was used as a literal part of your user filter which would be very unlikely.

Updating to v24.02 or higher

Comments - The ability to use markdown content in comments has been removed in this release, replaced by a WYSIWYG editor. Markdown in comments was a fairly hidden feature though so was not commonly utilised. Existing markdown comments will remain although formatting may be lost if old markdown comments are edited.

Commands - The "Regenerate Comment Content" command has been removed in this release since this action is now redundant.

OIDC Authentication - Proof Key for Code Exchange (PKCE) support has been added to BookStack OIDC authentication. This should not affect existing OIDC use but you may want to enforce PKCE to be required for BookStack on your authentication system, if supported, for extra security.

Updating to v23.12.3 or higher

Security - v23.12.3 addresses a vulnerability in PDF generation that could be exploited, by users with the ability to create/edit/update page content, to perform blind server-side-request forgery.

Updating to v23.12 or higher

Page Includes - The way page include content is fetched & merged has changed significantly in this release, which in some cases may alter how included content appears on the page.

Updating to v23.10.3 or higher

Security - v23.10.3 addresses a vulnerability relating to image handling which could be exploited, by users with the ability to create/edit/update page content, to perform server-side requests or read the contents of files on the server system. Additionally, this update addresses a lack of permission check in some image creation actions.

Updating to v23.10 or higher

User Detail/Preference Changes - Many of the URLs, paths and interfaces for user-self management have changed in this release. You may need to update any documentation or user guidance you may have surrounding users updating their own details or preferences.

Updating to v23.08 or higher

Security - Webhooks - In scenarios where admin users are not trusted, webhooks could potentially be used maliciously. This update adds a control for such functionality. Please read [our documentation for the new `ALLOWED\_SSR\_HOSTS` option](#) if this may be a concern for your instance.

Updating to v23.06.2 or higher

Shelf Create Permissions - If you upgraded specifically to v23.06 or v23.06.1, then create permissions for bookshelves would have been removed upon upgrade. If you made use of these via the "Copy Permissions to Books" action, or CLI command, then you will need to re-apply these permissions where required. If you jumped right over v23.06 and v23.06.1, then no permissions were removed.

Updating to v23.06.1 or higher

Email Configuration (TLS) - Due to issues experienced in v23.06, `MAIL_ENCRYPTION=ssl` or `MAIL_ENCRYPTION=tls` will now simply ensure that TLS or STARTTLS are used, rather than forcing full TLS to be used. Our [email documentation](#) has been updated to reflect this.

Updating to v23.06 or higher

Email Configuration - If you've configured mail with `MAIL_ENCRYPTION=ssl` it's advised to test sending (via the button in "Settings > Maintenance") after updating to v23.06 since support for SSL has been dropped for email sending, but we instead now force TLS to be required when this option is set. - *Note - this was amended further in v23.06.1 ([see above](#))*

Font Customization - The technique for customizing fonts has changed to be simpler, less fragile and more flexible. If customizing fonts it's advised to update to the new method as shown in our updated documentation on [changing fonts](#).

Guest User Account - Previously custom roles could be given to the "Guest" user account but permissions for those roles would not fully apply. That's been changed in v23.06 so additional role permissions fully apply but, as a precaution to prevent unexpected additional grant of permissions upon upgrade, any additional roles assigned to the "Guest" user will be removed upon update migration. If needed, simply re-assign any desired custom guest user roles after updating.

Updating to v23.05 or higher

Page Include Tags - Nesting is now allowed for [include tags](#), up to 3 levels of depth. You may now see more content loaded for pages which previously had unparsed nested include tags.

SAML2 - Single LogOut (SLO) requests will now include a "session_index" for the current user. This technically brings BookStack's implementation closer to the spec, and is not expected to cause issues, but if using SLO it may be wise to check your identity provider behavior remains the same as before during logout.

Custom Code Block Themes - Due to a change of library, the method of defining custom codeblock themes has significantly changed, and "window.CodeTheme" code is no longer used. Refer to our ["Changing Code Block Themes"](#) documentation for further information.

Editor Event - editor-markdown::setup - This event no longer contains "codeMirrorInstance" in the event data. It instead has a "cmEditorView" property. [See the event docs for more details](#).

Editor Event - editor-markdown-cm::pre-init - This event has been renamed to "editor-markdown-cm6::pre-init" and no longer contains "config" in the event data. It instead has a "editorViewConfig" property. [See the event docs for more details](#).

Upload Timeouts - The use of "window.uploadTimeout" has been removed as a way to control upload timeouts. This would previously only be used in certain cases. Instead, if required, timeouts can usually be enforced at the web-server level.

Updating to v23.02 or higher

PHP Version Requirement Change - The minimum required version of PHP has changed from 7.4 to 8.0.2. This should not be a concern for those that are using common containers. Installations via our Ubuntu 22.04 install script are already using PHP 8.1 and therefore they don't need to be upgraded at this time.

For installs that have used our Ubuntu 18.04 and Ubuntu 20.04 install scripts, PHP can generally be upgraded to 8.2 using the below commands:

Warning: If you run other applications on this machine, PHP applications in particular, then those may also be affected by these changes.

```
sudo apt update
sudo apt install software-properties-common
sudo add-apt-repository ppa:ondrej/php
sudo apt update
sudo apt install -y php8.2 php8.2-curl php8.2-mbstring php8.2-ldap php8.2-xml php8.2-zip
php8.2-gd php8.2-mysql libapache2-mod-php8.2
sudo a2dismod php7.2 php7.4 php7.3 php8.0 php8.1
sudo a2enmod php8.2
sudo systemctl restart apache2
```

You may also need to [update composer](#) to be compatible with PHP 8.2.

Logical Theme System Event Change - The `commonmark_environment_configure` event argument and return type has changed. Please [see the event definition](#) to understand the new types.

Updating to v23.01.1 or higher

Security - v23.01.1 patches a vulnerability in PDF generation that could be used to make server-side requests or run potential other PHP code.

Updating to v23.01 or higher

Permission Changes - There have been changes to the permission system which can affect how permissions apply and therefore could lead to changes in provided abilities upon update. This is only really relevant to complex permission scenarios that have only been possible since BookStack v22.10. Please see the [Permission System Changes section of the v23.01 blogpost](#) for more details on this.

Database Upgrade Time - Changes to the permission system have required permissions to be regenerated upon update. Due to this, the `php artisan migrate` upgrade step may take extra time to run, especially where there's a lot of content and/or roles in the system.

Updating to v22.10 or higher

Permission Management Changes - The interface and logic for managing shelf, book, chapter & page permissions has changed significantly in this release. The following should be noted:

- Content permissions that were not active (where the "Enable Custom Permissions" checkbox was unchecked) will be removed upon upgrade to v22.10.

- Content permission role entries, that had no permissions provided, will not be reflected/shown as a row in the permissions interface immediately upon upgrade. Instead such cases will be reflected via the "Everyone Else" permission entry being active, in a non-inheriting state, with no permissions set.
- There should be no functional change to active permissions upon upgrade. Care has been taken to ensure existing permissions are migrated so that access control remains the same as pre-upgrade.

Updating to v22.09 or higher

Revision Visibility - This update fixes a permission disparity with revisions. Revision content has always been accessible to those with page-view permissions, but the links to the revisions list previously required page-edit permission to show. This has been aligned, which may mean page revision links may now show to those that did not previously see them.

Revision Limit Change - The default, per-page, revision limit has been doubled from 50 to 100, to account for new system-content updates that may occur. If desired, you can [configure this to a custom value](#).

Reference Index - New features have been added to track links between content in BookStack, which uses an internal reference index. Upon upgrade from an older BookStack version, this index will need to be rebuilt. This can be done with the ["Regenerate References" command](#) or via the "Regenerate References" maintenance action within BookStack.

Updating to v22.07.3 or higher

Security - v22.07.3 added a "Content Security" section to the API docs and [BookStack documentation](#) with security considerations for using BookStack content externally. Read this new section if you are using BookStack user content externally.

Updating to v22.06 or higher

SAML/LDAP Group Mapping - Within the "External Authentication Ids" field for a BookStack role, a backslash followed by a comma (`\,`) will now cause the comma to be treated as a literal comma within the mapping name, instead of acting as a value separator to define multiple mappings.

Updating to v22.04 or higher

Database Changes - This release makes some significant changes to data within the database which may cause the update to take a little longer than usual to run. Please give the update extra time to complete.

REST API Page Create/Update Changes - Create & update page requests now have the potential to change the current editor type for that page, depending on the content type sent in the

request, if the API user has permission to change the page editor.

URL Handling - The way we handle URLs has changed this release to hopefully address some issues in specific scenarios. These changes have been tested and should not affect existing working environments but there's an increased risk this release for setups with more complex URL handling. Please [raise an issue](#) or jump into our Discord server if you have any issues with URLs after upgrading.

Updating to v22.03 or higher

Webhook Data Changes - Properties found at the `related_item -> created_by/updated_by/owned_by` path of the webhook data will now be an object instead of an ID integer. If you were using these ids you'd now need to access them within the relevant objects. (For example `related_item.created_by.id`).

Updating to v22.02.3 or higher

Security - v22.02.3 adds controls to limit external/iframe content on BookStack pages to prevent potential malicious sources being used. See [the added "Iframe Source Control" section on our security page](#) for more detail regarding the added controls.

Updating to v22.02 or higher

PHP Version Requirement Change - The minimum required version of PHP has changed from 7.3 to 7.4. This should not be a concern for those that are using common containers or for those that have installed using our install scripts.

Updating to v21.12.3 or higher

Composer Version Requirement Change - Composer v2.0 or greater is now required to install or update BookStack. See the ["Updating Composer"](#) section of this page below.

Updating to v21.12.1 or higher

Security - v21.12.1 better enforces permissions on book-sort & chapter-move operations to address scenarios where content could be moved to non-permissible locations.

Updating to v21.11.3 or higher

Security - v21.11.3 helps prevent potential discovery and harvesting of user details including name and email address.

Updating to v21.11.2 or higher

Security - v21.11.2 addresses a couple of vulnerabilities relating to API access and page draft related content visibility. If the "Public" role was provided API access then the API could be accessed, in certain scenarios, by non-authenticated users even if the "Allow public access" setting was disabled. In some specific scenarios, content related to page drafts (Such as attachments) could be visible to non-owners (Whom would have permission to view the page if saved as a non-draft at that point).

Updating to v21.11 or higher

API Changes - As of v21.11 any dates in API responses will be formatted as per ISO-8601, with `2019-12-02T20:01:00.283041Z` reflecting an example of this format. You may need to review any of your scripts that utilise dates from API responses.

Upload Limit - System file upload limits are now configured using a `FILE_UPLOAD_SIZE_LIMIT` option in your `.env` file. This value is specified as an integer and represents the max upload size in MegaBytes. This defaults to `50`. This replaces the old `window.uploadLimit` HTML head option that could be set.

Search Index Changes - Changes to search indexing and scoring were made in this release. It's recommended to run `php artisan bookstack:regenerate-search` to ensure a consistent search experience and take advantage of these changes.

Logout Endpoints - Logout endpoints have now changed to be CSRF protected POST endpoints instead of GET endpoints. If you were using these for any external purposes you may now need to implement an alternative workflow.

Updating to v21.10.3 or higher

Security - v21.10.3 looks to address a couple of vulnerabilities within the attachment and image serving mechanisms. The attachment vulnerability could result in users uploading content to be served in a way that can be utilized for phishing. The image serving vulnerability could result in unintended file access within your BookStack storage folder.

Updating to v21.10.1/v21.10.2 or higher

Security - Both v21.10.1 and v21.10.2 were released to address a vulnerability which would allow malicious users, who have permission to update or create pages, to upload content that could then be utilized for phishing or other general malicious intent.

Updating to v21.08.5 or higher

Security - v21.08.5 fixes a vulnerability which would allow malicious users, who have permission to update or create pages, to load content from files stored within the `storage/` or `public/` directories (Such as application logs) via the page HTML export system. In addition, this release adds stricter cache-control headers to http responses while logged in to prevent back navigation to authorized resources after logout.

Updating to v21.08.2 or higher

Security - v21.08.2 fixes a couple of XSS security vulnerability scenarios that could be achieved by malicious users that had permission to edit pages. In addition, v21.08.2 introduces more [CSP rules](#) to help prevent any future XSS vulnerabilities from taking affect. If you've performed some more advanced customizations on your instance, they may need to be altered to work with the built-in CSP system.

Updating to v21.08 or higher

Config & Administration - The introduction of multi-factor authentication brings the first use of encryption in the platform. This uses the `APP_KEY` value in your `.env` file. Ensure you have this stored safely since it would be required if you ever restore/migrate your instance to another system.

Security/Exports - During this release cycle it was highlighted that server-side request forgery could be achieved via the PDF export system. External fetching in the default PDF renderer has been disabled by default. The WKHTMLtoPDF renderer will now not be used if active. Either of these changes can be overridden by setting `ALLOW_UNTRUSTED_SERVER_FETCHING=true` in your `.env` file. This should only be used were only trusted users can create and export content. To support this we've added permissions that allow disabling of exports per role.

Security/Authentication - A slight change was made in relation to how email addresses are confirmed. Email confirmations are now primarily checked at point-of-login rather than being checked on every request. Enabling email confirmation, or email domain restrictions, may no longer take action on unconfirmed users right away in the future.

Updating to v21.04 or higher

Requirements Change - The minimum required PHP version has changed from 7.2 to 7.3. If you originally updated using the Ubuntu 18.04 installation script, the below commands should help you to upgrade to PHP8:

```
sudo add-apt-repository ppa:ondrej/php
sudo apt update
sudo apt install -y php8.0 php8.0-fpm php8.0-curl php8.0-mbstring php8.0-ldap php8.0-xml
php8.0-zip php8.0-gd php8.0-mysql libapache2-mod-php8.0
sudo a2dismod php7.2
sudo a2enmod php8.0
systemctl restart apache2
```

User Reference Changes - References to users in URLs of profile pages, and within search filters, has been changed to be name (Slugified) based instead of ID based. Old links or saved search filters may no longer work as expected.

Updating to v0.31.0 or higher

Requirements Change - The minimum required PHP version has changed from 7.2 to 7.2.5. Additionally, the `Tidy` PHP extension is no longer required.

GitLab Authentication - The `read_user` scope will now be passed and is required on the "Application" setup within GitLab. Not having this scope may lead to errors when users attempt to authenticate via GitLab.

Security & IFrame Usage - By default BookStack will set headers to prevent usage within an iframe. You can set trusted iframe hosts through the `ALLOWED_IFRAME_HOSTS` option in your `.env` file. See the [security page](#) for more information on this option.

Updating to v0.30.6, v0.30.7 or higher

Security - v0.30.6 and v0.30.7 both address issues where page content could be visible to those without permission. If a chapter was visible to a user, but all of its pages were made not visible, then the details of these pages could be visible. Within the BookStack interface, the names of the pages and preview content could be seen. If the parent book was exported then this would include the content of the pages that had been restricted. If using BookStack v0.30.6, then all non-visible page content could be visible in plaintext exports. Please see the blog release pages for more details: [v0.30.6](#), [v0.30.7](#).

Updating to v0.30.5 or higher

Security - v0.30.5 fixes an potential vulnerability where a user with edit permissions could perform server-side requests using the export system. Additionally it was found that, if using standard email/password authentication, the system host URL could be manipulated on the forgot password form which could allow for email phishing attempts. Ensure you have set the `APP_URL` option in your `.env` file to help prevent this. Please see the [blog release page for more details](#).

Updating to v0.30.4 or higher

Security - v0.30.4 fixes a couple of XSS vulnerabilities that could be exploited by untrusted users via page content and page link attachments. Please see the [blog release page for more details](#).

Updating to v0.30 or higher

Security - Possible Privilege Escalation. During the v0.30 release cycle it was advised that current privilege escalation situations are not made clear when applying role permissions. Any user with a "Manage app settings", "Manage users" or "Manage roles & role permissions" system permission assigned to one of their roles could technically alter their own permissions to gain wider access. A clear advisory of these cases has been added in the UI in v0.30 but admins are advised to review which users have these permissions with the above in mind.

LDAP & SAML Group Matching - During the v0.30 release cycle it was found that BookStack roles would be matched to LDAP/SAML groups based upon the role display name, which is expected, but only those roles with a matching "name" value would be considered. This "name" field was redundant, and has now been removed, but it would store a cleaned version the first-set name of the role. All roles will now be considered before being matched on name which may mean that roles which did not sync before, that would have been expected to based on their name, may now start to sync.

Updating to v0.29.3 or higher

Security - v0.29.3 fixes an issue where the names of restricted/private books could be seen by those without permission, if added to a shelf. This issue was introduced in BookStack v0.28.0.

Updating to v0.29.2 or higher

Security - v0.29.2 fixes a XSS security vulnerability in the comment system, that was introduced in BookStack v0.18. Upon updating the command `php artisan bookstack:regenerate-comment-content` should be ran to regenerate comment content to ensure that it is safe.

Updating to v0.28 or higher

Requirements Change - Minimum PHP version has increased from 7.0.5 to 7.2.

If you installed BookStack on Ubuntu 16.04 using the install script, You should be able to upgrade your PHP version to 7.4 by running the following commands:

```
sudo add-apt-repository -y ppa:ondrej/php
sudo apt update
sudo apt install -y php7.4 php7.4-fpm php7.4-curl php7.4-mbstring php7.4-ldap php7.4-tidy
php7.4-xml php7.4-zip php7.4-gd php7.4-mysql
sudo sed -i.bak 's/php7\..0-fpm/php7.4-fpm/' /etc/nginx/sites-available/bookstack
sudo systemctl restart nginx.service
```

Updating to v0.26 or higher

Internet Explorer Support - IE11 Support has now been dropped. Please use a modern browser.

Translations - Since many interfaces and lines of text have been updated, It may take a little while for some translations to catch-up. Expect to see more English text than usual if you're using a non-English language option.

Images - Due to changes how images are handled, as detailed below, some types of images may become inaccessible. Old logo images will be deleted when changed. Unused Book/Shelf cover images & User profile images will become inaccessible after the update so you may want to delete them before upgrade.

Security - On previous versions of BookStack it was possible for users to insert JavaScript via the Markdown editor using `on*` html attributes. These will now be removed on page render unless you have set `ALLOW_CONTENT_SCRIPTS=true`. If untrusted users has access to your BookStack you may want to scan for `<<space_char>>on` in the HTML column of the pages table to identify any malicious intent.

Updating to v0.25.3 or higher

Security - On previous versions of BookStack it was possible to upload PHP files via the image upload endpoints. If you have a BookStack instance where untrusted users could upload image files, and you were using the default file storage option, It would have been possible for the user to access anything that the PHP process could. This would likely include, at minimum, any credentials stored in the `.env` file.

Updating to v0.25.2 or higher

Configuration Change - The `.env` option `REDIS_CLUSTER` has now been removed. If more than one redis server is provided they will automatically be clustered by BookStack.

Updating to v0.25 or higher

Security - During the release cycle for Version v0.25 it was found that page content includes could leak their content as preview text to users that don't have permission to view the included content. It's recommended to re-save any pages that included other page content that's restricted to ensure included text is not shown in page preview text.

Requirements Change - Minimum required version of PHP has changed from 7.0.0 to 7.0.5.

Configuration Change - The `.env` option `GRAVATAR_URL=false` has been replaced by `AVATAR_URL=false`.

Updating to v0.24 or higher

Version v0.24 changes the way the homepage option is stored. After updating, You may need to re-configure this setting.

If updating from a much older BookStack version (Pre v0.20) you may need to update the permission and search indexes. You can do this by running the following commands from your BookStack install folder:

```
php artisan bookstack:regenerate-search
php artisan bookstack:regenerate-permissions
```

Updating to v0.19 or higher

Version v0.19 needs the following requirement change:

- Minimum required version of PHP has changed from 5.6.4 to 7.0.0.

Updating to v0.18 or higher

Version v0.18 introduced a commenting system. After updating you should check the permissions for all roles if you'd like to enable comments for your users.

Updating to v0.13 or higher

The v0.13 release contained some new features and updates which change the requirements of BookStack.

- Minimum required version of PHP has changed from 5.5.9 to 5.6.4. Upgrade your PHP version if below 5.6.4.
- PHP-Tidy extension is now required.
 - On Ubuntu 16.04 this can be installed via `sudo apt install php7.0-tidy`.
 - On Ubuntu 14.04 (Using the default PHP option) this can be installed via `sudo apt-get install php5-tidy`.
- Page attachments will be stored in the `storage/uploads` folder (Unless you use Amazon S3). This folder will be created on update. Ensure your webserver has write permissions for this folder.

👤 #1

👤 feibisi 👤 2026-10-25 09:38:32 UTC

👤 feibisi 👤 2026-10-25 09:38:32 UTC