

BookStack



- [Backup and Restore](#)
- [Commands](#)
- [Installation](#)
- [Security](#)
- [Updating BookStack](#)
- [Customising Visuals](#)

Backup and Restore

“ ” BookStack

While BookStack does not currently have a built-in way to backup and restore content, it can usually be done via the command line with relative ease. The below commands are based on using Ubuntu. If you are using a different operating system you may have to alter these commands to suit.

Backup

There are two types of content you need to backup: Files and database records.

Database

The easiest way to backup the database is via `mysqldump`:

```
# Syntax

## Only specify the `-p` option if the user provided has a password

mysqldump -u {mysql_user} -p {database_name} > {output_file_name}


# Example

mysqldump -u benny bookstack > bookstack.backup.sql
```

If you are using MySQL on Ubuntu, and are using the `root` MySQL user, you will likely have to run the command above with `sudo`:

```
sudo mysqldump -u root bookstack > bookstack.backup.sql
```

The resulting file (`bookstack.backup.sql` in the examples above) will contain all the data from the database you specified. Copy this file to somewhere safe, ideally on a different device.

Files

Below is a list of files and folders containing data you should back up. The paths are shown relative to the root BookStack folder.

- `.env` - File, contains important configuration information.
- `public/uploads` - Folder, contains any uploaded images.
- `storage/uploads` - Folder, contains uploaded page attachments.
- `themes` - Folder, contains any configured [visual/logical themes](#).

Alternatively you could backup up your whole BookStack folder but only the above contain important instance-specific data by default.

The following command will create a compressed archive of the above folders and files:

```
tar -czvf bookstack-files-backup.tar.gz .env public/uploads storage/uploads themes
```

The resulting file (`bookstack-files-backup.tar.gz`) will contain all your file data. Copy this to a safe place, ideally on a different device.

Restore

If you are restoring from scratch follow the [installation](#) instructions first to get a new BookStack instance set-up but **do not run the** `php artisan migrate` **installation step when installing BookStack**. You may need to comment this command out if using an installer script.

If you are using a docker-container-based set-up, restore the database before running the BookStack container. An example of the process using a linuxserver.io-based docker-compose setup can be seen [in our video here](#).

Database

To restore the database you simply need to execute the sql in the output file from the `mysqldump` you performed above. To do this copy your database SQL backup file onto the BookStack or database host machine and run the following:

```
# Syntax

mysql -u {mysql_user} -p {database_name} < {backup_file_name}

## Only specify the -p if the user provided has a password


# Example

mysql -u benny -p bookstack < bookstack.backup.sql
```

```
# If using the root user on Ubuntu you may
# have to run the above with root permissions via sudo:
sudo mysql -u root bookstack < bookstack.backup.sql
```

If you are restoring to a new version of BookStack you will have to run `php artisan migrate` after restore to perform any required updates to the database.

Files

To restore the files you simply need to copy them from the backup archive back to their original locations. If you created a compressed `bookstack-files-backup.tar.gz` archive as per the backup instructions above you can simply copy that file to your BookStack folder then run the following command:

```
tar -xvzf bookstack-files-backup.tar.gz
```

If you get errors during the above command it may be due to permissions. Change permissions so you can write to the restore locations.

After a backup of the files you should reset the permissions to ensure any write-required locations are writable by the server. The locations required for this can be found in the [installation instructions](#).

Configuration (.env File)

During a restore, you may end up merging various configuration options between your old and new instance `.env` files, to get things working for the new environment. For example, it's common to use the old `.env` settings for most things but use database settings from the `.env` file of a newly created instance.

One thing to be aware of is that you should use the `APP_KEY` value of the old `.env` file since this is used for various features like the encryption of multi-factor authentication credentials. Changing the `APP_KEY` may cause such features to break.

URL Changes

If you are restoring into an environment where BookStack will run on a different URL, there are a couple of things you'll need to do after restoring everything:

- Within the `.env` config file update the `APP_URL` value to exactly match your new base URL.
- Run the ["Update System URL" command](#) to update your database content to use your new URL.

If you migrated web-server configuration files, you may also need to tweak those to correctly use the new URL.

Commands

“ ” BookStack

BookStack has some command line actions that can help with maintenance and common operations. There are also many commands available from the underlying Laravel framework. To list all available commands you can simply run `php artisan` from your BookStack install folder. Custom BookStack commands are all under the 'bookstack' namespace.

Below is a listing of the BookStack specific commands. For any you can provide a `-h` option to list details and options for the command.

Create an Admin User

Create a new admin user via the command line. Can offer a good last resort if you ever get locked out the system. Will use the details provided as options otherwise will request them interactively.

```
# Interactive usage
php artisan bookstack:create-admin

# Non-interactive usage example
php artisan bookstack:create-admin --email="barry@example.com" --name="Bazza" --
password="hunter2"

# Defining "External Authentication ID" instead of password for LDAP/SAML2/OIDC environments
php artisan bookstack:create-admin --email="barry.booker@example.com" --name="Bazza" --
external-auth-id="bbooker"
```

Copy Shelf Permission

By default shelf permissions will not auto-cascade since a book can be in many shelves. This command will copy the permissions of a shelf to all child books. This can be done for a single shelf or for all shelves in the system:

```
# Run for all shelves
php artisan bookstack:copy-shelf-permissions --all

# Run for a single shelf
php artisan bookstack:copy-shelf-permissions --slug=my_shelf_slug
```

Update System URL

BookStack will store absolute URL paths for some content, such as images, in the database. If you change your base URL for BookStack this can be problematic. This command will essentially run a find & replace operation on all relevant tables in the database. Be sure to take a database backup for running this command.

```
# Searches for <oldUrl> and replaces it with <newUrl>
php artisan bookstack:update-url <oldUrl> <newUrl>

# Example:
php artisan bookstack:update-url http://docs.example.com https://demo.bookstackapp.com
```

Reset User MFA Methods

This will reset/clear any existing multi-factor-authentication methods for the given user. If MFA is enforced for one of their roles they'll be prompted to reconfigure MFA upon next login.

```
# Via email address:
php artisan bookstack:reset-mfa --email=john@example.com

# Via system ID:
php artisan bookstack:reset-mfa --id=5
```

Refresh User Avatars

This will re-fetch avatar images for users in the system. By default avatars are fetched from [Gravatar](#) unless an alternative avatar system [has been configured](#).

*Note: This will **not** load avatars from any connected authentication system.*

```
# Refresh avatar for just the user of the given email
php artisan bookstack:refresh-avatar --email=user@example.com

# Or the user of the given id
php artisan bookstack:refresh-avatar --id=101


# Refresh avatars for all users without avatars already assigned
php artisan bookstack:refresh-avatar --users-without-avatars


# Refresh avatars for all users in the system
php artisan bookstack:refresh-avatar --all
```

Delete All Activity History

This will clear all tracked activities in the system. Note: Some areas of the interface rely on this data, including the Audit Log and any "Recent Activity" lists.

```
php artisan bookstack:clear-activity
```

Delete Page Revisions

By default this deletes all page revisions apart from page update drafts which share the same system. A `-a` flag can be used to also delete these update drafts.

```
# Delete just the page revisions
php artisan bookstack:clear-revisions


# Delete all page revisions from the system including update drafts
php artisan bookstack:clear-revisions -a
```

Delete Page Views

Delete tracked content views from the system. These are primarily used to populate any "Recently Used" lists.

```
php artisan bookstack:clear-views
```

Cleanup Unused Images

Searches and removes images that are not used in page content. While this can be done in the "Maintenance" section of the interface, running this via the command-line is often safer to avoid timeouts.

```
php artisan bookstack:cleanup-images
```

Regenerate the Search Index

BookStack uses a custom database-based search index system for efficient querying within the system. The command below re-builds this search index. This does not usually need to be manually ran, but it can be useful if manually inserting pages into the system or to pick-up BookStack indexing changes.

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

Regenerate Access Permissions

BookStack pre-calculates and stores certain access permissions in the database so that access can be calculated in a performant manner. The below command will regenerate these permissions. This is primarily used in development but can be useful if manually adding content via the database.

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

Regenerate Reference Index

BookStack stores references between content within the system to track how content is interlinked. Such references are generally managed by BookStack upon certain actions, such as when saving a page, but in some cases the below command may help to re-index these references. This can be useful upon upgrade of old content, or when manually adding content via the database.

```
php artisan bookstack:regenerate-references
```

Delete Users

Delete all users from the system that are not original "admin" or system-level users.

```
php artisan bookstack:delete-users
```

Generate UTF8mb4 SQL Upgrade Commands

Generates out the SQL which can be used to upgrade the database to UTF8mb4. See [UTF8mb4/Emoji Support](#) for further details.

```
php artisan bookstack:db-utf8mb4
```

Installation



Below you can find details on how to install BookStack on your own hosting. There are a number of installation options available depending on your setup. The install process will require some knowledge of hosting a PHP web application & database.

- [Requirements](#)
- [Shared Hosting](#)
- [Manual](#)
- [Docker](#)
- [Ubuntu 24.04 Script](#)
- [Ubuntu 22.04 Script](#)
- [Ubuntu 20.04 Script](#)
- [Ubuntu 18.04 Script](#)
- [Community Guides](#)
- [Other Hosting Options](#)
- [High Availability](#)

Requirements

BookStack has the following core requirements:

- **PHP** $\geq$ 8.1
 - For installation and maintenance, you'll need to be able to run `php` from the command line.
 - Required Extensions: gd, dom, iconv, mbstring, mysqlnd, openssl, pdo, pdo_mysql, tokenizer, xml.
 - Optional Extensions: ldap (*If wanting to use LDAP Auth*).
 - *For PHP MySQL extensions use `nd` (Native Driver) variants where provided, otherwise these may be the default provided in modern `mysql` PHP extension packages.*

- **MySQL** ≥ 5.7 or **MariaDB** ≥ 10.2
 - For the storage of BookStack content and data.
 - Single Database (*All permissions advised since application manages schema*)
 - **Git Version Control**
 - For application of updates when following our standard process.
 - **Composer** $\geq v2.2.0$
 - For installation and management of our PHP dependencies.
 - **A PHP Compatible Webserver**
 - For usage with PHP and for serving static files.
-

Shared Hosting

BookStack does not currently support shared PHP hosting. There are too many differences between shared hosting providers and too many limitations to support the current install process although we would like to make this easier in the future. You can try searching for 'Laravel Install Guides' for your hosting provider as the process would be similar. Beware that modifying the application source files or applying large work-arounds could lead to security or stability issues.

Manual Installation

Ensure the above requirements are met before installing.

This project currently uses the `release` branch of the BookStack GitHub repository as a stable channel for providing updates. The installation is currently somewhat complicated and will be made simpler in future releases. Some PHP or Laravel experience will make this easier.

1. Clone the release branch of the BookStack GitHub repository into a folder.

```
git clone https://github.com/BookStackApp/BookStack.git --branch release --single-branch
```

2. `cd` into the application folder and run `composer install --no-dev`.
3. Copy the `.env.example` file to `.env` and fill with your own database and mail details.
4. Ensure the `storage`, `bootstrap/cache` & `public/uploads` folders are writable by the web server ([More information here](#)).
5. In the application root, Run `php artisan key:generate` to generate a unique application key.

6. If not using Apache or if `.htaccess` files are disabled you will have to create some URL rewrite rules as shown below.
7. Set the web root on your server to point to the BookStack `public` folder. This is done with the `root` setting on Nginx or the `DocumentRoot` setting on Apache.
8. Run `php artisan migrate` to update the database.
9. Done! You can now login using the default admin details `admin@admin.com` with a password of `password`. You should change these details immediately after logging in for the first time.

Webserver Configuration

- [Example Apache VirtualHost configuration](#)
 - [Example Nginx Server block](#)
-

Docker Containers

Community docker setups are available for those that would prefer to use a containerised version of BookStack:

LinuxServer.io

- [GitHub Repository](#)
- [GitHub container package](#)

solidnerd

- [GitHub Repository](#)
 - [Docker Hub page](#)
-

Ubuntu 24.04 Installation Script

A script to install BookStack on a fresh instance of Ubuntu 24.04 is available. This script is ONLY FOR A FRESH OS, it will install Apache, MySQL 8.0 & PHP 8.3 and could OVERWRITE any existing web setup on the machine. It also does not set up mail settings or configure system security so you will have to do those separately. You can use the script as a reference if you're installing on a non-fresh machine.

- [Link to installation script](#)

Running the Script

```
# Ensure you have read the above information about what this script does before executing
these commands.

# Download the script
wget https://raw.githubusercontent.com/BookStackApp/devops/main/scripts/installation-ubuntu-
24.04.sh

# Make it executable
chmod a+x installation-ubuntu-24.04.sh

# Run the script with admin permissions
sudo ./installation-ubuntu-24.04.sh
```

The script will output a log file for debugging within your current working directory when running the script. Permissions for the BookStack installation files & folders will be set based upon the user used to run the script.

Ubuntu 22.04 Installation Script

A script to install BookStack on a fresh instance of Ubuntu 22.04 is available. This script is ONLY FOR A FRESH OS, it will install Apache, MySQL 8.0 & PHP 8.1 and could OVERWRITE any existing web setup on the machine. It also does not set up mail settings or configure system security so you will have to do those separately. You can use the script as a reference if you're installing on a non-fresh machine.

- [Link to installation script](#)
- [Video guide](#)

Running the Script

```
# Ensure you have read the above information about what this script does before executing
these commands.

# Download the script
```

```
wget https://raw.githubusercontent.com/BookStackApp/devops/main/scripts/installation-ubuntu-22.04.sh

# Make it executable
chmod a+x installation-ubuntu-22.04.sh

# Run the script with admin permissions
sudo ./installation-ubuntu-22.04.sh
```

The script will output a log file for debugging within your current working directory when running the script. Permissions for the BookStack installation files & folders will be set based upon the user used to run the script.

Ubuntu 20.04 Installation Script

A script to install BookStack on a fresh instance of Ubuntu 20.04 is available. This script is **ONLY FOR A FRESH OS**, it will install Apache, MySQL 8.0 & PHP 8.2 and could **OVERWRITE** any existing web setup on the machine. It also does not set up mail settings or configure system security so you will have to do those separately. You can use the script as a reference if you're installing on a non-fresh machine.

- [Link to installation script](#)
- [Video guide](#)

Running the Script

```
# Ensure you have read the above information about what this script does before executing these commands.

# Download the script
wget https://raw.githubusercontent.com/BookStackApp/devops/main/scripts/installation-ubuntu-20.04.sh

# Make it executable
chmod a+x installation-ubuntu-20.04.sh

# Run the script with admin permissions
sudo ./installation-ubuntu-20.04.sh
```

Ubuntu 18.04 Installation Script

A script to install BookStack on a fresh instance of Ubuntu 18.04 is available. This script is ONLY FOR A FRESH OS, it will install Apache, MySQL 5.7 & PHP 8.2 and could OVERWRITE any existing web setup on the machine. It also does not set up mail settings or configure system security so you will have to do those separately. You can use the script as a reference if you're installing on a non-fresh machine.

[Link to installation script](#)

Running the Script

```
# Ensure you have read the above information about what this script does before executing
these commands.

# Download the script
wget https://raw.githubusercontent.com/BookStackApp/devops/main/scripts/installation-ubuntu-
18.04.sh

# Make it executable
chmod a+x installation-ubuntu-18.04.sh

# Run the script with admin permissions
sudo ./installation-ubuntu-18.04.sh
```

Community Guides

This is a collection of guides created by awesome members of the BookStack community:

- [Debian 11 with PHP 8.2 by @armando-femat](#)
- [RedHat 8.9 with PHP 8.1 \(Rocky, Alma, Oracle, etc.\) by @xhark - french guide](#)
- [Sample Docker Swarm Stack by @neuroforgede](#)

In addition to written guides, there are a bunch [community videos on YouTube](#) in addition to the guides on the official [BookStack YouTube channel](#) or [BookStack PeerTube channel](#).

Old Guides

The below are community guides that are no longer current, due to using old operating systems or installing out-of-date dependencies, but they are still listed here as a useful resource:

- [CentOS 7 Install by Deviant Engineer](#)
 - [Debian 11 Install by Othman Alikhan](#)
 - [Fedora 27 Install by Jared Busch](#)
-

Other Hosting Options

Below are some alternative platforms and services that can be used to host BookStack.

Note: These are not tested, vetted nor supported by the official BookStack project in any manner.

- [Cloudron](#) - A solution for running apps on your own server.
 - [Uberspace](#) - A European based hosting provider.
 - [Home Assistant Community Add-on](#) - For [Home Assistant](#) users.
 - [Stellar Hosted](#) - A European based managed hosting provider.
 - [alwaysdata](#) - A European based managed hosting provider.
 - [PikaPods](#) - Managed open source hosting, EU and US regions available.
 - [YunoHost](#) - A Debian-based distribution that automates personal web server installation.
 - [Elestio](#) - Managed hosting in common cloud services or on-premise.
 - [Nexxwave](#) - Managed application hosting in the EU.
 - [Easypanel](#) - A modern server control panel. You can use it to deploy BookStack on your own server.
 - [K&T Host](#) - US based managed BookStack hosting with a focus on high availability.
-

High Availability

Some enterprise environments may need to configure a "High Availability" setup of BookStack to include some operational redundancy. **This type of setup is not needed for the vast majority of BookStack instances.** For a "High Availability" BookStack setup you'll likely need to consider the following:

- High availability is not something we assure to support. There may be scenarios that will not allow availability.
 - For example: The BookStack upgrade process does not assure availability when ran.
- Sessions and Cache use the local filesystem by default.
 - The database/memcached/redis options allow sharing across instances.
 - [Cache and session options are documented here.](#)
- Uploaded files use the local filesystem by default.
 - You could instead use S3 or an S3 like storage system for these files.
 - Alternatively you could mount/link the used directories to shared locations.
 - [Directory locations and storage options are documented here.](#)
- The [theme system](#) and [error log](#) also use the local filesystem.
- A simplistic health-check endpoint can be found at the `/status` URI.
 - This performs basic checks on subsystems.
 - This should return a HTTP error status code (≥ 400) on any failure otherwise a 200 status code.

Security

“ BookStack

Since BookStack can hold important information for users you should be aware of any potential security concerns. Read through the below to ensure you have secured your BookStack instance. Note, The below only relates to BookStack itself. The security of the server BookStack is hosted on is not instructed below but should be taken into account.

If you'd like to be notified of new potential security concerns you can sign-up to the [BookStack security mailing list](#). For reporting security vulnerabilities, please see the ["Security" section](#) of the project readme on GitHub.

Initial Security Setup

1. Ensure you change the password and email address for the initial `admin@admin.com` user.
2. Ensure only the `public` folder is being served by your webserver. Serving files above this folder opens up a lot of code that does not need to be public. Triple check this if you have installed BookStack within the commonly used `/var/www` folder.
3. Ensure the database user you've used for BookStack has limited permissions for only accessing the database used for BookStack data.
4. Check that you've set the `APP_URL` option in your `.env` file so that system generated URLs cannot be manipulated.
5. Within BookStack, go through the settings to ensure registration and public access settings are as you expect.
6. Review the user roles in the settings area.
7. Read the below to further understand the security for specific functionality and features.

Multi-Factor Authentication

Any user can enable multi-factor authentication (MFA) on their account. Upon login they would then need to use an extra proof of identity to gain access. BookStack currently supports the following mechanisms:

- TOTP (Time-based One-Time Passwords)

- Labelled as "Mobile App" (Google/Microsoft Authenticator etc...).
- Uses a SHA1 algorithm internally (Greater algorithms have poor cross-app compatibility).
- Backup Codes
 - These are a list of 16 one-time-use codes.
 - Users will be warned once they have less than 5 codes remaining.

Secrets and values for these options are stored encrypted within the database.

Where required, MFA can be forced upon users via their roles. This can be found via a "Requires Multi-Factor Authentication" checkbox seen when editing a role. If a user does not already have an MFA method configured, they will be forced to set one up upon next login.

Securing Images

By default, Images are stored in a way which is publicly accessible which ensures performance while using BookStack. Listed below are a few options for increasing image security.

Alternative Storage Options

Review our [file upload storage options](#) documentation for image storage options that add additional access or permission control to image requests.

Complex Urls

In the settings area of BookStack you can find the option 'Enable higher security image uploads?'. Enabling this will add a 16 character random string to the name of image files to prevent easy guessing of URLs. This increases security without potential performance concerns.

Prevent Directory Indexes

It's important to ensure you disable 'directory indexes' to prevent unknown users from being able to navigate their way through your images. Here's the configuration for NGINX & Apache if your server allows directory indexes:

NGINX

```
# By default indexes are disabled on Nginx but if you have them enabled
# add this to your BookStack server block
location /uploads {
    autoindex off;
}
```

Apache

```
# Add this to your Apache BookStack virtual host if Indexes are enabled.  
# If .htaccess file are enabled then the below should already be active.  
<Location "/uploads">  
    Options -Indexes  
</Location>
```

You can test that indexes are disabled by attempting to navigate to

`<your_bookstack_url>/uploads/images` in the browser after having uploaded at least one image. You should not see a list of files but instead a BookStack "Not Found" page.

Attachments

Attachments, if not using Amazon S3, are stored in the `storage/uploads` directory. By default, unlike images, these are stored behind the application authentication layer so access depends on permissions you have set up at a role level and page level.

If you are using Amazon S3 for file storage then access will depend on your S3 permission settings. Unlike images, BookStack will not automatically attempt to make uploaded attachments publicly accessible.

Filesystem Permissions

It's usually a good idea to limit the file and folder access privileges for the user/group used to run the application PHP, which is typically the user/group for PHP or the running web-server processes. Limiting permissions can help avoid a range of potential vulnerability exploits.

Details on required [filesystem permissions can be found here](#).

User Passwords

User passwords, if not using an alternative authentication method, are stored in the database. These are hashed using the standard Laravel hashing methods which use the Bcrypt hashing algorithm.

JavaScript in Page Content

By default, JavaScript tags within page content is escaped when rendered. This can be turned off by setting `ALLOW_CONTENT_SCRIPTS=true` in your `.env` file. Note that even if you disable this escaping the WYSIWYG editor may still perform its own JavaScript escaping. This option will also alter the [CSP rules](#) set by BookStack.

This option disables some fundamental cross-site-scripting protections. Only use this option on secure instances, where only very trusted users can edit content

Web Crawler Control

The rules found in the `/robots.txt` file are automatically controlled via the "Allow public viewing?" setting. This can be overridden by setting `ALLOW_ROBOTS=false` or `ALLOW_ROBOTS=true` in your `.env` file. If you'd like to customise the rules this can be done via theme overrides.

Secure Cookies

BookStack uses cookies to track sessions, remember logins and for XSRF protection. When using HTTPS you may want to ensure that cookies are only sent back to the browser if the connection is over HTTPS. If you have set a `https APP_URL` option in your `.env` this will enabled automatically but it can also be forced on by setting `SESSION_SECURE_COOKIE=true` in your `.env` file.

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.com 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.

Failed Access Logging

An option is available to log failed login events to a log file which is useful to identify users having trouble logging in, track malicious login attempts or to use with tools such as Fail2Ban. This works with login attempts using the default email & password login mechanism or attempts via LDAP login. Failed attempts are **not logged** for "one-click" social or SAML2 options.

To enable this you simply need to define the `LOG_FAILED_LOGIN_MESSAGE` option in your `.env` file like so:

```
LOG_FAILED_LOGIN_MESSAGE="Failed login for %u"
```

The optional "%u" element of the message will be replaced with the username or email provided in the login attempt when the message is logged. By default messages will be logged via the php `error_log` function which, in most cases, will log to your webserver error log files.

Untrusted Server Side Requests

Some features, such as the PDF exporting, have the option to make http calls to external user-defined locations to do things such as load images or styles. This is disabled by default but can be enabled if desired. This is required for using WKHTMLtoPDF as your PDF export renderer. This should only be enabled in BookStack environments where BookStack users and viewers are fully trusted.

To enable untrusted server side requests, you need to define the `ALLOW_UNTRUSTED_SERVER_FETCHING` option in your `.env` file like so:

```
ALLOW_UNTRUSTED_SERVER_FETCHING=true
```

Note that this is not connected to the `ALLOWED_SSR_HOSTS` setting at all.

`ALLOW_UNTRUSTED_SERVER_FETCHING` is used for typically "untrusted" scenarios/functionality whereas `ALLOWED_SSR_HOSTS` is used for typically "trusted" user scenarios/functionality (where admin-level permissions are required).

Server Side Request Allow List

There is some functionality in BookStack, like webhooks for example, that is typically only accessible by trusted (admin-level) users. In some cases, those admin users may not be trusted to the level where they can freely make server side requests. In such scenarios, you can define a `ALLOWED_SSR_HOSTS` option in your `.env` file to limit the hosts that can be called for such typically trusted functionality:

```
# Allow all hosts (Default)
ALLOWED_SSR_HOSTS="*"

# Allow a single host
ALLOWED_SSR_HOSTS="https://example.com"

# Allow multiple hosts via space-separated entries
ALLOWED_SSR_HOSTS="https://example.com https://example.org"

# Use '*' as wildcards and/or define required paths
```

```
ALLOWED_SSR_HOSTS="https://*.example.com https://example.org/bookstack/"
```

Values will be compared prefix-matched, case-insensitive, against called SSR urls.

Note that this is not connected to the `ALLOW_UNTRUSTED_SERVER_FETCHING` setting at all.

`ALLOW_UNTRUSTED_SERVER_FETCHING` is used for typically "untrusted" scenarios/functionality whereas `ALLOWED_SSR_HOSTS` is used for typically "trusted" user scenarios/functionality (where admin-level permissions are required).

Content Security Policy (CSP)

BookStack serves responses with a CSP header to increase protection against malicious content. This is especially important in a system such as BookStack where users can create a variety of HTML content, especially so if you allow untrusted users to create content in your instance. The CSP rules set by BookStack are as follows:

- `frame-ancestors 'self'`
 - Restricts what websites can embed BookStack pages via iframes.
 - See the "[Host Iframe Control](#)" section above for details on expanding this rule to other hosts.
- `frame-source 'self' https://*.diagrams.net https://*.draw.io https://*.youtube.com https://*.youtube-nocookie.com https://*.vimeo.com https://embed.diagrams.net`
 - Restricts what sources are allowed to load for frames/iframes.
 - Can be configured via a `ALLOWED_IFRAME_SOURCES` .env option.
 - May be different depending on other configuration set.
- `script-src http: https: 'nonce-abc123' 'strict-dynamic'`
 - Restricts what scripts can be ran on a BookStack-served page.
 - Will not be set if the `ALLOW_CONTENT_SCRIPTS` .env option is active.
 - The nonce value used is randomly generated upon each request. It is automatically applied to any "Custom HTML Head Content" scripts.
- `object-src 'self'`
 - Restricts which embeddable content can be loaded onto a BookStack-served page.
 - Will not be set if the `ALLOW_CONTENT_SCRIPTS` .env option is active.
- `base-uri 'self'`
 - Restricts what `<base>` tags can be added to a BookStack-served page.

If needed you should be able to set additional CSP headers via your webserver. If there's a clash with an existing BookStack CSP header then browsers will generally favour the most restrictive policy.

MySQL SSL Connection

If your BookStack database is not on the same host as your web server, you may want to ensure the connection is encrypted using SSL between these systems. Assuming SSL is configured correctly on your MySQL server, you can enable this by defining the `MYSQL_ATTR_SSL_CA` option in your `.env` file like so:

```
# Path to Certificate Authority (CA) certificate file for your MySQL instance.  
# When this option is used host name identity verification will be performed  
# which checks the hostname, used by the client, against names within the  
# certificate itself (Common Name or Subject Alternative Name).  
MYSQL_ATTR_SSL_CA="/path/to/ca.pem"
```

Using BookStack Content Externally

In some scenarios you may use BookStack user-provided content externally (Accessed via the database or API). Such content is not guaranteed to be safe so keep security in mind when dealing with such content. In some cases, the system will apply some filtering to content in an attempt to prevent certain vulnerabilities, but this is not assured to be a bullet-proof defence.

Within its own interfaces, unless disabled, BookStack makes use of Content Security Policy (CSP) rules to heavily negate cross-site scripting vulnerabilities from user content. If displaying user content externally, it's advised you also use defences such as CSP or other techniques such as disabling of JavaScript entirely.

Updating BookStack

“ ” BookStack

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 a 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 be 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.

Customising Visuals

“  BookStack 

You may want to customise BookStack to use custom branding, or you may just not like the default blue theme. Customising the branding of BookStack is super simple and can be done within the "Settings > Customization" area of the interface. Here you can change the application name, logo and the core colours used. Additional ways to customise are listed below:

Changing Fonts

To change fonts you can make use of the "Custom HTML Head Content" customization setting by adding custom CSS to alter fonts used. Copy the code below into this setting and alter the font names to your desired fonts:

```
<style>
  body {
    --font-body: 'Noto Serif', serif;
    --font-heading: 'Roboto', sans-serif;
    --font-code: 'Source Code Pro', monospace;
  }
</style>
```

Here's an example of using the 'Lato' font from [Google Web Fonts](https://fonts.googleapis.com/css?family=Lato) as the main body text font:

```
<link href="https://fonts.googleapis.com/css?family=Lato" rel="stylesheet">
<style>
  body {
    --font-body: 'Lato', sans-serif;
  }
</style>
```

Some additional notes to consider when setting custom fonts:

- Changes won't apply to the main `/settings` pages of BookStack, since custom HTML head content is not applied here.

- If a heading font is not set via `--font-heading`, then the `--font-body` value will be used as a fallback.
- This system simply makes use of normal [CSS variables](#), and the values are used for the standard [CSS font-family](#) property.
- These fonts won't apply to PDF exports, where font availability and usage is more limited.
- The font used for `--font-code`, if set, should be a monospace font.

Changing Code Block Themes

When inserting code into a page, or when using the Markdown editor, the text you enter is highlighted by the [CodeMirror library](#). For those that'd prefer a different colour scheme for code blocks, we do provide a custom `library-cm6::configure-theme` JavaScript event which provides a couple of methods that allow registration of CodeMirror UI and syntax highlighting themes.

You can find more information, along with an example, in our [JavaScript public events documentation here](#).

Default Light/Dark Mode

By default, BookStack will be presented in "light mode". Users can toggle their light/dark mode preference using one of the buttons either found on the homepage view, or within the header bar user dropdown menu.

If you'd instead like your instance to be presented in "dark mode" by default, you can add the following option to your `.env` file:

```
# Use dark mode by default
# Will be overridden by any existing user/session preference.
APP_DEFAULT_DARK_MODE=true
```

Default Book View

By default the `/books` page displays your books as a list. Users can change this option to list or grid view but if you'd like to set the default for public viewers or new users you can add the following to your `.env` file:

```
# Show grid view by default
APP_VIEWS_BOOKS=grid
```

```
# Show list view by default
```

```
APP_VIEWS_BOOKS=list
```

Further Customisation

If you need to customise BookStack further to the given controls in the settings area you can make use of the 'Custom HTML head content' setting. Using this you can add in any custom JavaScript or CSS content to override default BookStack functionality and styles.

[View the Hacking BookStack](#) page for more advanced ways to achieve deeper customisation.