WordPress Security Tips for B2B Websites

BOP DESIGN®

There are many things you can do to secure your website to prevent hackers and vulnerabilities. In this guide, we share WordPress security tips to help you protect against the most common and dangerous vulnerabilities.

WordPress is secure when best practices are followed

Overall, WordPress is a secure CMS and is audited regularly by hundreds of developers.

However, WordPress is open-source software, meaning that the source code is available for anyone to modify and distribute, and its functionality can be extended or improved by thousands of plugins and themes. This flexibility and infinite customization options are defining features of WordPress, making it powerful and widely used. But it also makes it suffer from various vulnerabilities. However, if users take appropriate steps to follow best practices, WordPress is a secure platform.

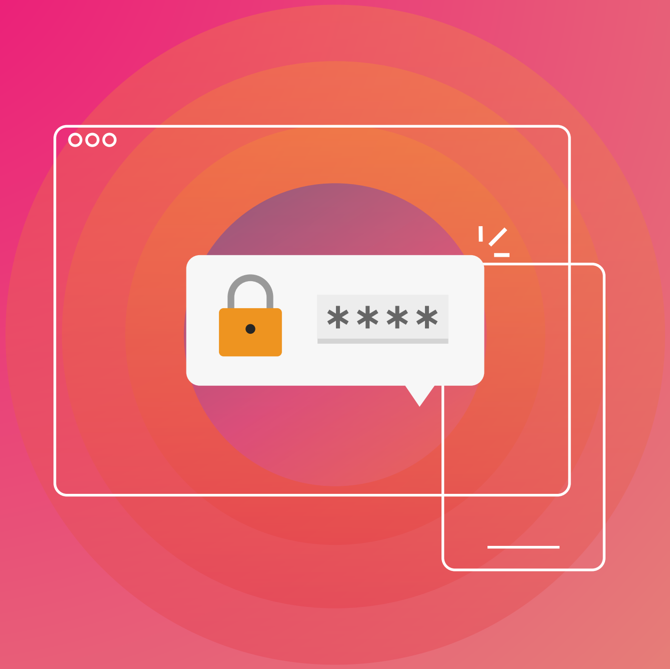
Use secure WordPress hosting

Your WordPress hosting service has the most important role in the security of your B2B website, as there is web server-level security for which it is responsible. A good hosting provider takes extra measures to protect its servers against common threats and so it can promptly recover if an attack occurs. If you are hosting WordPress on your own VPS, then you need to have a technical team do these things for you.

Secure your login – strong passwords and user permissions

The fundamental step to securing your B2B website is keeping your login accounts safe, as the most common WordPress hacking attempts use stolen passwords.

To do this, use strong passwords that are unique to your website, not just your WordPress admin area, but also (S)FTP accounts, database, hosting account, etc. We recommend using a password manager to generate strong passwords and keep track of them.



Enable two-factor authentication (2FA), which requires users to verify their sign-in with a second device. For this there are a couple of plugins we recommend:

- → **Two Factor Authentication**
- → **Duo Two-Factor Authentication**
- → **MiniOrange's Google Authenticator**

Don't make any account username "admin". Chances are, this is the very first username attackers will try during a brute-force attempt. We recommend deleting the default WordPress admin account. Create a new administrator account and delete the "admin" user.

Limit login attempts, by placing a cap on the number of times a user can enter the wrong credentials in a certain amount of time. This prevents hackers from brute-force login. Some hosting services and firewalls might take care of this, but you can also install a plugin like Limit Login Attempts to do the job.

Enable auto-logout, which prevents strangers from snooping in your account if you forget to log out when finished. To enable auto-logout on your WordPress account, try the Inactive Logout plugin.

Update Your WordPress, Plugins, and Themes on a Regular Basis

One of the ways to mitigate the possibility of being hacked is to update your software on a regular basis. This includes WordPress core, plugins, and themes (both those from the WordPress repository and premium ones), which usually include the latest security patches and bug fixes.

USE THE LATEST VERSION OF PHP

PHP is the backbone of your WordPress site and upgrading to the latest version is one of the most important steps. Each major release of PHP is typically fully supported for 2 years after its release. It takes time to test the compatibility of the latest PHP version with your code, but it's better than running on something without security support, aside from having a performance impact running on older versions.

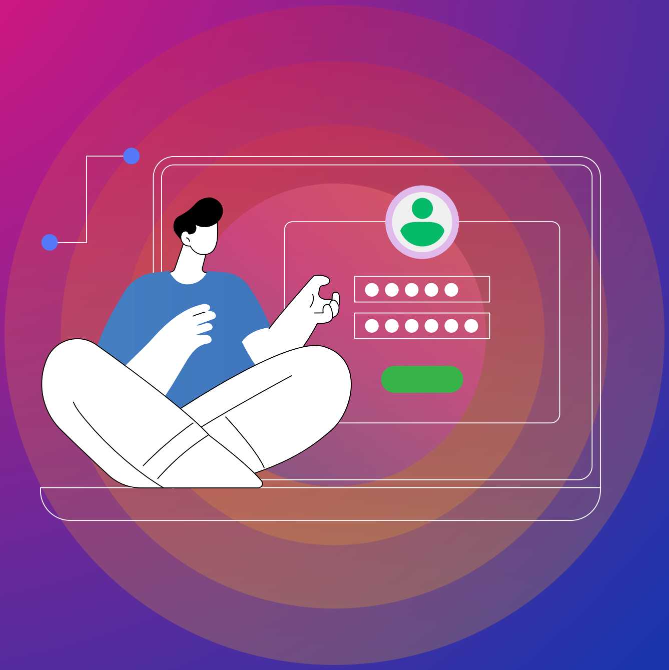
HIDE YOUR WORDPRESS LOGIN URL

Making it harder for attackers to find certain backdoors is an effective strategy for a WordPress website. Changing your WordPress Login URL is a good way to improve security. By default, your WordPress login URL is **example.com/wp-login.php**, you know it and all the bots and hackers out there know it. Changing URLs can better protect you from brute-force attacks and make you less of a target. It's a simple and quick trick, but not a fix-all solution.

There are several free plugins that can get the job done, we recommend a free plugin: WPS Hide Login.

Make sure to set a unique URL, that is less likely to already be on a list that a bot may attempt to scan.

While the change of URL can help to decrease the majority of the bad login attempts, there is another step that can further the security of the website. Putting a limit on failed login attempts is a great way to stop an internet address from making further attempts after a specified limit on entries has been reached, making a brute-force attack difficult or impossible. Free plugins like WPS Limit Login or Login LockDown are easy ways to set up lockout durations, login attempts, and IP whitelists and blacklists.



Use WordPress Security Plugins

One step to help you in securing your B2B website is to install one or more security plugins. There are a lot of great options out there, here are a couple of them:

- → **Sucuri Security**
- → **Wordfence Security**
- → **SecuPress Free – WordPress Security**
- → **iThemes Security**
- → **WP fail2ban**

These plugins do much of the security-related manual work for you, including:

- **Malware scanning**
- **File integrity monitoring**
- **User action logging**
- **Force strong passwords when creating use profiles**
- **Force passwords to expire and reset on a regular basis**
- **Block malicious networks**

and more...

Enable SSL – Use HTTPS for Encrypted Connections

Your B2B website needs SSL enabled, not only it will boost SEO, but it also displays the trust and credibility of the website.

This credibility factor plays directly into your visitors' first impression, as some of the browsers warn users of unsafe sites, which can negatively impact website traffic.

Disable XML-RPC

XML-RPC is a remote procedure call (RPC) protocol that uses XML to encode its call and HTTP as a transport mechanism. It is enabled in WordPress by default and helps connect the WordPress website with web and mobile applications. One of XML-RPC features is that it lets submit requests containing hundreds of commands, which opens doors for the hacker to commit brute-force login attacks.

THERE ARE SEVERAL METHODS TO DISABLE XML-RPC IN WORDPRESS:

METHOD #

1

WordPress security plugins

Some WordPress security plugins may have an option to disable it, if not you can use a plugin called Disable XML-RPC-API.

METHOD #

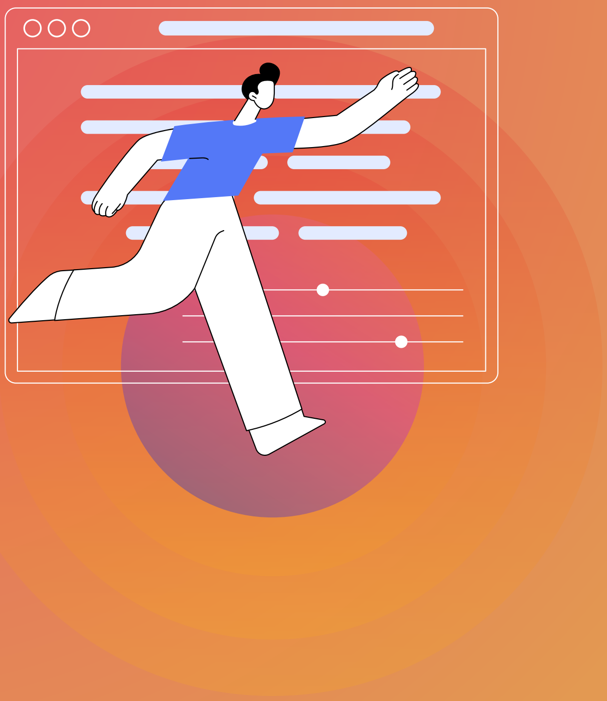
2

Manually Disable XML-RPC in WordPress

In order to do this, you need to add a code snippet to your WordPress **theme functions.php** file (or any file responsible for managing filters or hooks):

```
add_filter( ‘xmlrpc_enabled’, ‘__return_false’ )
```

Hide Your WordPress Version



Hiding your WordPress version is a mechanism of **WordPress security by obscurity**. The less information about your site configuration that is available, the fewer backdoor exploits can be applied to it. The best way to stay safe is to make sure your WordPress installation is always up to date. However, if this is not always possible, then the least that you can do is to mitigate the chance of exploitation, by hiding the information.

TO ACHIEVE THAT THERE ARE SEVERAL METHODS:

METHOD # 1

Use a Plugin

Free – WP Hardening – Fix Your WordPress Security.

Premium – Perfmatters.

METHOD # 2

Hide WordPress Version Number Manually

If you are confident in editing theme files, you can hide the WordPress version number using the following ways:

Remove Generator Meta Tag

Add the line of code at the bottom of the theme’s **function.php** file (or any file responsible for managing filters or hooks):

```
remove_action( ‘wp_head’, ‘wp_generator’ );
```

Remove generator version number

Add the line of code at the bottom of the theme’s **function.php** file (or any file responsible for managing filters or hooks):

```
function wp_version_remove_version() {
return ”;
}
add_filter( ‘the_generator’, ‘wp_version_remove_version’ );
```

METHOD # 3

Remove Readme.html File (optional)

If you’re using WordPress 5.0 or higher you can skip this step, otherwise, read on. The version number is available in the default **readme.html** file, which is included in all WordPress versions. It is at the root of your installation – **example.com/readme.html.** You can simply and safely delete it via (S)FTP.

Harden Database Security

By default, WordPress uses “wp_” prefix for all tables in your database. It makes it easier for hackers to guess what your table name is, and it is recommended that you change it. It is possible to change the prefix when installing WordPress. If your site is already live, then you can update it using a plugin, or manually by someone from your development team. Changing to something like “wptable_” or “23mj_” can be much more secure.

Another step is to use a unique database name, as by default your WordPress is most likely named after your domain name, i.e., **example.com** will have a database name **wp_example**. By obscuring the database name, it makes it more difficult for hackers to access your database details.

NB: Only proceed, if you know what you’re doing and feel comfortable with changing this, as it can break your site if not done properly.

WORDPRESS SECURITY TIPS FOR B2B WEBSITES | 619.330.0730 | WWW.BOPDESIGN.COM 15

Disable File Editing in WordPress Dashboard

WordPress comes with a built-in editor which lets administrators edit the code of your theme and plugins. In the wrong hands, this feature is a great security risk. It is much safer to edit the file locally and upload it to the server via (S)FTP, and even better to test it on a development environment first. We recommend turning this feature off.

Place the code below in your **wp-config.php** file:

```
// Disallow file edit.

define( ‘DISALLOW_FILE_EDIT’, true );
```

Make sure to place it above the lines something like this:

```
/* That’s all, stop editing! Happy publishing. */
```

or

```
/** Absolute path to the WordPress directory. */
```

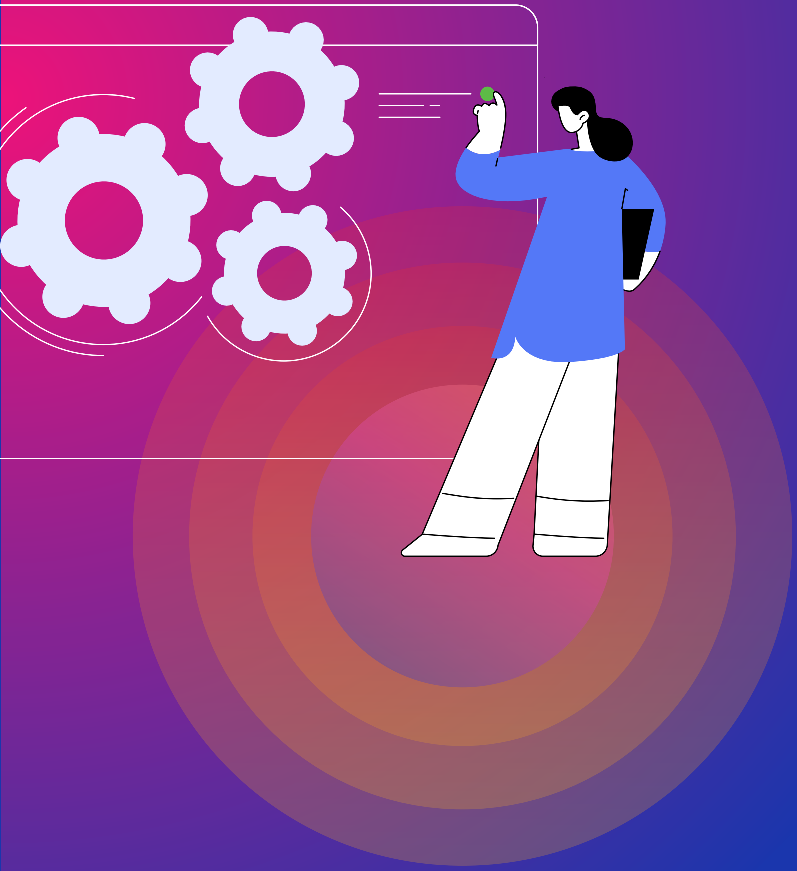
or

```
# That’s It. Pencils down
```

Backup Your Website

Backups are a great thing to have not only in the event of being hacked, but also in the event of any incident that causes data loss.

Make backups automatic, at regular intervals, and save them to a remote location (not the same server your website is installed at). Most managed WordPress hosting providers have this service included, and you can even restore your site with one click. In case you need to set up a backup solution yourself, we recommend storing your backups on cloud services like **Amazon S3, Google Cloud, Dropbox,** or private clouds like **Stash**, using plugins to automate the process, like **Duplicator**, **BackupBuddy**, **UpdraftPlus**. There are also services like **VaultPress**, **BlogVault**, **CodeGuard**.



Use Latest HTTP Security Headers

Take advantage of HTTP security headers to harden your WordPress security. These headers are a fundamental part of website security. They protect your website against the types of attacks that are most common. The HTTP headers are usually configured at the server level and tell the browser how to behave when handling your site.

Below is the list of the most important ones in no particular order:

- **X-XSS-Protection**
- **Strict-Transport-Security**
- **Content-Security-Policy**
- **Referrer-Policy**
- **Permissions-Policy**
- **X-Frame-Options**
- **X-Content-Type-Options**

You'll need to modify it to match your needs, especially the Content-Security-Policy. Free tools like **SecurityHeaders.com** scan your website to show which HTTP security headers you currently have, and link to additional information on how to improve your security header profile. You can always ask your host for help if you aren't sure how to implement them.

BOP DESIGN®

Considering building a new WordPress website for your B2B business? Contact Bop Design to chat about your WordPress website.

Contact us today to schedule a consultation with experienced B2B marketing team.

www.bopdesign.com | 619.330.0730