Your WordPress Security Audit Workbook

SIMPLY STATIC

simplystatic.com
Fast and secure WordPress without the headache

Introduction

This workbook will help you see how secure your WordPress site really is.

You'll go through 12 stages. In each one, you'll review part of your site and note what needs attention. You don't need to fix anything now, just record what you find.

When you're finished, you'll have a clear list of tasks to complete later, plus an easy way to simplify future security work.

How to use this workbook:

1. Download the PDF and save it to your device.
2. You can type responses to the questions directly in the boxes provided. Or you can print out the template and complete it by hand.
3. If editing via your browser, make sure to save as you go. If you click away from the workbook (for example, if you click on a link within this workbook), you might lose your changes.

Studio shortcut

Throughout this workbook, you'll see small 'Studio shortcut' notes. These point out tasks that can be automated using a secure WordPress setup like Simply Static Studio. We talk about Simply Static Studio on the last page of this workbook.

Note: Always right-click links within this workbook and select 'Open link in a new tab' to make sure you don't lose your hard work.

SIMPLY STATIC

Table of Contents

Stage 1: WordPress core (version & updates) 4

Stage 2: Themes and plugins 5

Stage 3: Users and logins 6

Stage 4: Login page security 7

Stage 5: SSL / HTTPS 8

Stage 6: Hosting security 9

Stage 7: Sensitive files 10

Stage 8: Malware & vulnerability scans 11

Stage 9: Database safety 12

Stage 10: CDN & edge protection 13

Stage 11: Audit summary 14

Stage 12: Action plan 15

Simplify your WordPress security with Simply Static Studio 16

Stage 1: WordPress core (version & updates)

WordPress releases often include fixes for known security issues. If you're running an older version, hackers can exploit vulnerabilities that have already been patched. Checking this now shows whether your site is protected by the latest fixes.

Steps:

1. From your WordPress dashboard, go to Dashboard > Updates.
2. Note the version number of WordPress.
3. Compare it to the latest version listed on the official WordPress releases page.

Write down what you find:

Current WordPress version:		
Up to date?	☐ Yes	☐ No
Automatic updates turned on?	☐ Yes	☐ No

Task notes (for later):

Stage 2: Themes and plugins

Plugins and themes add features, but every one of them also adds potential weak spots. Out-of-date or abandoned ones can contain known bugs that hackers target. Keeping only what you use and updating regularly reduces risk and speeds up your site.

Steps:

1. Go to Plugins > Installed Plugins and count how many are active.
2. Look for any marked as needing an update.
3. To check how recently a plugin has been updated:
    a. Click the plugin's View details link, or
    b. Search for the plugin name on wordpress.org/plugins it shows the "Last updated" date at the top of the page.
4. If a plugin hasn't been updated in over a year, make a note to review or replace it.
5. Go to Appearance > Themes and check when your active theme was last updated too.

Write down what you find:

Total plugins installed:	
Plugins needing an update:	
Unused plugins or themes?	☐ Yes ☐ No

Task notes (for later):

Examples: "Check for a newer contact form plugin," "Remove old theme from 2019."

Stage 3: Users and logins

Every account that can log in is another door into your site. Old or unnecessary admin accounts, or weak passwords, make those doors easy to open. Knowing exactly who can log in helps you close the ones you don't need.

Steps:

1. In your WordPress dashboard, go to Users > All Users.
2. Look at the Role column next to each name.
    a. Administrator - full control of your site.
    b. Editor / Author / Contributor - can edit or add content.
    c. Subscriber - very limited access.
3. Count how many users have Administrator access.
4. Note any usernames you don't recognize or that no longer need access.
5. Check if each Administrator uses a strong password and has two-factor authentication (2FA) turned on.
6. Record what you find below. You'll decide what to change later.

Studio shortcut

If you use Simply Static Studio, you get two-factor authentication built-in. It makes it far harder for hackers to log in, even if they know a password.

Write down what you find:

Number of Administrator accounts:		
Any unused / unknown users?	☐ Yes	☐ No
Two-factor authentication in use?	☐ Yes	☐ No

Task notes (for later):

Examples: "Ask host to remove old user accounts," "Set up 2FA for admins," "Check password policy."

Stage 4: Login page security

Bots constantly try to log in by guessing passwords thousands of times a day. Changing the default login page or limiting attempts makes it much harder for them to get in. Even simple measures here can automatically block a large number of attacks.

Steps:

1. Open your browser and check how you normally log in.
    a. If your login address ends with /wp-admin or /wp-login.php, note it below.
    b. If you use a custom login address (for example, /my-login), note that too.
2. In your dashboard, check if you have a plugin that limits failed login attempts.
    a. These plugins usually appear under the “Plugins” menu.
3. If you see an option for idle logout or session timeout, check whether it’s enabled. This signs users out after a period of inactivity.
4. Record your findings below; you’ll decide what to improve later.

Studio shortcut

If you use Simply Static Studio, your public site doesn’t have a WordPress login page at all. All admin access happens through Studio’s secure dashboard, which keeps your wp-admin and wp-login.php areas completely hidden from hackers.

Write down what you find:

Login page address:		
Custom login URL used?	☐ Yes	☐ No
Limit on failed logins?	☐ Yes	☐ No
Idle logout/session timeout enabled?	☐ Yes	☐ No

Task notes (for later):

Examples: “Ask developer to hide login page,” “Add plugin to limit login attempts,” “Enable session timeout.”

Stage 5: SSL / HTTPS

SSL (Secure Sockets Layer) encrypts all data sent between your website and visitors, including login details, contact form messages, and payment information. Without it, hackers can intercept this data. A valid SSL certificate also prevents browsers from showing “Not Secure” warnings and helps search engines trust your site.

Steps:

1. Open your website in a browser.
    a. Look for a padlock icon to the left of your URL.
    b. If it shows “Not secure” or a warning symbol, your SSL certificate might be missing or expired.
2. Click the padlock icon (or warning) to view certificate details. This shows whether it’s valid and who issued it.
3. Record your findings below.

Studio shortcut

If you use Simply Static Studio, SSL protection is built in. Your site automatically runs over HTTPS with a valid, auto-renewing certificate. No manual setup, purchase, or renewal needed. Studio also ensures all pages load securely without mixed-content warnings.

Write down what you find:

HTTPS active (padlock visible)?	☐ Yes	☐ No
SSL valid and current?	☐ Yes	☐ No

Task notes (for later):

Examples: “Ask host to renew SSL,” “Force HTTPS in settings,” “Fix mixed-content warnings.”

Need help?

Ask your host: “Can you confirm my SSL certificate is active and set to renew automatically?”

Stage 6: Hosting security

Your host is your site's first line of defense. Strong hosting security can block attacks before they ever reach your site, reducing the need for extra plugins or manual fixes. Knowing what's included helps you fill any missing gaps later.

Steps:

Log in to your hosting panel and check for:

- **Daily backups** (automatic copies of your site)
- **Firewall** (protects against suspicious traffic)
- **Malware scanning** (detects infected files)
- **DDoS protection** (prevents overload from fake visitors)
- **Secure connections (SFTP/SSH)** for safe file transfers

Studio shortcut

Studio includes secure WordPress hosting behind a protected control panel. It already provides SSL, firewalls, malware scanning, DDoS protection, and daily backups. No separate setup required.

Write down what you find:

Daily backups?	☐	Yes	☐	No
Firewall?	☐	Yes	☐	No
Malware scans?	☐	Yes	☐	No
DDoS protection?	☐	Yes	☐	No
SFTP/SSH?	☐	Yes	☐	No

Task notes (for later):

Examples: "Ask host to enable daily backups," "Upgrade to plan with firewall," "Check SFTP access details."

Need help?

Ask your host: "Can you confirm if my hosting plan includes a web application firewall, malware scanning, daily backups, and DDoS protection? If not, what's the best way to add them?"

Stage 7: Sensitive files

These files act as the control centre of your site. If hackers can read or change them, they can take over your site completely. Knowing whether they're hidden and protected helps you avoid serious data leaks or malware infections.

Steps:

1. Open your hosting control panel or file manager (often called File Manager, cPanel).
2. Look in the main folder that holds your WordPress files, usually called public_html.
3. Check if you can see these files:
    - wp-config.php: holds your database login details and secret keys.
    - .htaccess: controls how your site handles traffic and permissions.
4. You don't need to open them, just confirm they exist and are not publicly accessible.
    - If your host lets you visit yourdomain.com/wp-config.php and see anything but a blank or error page, note it below.
- Record whether your host lists file permissions (numbers like *400*, *440*, *644*). If you can see them, note whether they're restrictive (not open to "public").

Studio shortcut

If you use Simply Static Studio, these files are never publicly exposed. Your live site runs as static pages, while the original WordPress installation stays safely behind Studio's protected environment. That means wp-config.php, .htaccess, and other system files can't be accessed, edited, or exploited by hackers.

Write down what you find:

wp-config.php accessible to public?	☐ Yes	☐ No
File permissions set securely?	☐ Yes	☐ No
.htaccess file exists?	☐ Yes	☐ No

Task notes (for later):

Examples: "Ask host to restrict access to wp-config.php," "Confirm file permissions are correct."

Need help?

Ask your host: "Can you confirm that my wp-config.php file isn't publicly accessible and that file permissions are correctly set to prevent outside access?"
"Can you confirm my .htaccess file exists and includes rules to block access to sensitive files?"

Stage 8: Malware & vulnerability scans

Malware is harmful code added to your site without permission. It can redirect visitors to scam websites, add spam content, and steal login or customer data. Regular scans catch these issues early, before they damage your site's reputation or ranking.

Steps:

1. In your WordPress dashboard, go to Plugins > Installed Plugins.
2. Check if you have a security or malware plugin installed.
3. If you have one, note whether automatic scans are scheduled.
4. If you don't have one, record that your site currently isn't being scanned.

Studio shortcut

If you use Simply Static Studio, you don't need a malware or security plugin. Studio's private environment is automatically monitored for threats, and your live static site can't be infected because it contains no executable code.

Write down what you find:

Security or malware plugin installed?	☐ Yes	☐ No
Automatic scans scheduled?	☐ Yes	☐ No
Scan frequency (if known):		

Task notes (for later):

Examples: "Install security plugin," "Review scan settings," "Enable automatic scans."

Stage 9: Database safety

Your database stores everything including posts, users, settings, and passwords. If attackers know your database structure or credentials, they can inject or steal data. Changing default details and limiting exposure make your site much harder to compromise.

Steps:

1. In your WordPress dashboard, check whether any users still have the default “admin” username.
2. If you have access to your site’s database settings (often found in your hosting control panel or wp-config.php), look for the database table prefix.
3. By default, it’s wp_.
4. Using a custom prefix makes it harder for attackers to target your database.
5. Record what you find below.

Studio shortcut

If you use Simply Static Studio, your WordPress database isn’t public at all. It stays securely inside your private Studio workspace, completely hidden from visitors and bots. This eliminates the risk of database exposure or SQL injection attacks.

Write down what you find:

Default “admin” username still used?	☐ Yes	☐ No
Database prefix changed from “wp_”?	☐ Yes	☐ No

Task notes (for later):

Examples: “Change admin username,” “Ask developer to update table prefix,” “Review database permissions.”

Need help?

Ask your host or developer: “Can you confirm that my WordPress database prefix isn’t set to the default ‘wp_’, and that direct file editing inside wp-admin is disabled?”

Stage 10: CDN & edge protection

A CDN stores copies of your site on servers around the world and serves them from the nearest location to each visitor. This improves site speed and adds an extra layer of protection by blocking malicious traffic before it reaches your server.

Steps:

1. Ask your host or check your account dashboard to see if you currently use a CDN. Common providers include Cloudflare and BunnyCDN.
2. If you use a plugin like Jetpack, Cloudflare, or a performance tool, check its settings to see if CDN features are active.
3. Record your CDN provider and whether any security features (like DDoS protection or firewall) are enabled.

Studio shortcut

If you use Simply Static Studio, a global CDN is included automatically. Your static site is distributed worldwide for speed and protected at the network edge, no separate Cloudflare or BunnyCDN setup required.

Write down what you find:

CDN in use?	☐ Yes	☐ No
Provider:		
Security features (firewall/DDoS) enabled?	☐ Yes	☐ No

Task notes (for later):

Examples: “Ask host to enable CDN,” “Review security settings in Cloudflare,” “Check if CDN is included in hosting plan.”

Need help?

Ask your host or developer: “Do I already have a CDN enabled on my site, or can you connect it to one like Cloudflare or BunnyCDN? Can you also turn on their security and caching features?”

Stage 11: Audit summary

This summary shows where your biggest vulnerabilities are. You don't need to fix everything right away. Start with the sections that scored "No" most often.

Steps:

1. Go back through the workbook and count how many boxes you ticked "No."
2. Use the table below to find your overall risk level.
3. Write down your total and list your top three areas that need improvement.

"No" count	Risk level
0-4	• **Low risk** - your site is in good shape. Keep maintaining updates and backups regularly.
5-10	• **Medium risk** - you have a few areas to tighten up. Prioritise easy wins first.
11+	• **High risk** - your site could be exposed to common attacks. Plan to address major gaps soon.

My totals

"No" count:	
Risk level:	

Top 3 issues I noticed:

Optional reflection

What surprised me most:	
Which task will make the biggest difference:	

Stage 12: Action plan

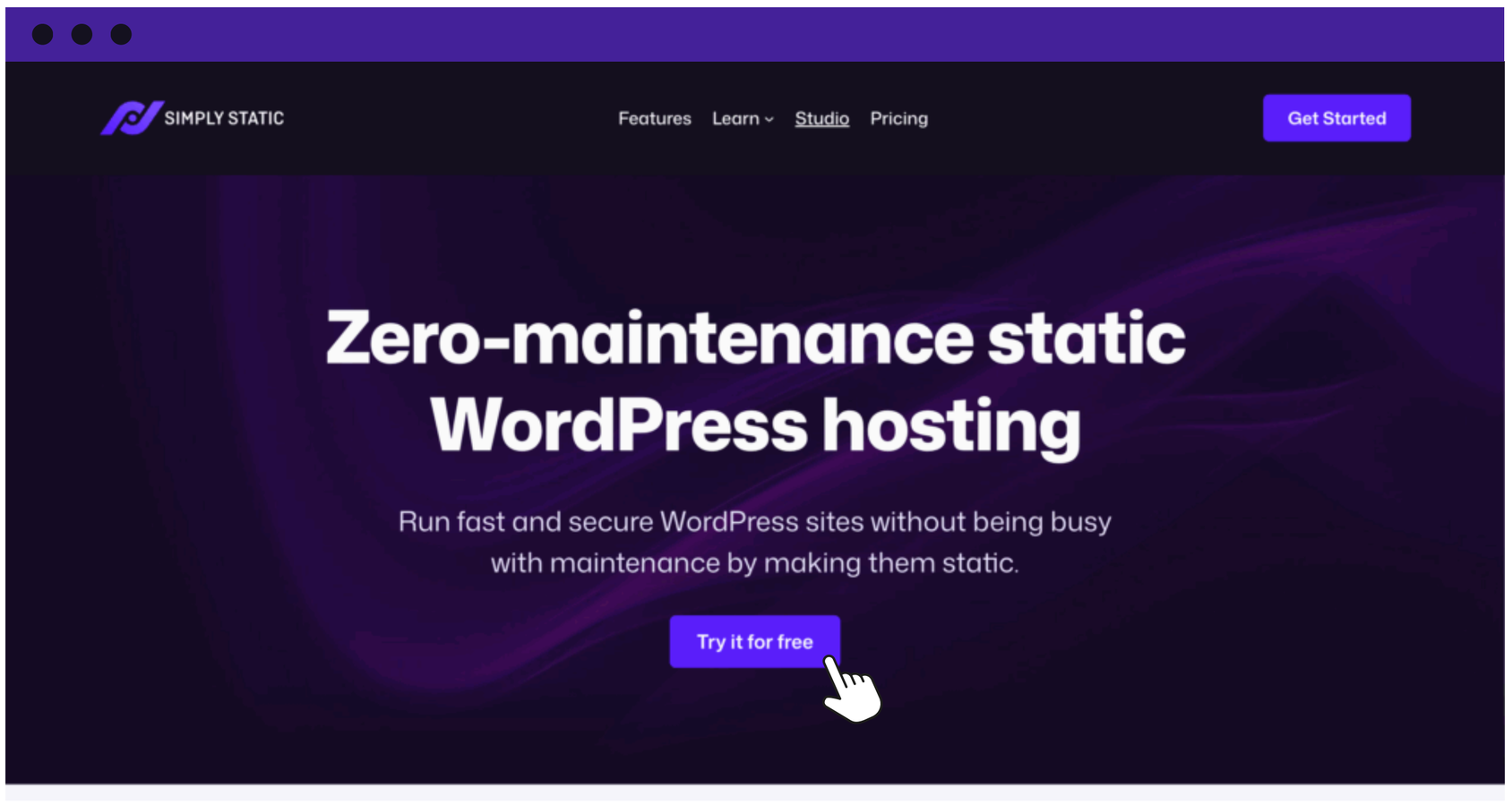
Steps:

1. Look back through your workbook and pick out the tasks from each stage.
2. Add them to the table below and set priorities:
    a. **High:** Fix soon, these are your biggest security risks.
    b. **Medium:** Important but not urgent.
    c. **Low:** Optional or ongoing improvements.
3. Note who will handle each one (you, your host, a team member, or your developer) and set a rough target date.

Priority	Task	Who will do it	Target date

Studio shortcut

If you use Simply Static Studio, many of your “No” answers from this audit become automatic “Yes.” The next page explains why.



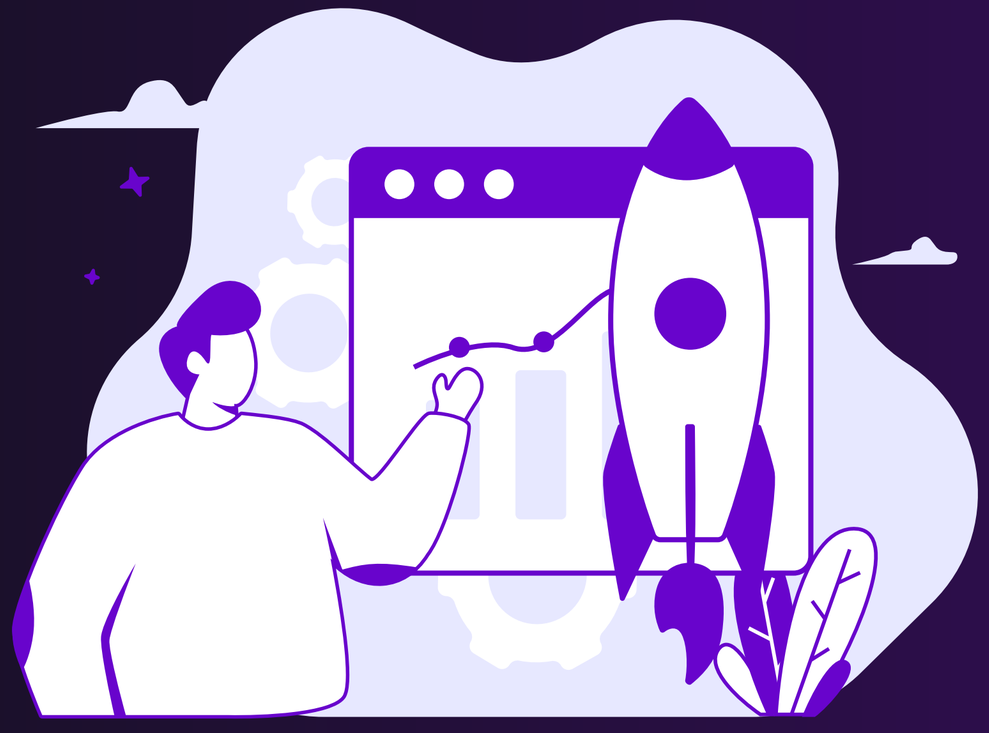
Simplify your WordPress security with Simply Static Studio

Now that you've identified your biggest risks, you have two choices: spend time maintaining each fix manually, or simplify your setup entirely. That's where Simply Static Studio comes in.

A simpler, safer way to run WordPress

Simply Static Studio takes everything you love about WordPress, flexibility, design freedom, easy publishing, and removes the parts that cause stress: constant updates, plugin conflicts, and security risks.

When you host with Simply Static Studio, your WordPress site is locked safely behind a secure dashboard. What visitors see is a static version. You still edit and manage your site in WordPress, but when you publish, Studio converts it into lightweight static files.



Ready to see what Simply Static Studio can do?

1. Start a free 7-day trial.
2. Migrate your existing WordPress site.
3. Enjoy faster, more secure, maintenance-free WordPress.

Get Simply Static Studio