The WordPress Security Workbook

BEST PRACTICES FOR SERVER-SIDE AND CLIENT-SIDE SECURITY

PART 1

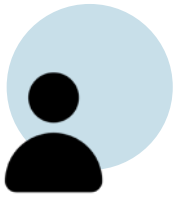
UNDERSTANDING THE STAKES

Why Bother Securing Your WordPress Site?

WordPress is open-source, which is great for flexibility but bad for security. Anyone can publish themes or plugins, and attackers exploit this.

3

THREE FACTS TO REMEMBER



Your customers share sensitive data

It’s your duty to protect their email, address, payment info, or any other data they shared on your website.

Your hosting is your first line of defense

Perfect security measures on your website don’t matter if you pick a bad webhost, select your hosting accordingly.

Plugins alone won’t save you

Security plugins are great to implement some features, but they are not sufficient to make your website safe.

QUICK LOOK

THE 3 MOST COMMON ATTACKS

BRUTE FORCE

How to prevent: Enforce strong password policies, rate-limiting, CAPTCHA, and multi-factor authentication.

Symptoms: Unusual spikes in login failures, excessive requests from a single IP, and account lockout.

How to solve: Block attacking IPs, reset compromised credentials, and implement lockout mechanisms.

SQL INJECTION

How to prevent: Use parameterized queries or stored procedures, strictly validate and sanitize all user inputs.

Symptoms: Unexpected database errors in responses, login bypass without valid credentials.

How to solve: Patch the vulnerable code by replacing dynamic query construction, revoke attacker access, and restore any compromised data from clean backups.

CROSS-SITE SCRIPTING (XSS)

How to prevent: Properly escape all user input, implement a strict Content Security Policy, and use secure coding frameworks.

Symptoms: Unexpected pop-us, unauthorized cookie or session token theft, and strange content appearing.

How to solve: Remove or neutralize the malicious script input, sanitize stored XSS payloads from the database, patch the vulnerable code with proper encoding.

PART 2

SECURITY CHECKLISTS

How to Use This Checklist

- *Check off each action as you complete it.*
- *Write the date you finished it.*
- *Add short notes (e.g., which plugin you used).*

SERVER-SIDE SECURITY (YOUR HOST'S JOB)

☐ Use secure WordPress hosting (with DDoS mitigation)

☐ Enable a Web Application Firewall (WAF)

☐ Install an SSL certificate (HTTPS)

☐ Keep PHP version updated to latest stable version

☐ Schedule automatic daily backups
Backup location: _____

Pro tip: If you don't know whether your host does these, email support now. Copy-paste this table into the email.

PART 2

SECURITY CHECKLISTS

How to Use This Checklist

- *Check off each action as you complete it.*
- *Write the date you finished it.*
- *Add short notes (e.g., which plugin you used).*

CLIENT-SIDE SECURITY (YOUR JOB)

- [ ] Limit login attempts (use a plugin like Limit Login Attempts)
  Max attemps:

- [ ] Block IPs after repeated failed logins

- [ ] Validate all form inputs (restrict special characters)

- [ ] Install plugins/themes only from wordpress.org or trusted sellers

- [ ] Run a weekly malware scan (use a security plugin)
  Plugin name:

- [ ] Never leave unused plugins/themes installed
  Last cleanup date:

  Pro tip: If you don't know whether your host does these, email support now. Copy-paste this table into the email.

PART 3

SECURITY CARDS

Use these cards to have an action plan regarding the most common security issues encountered by WordPress websites owners.

BRUTE FORCE ATTACK

What happens?

A bot tries thousands of password combinations.

Your specific action plan

- Install a plugin that limits login attempts (e.g., Wordfence, Limit Login Attempts Reloaded).
- Set max attempts to 5 or less.
- Set block duration to at least 15 minutes.

Write your settings

Plugin used: _____

Max attempts: _____

Block duration: _____

SQL INJECTION

What happens?

Malicious SQL code is typed into a form (search box, login, contact form) to read or delete your database.

Your specific action plan

- Use a security plugin to scan for SQL vulnerabilities weekly.
- Sanitize all input fields (most good form plugins do this automatically – check yours).
- Restrict characters like ‘ ; -- in public forms.

Write your actions

Forms on your site (e.g., contact, search, etc...): _____

Last SQL scan date: _____

PART 3

SECURITY CARDS

Use these cards to have an action plan regarding the most common security issues encountered by WordPress websites owners.

CROSS-SITE SCRIPTING - XSS

What happens

You unknowingly upload a theme or plugin that contains hidden malicious JavaScript.

Your specific action plan

- Never download “nulled” or free premium plugins from shady websites.
- Delete any theme/plugin you don’t actively use.
- Run a security scanner that checks for JavaScript injections.

Write your actions

List all active plugins

Date of last XSS scan: _____

MALICIOUS FILE INCLUSION

What happens

An attacker exploits a theme or plugin function to upload or remotely include a malicious file, giving them backdoor access to your server.

Your specific action plan

- Disable remote file inclusion in your php.ini
  `allow_url_include = Off`
- Regularly audit your file permissions (folders: 755, files: 644).
- Use a file integrity monitoring (FIM) tool to detect unexpected file changes.

Write your actions

Date of last file permissions audit: _____

Last file change alert: _____

allow_url_include (On / Off)

PART 3

SECURITY CARDS

Use these cards to have an action plan regarding the most common security issues encountered by WordPress websites owners.

TWO-FACTOR AUTHENTICATION (2FA) / MFA

What happens

An attacker obtains your admin password, without a second layer of verification, they login immediately and take control of your site.

Your specific action plan

- Enable 2FA for all admin and editor accounts using a plugin like Wordfence, Two-Factor, or Google Authenticator.
- Enforce 2FA for high-privilege users (do not make it optional).
- Use an authenticator app instead of SMS for better security.

Write your actions

List all admin/editor accounts

Date 2FA was enforced: _____

PLUGIN & THEME MANAGEMENT

What happens

Having a plugin or theme that is poorly coded, abandoned, or contains backdoors. This creates an entry point for attackers.

Your specific action plan

- Audit your active plugins quarterly.
- Delete all unused themes (especially default Twenty themes if you aren't using them).
- Only install plugins from the official WordPress repository or reputable developers, and check for recent updates.

Write your actions

Total active plugin count: _____

Date of last plugin audit: _____

PART 4

MONTHLY SECURITY REVIEW & ACTION TRACKER

The 5-Minute Monthly Audit
Do this on the 1st of every month.

Task	Done?	
	Yes	No
Check that automatic backups ran successfully		
Verify login attempt limit is still active (try a wrong password 4 times)		
Run a manual malware scan (your security plugin)		
Update all plugins, themes, and WordPress core		
Confirm SSL certificate is valid		

PART 5

EMERGENCY STEPS SUSPECT A BREACH?

If you see strange behavior (new admin users, ads you didn't have, login errors).

Immediately change all passwords
Use a password manager to generate strong, unique passwords for each account, do not reuse the old or similar ones.

Contact your hosting provider
Ask them to place your site into read-only mode or quarantine to prevent further damage while you investigate.

Restore from the latest clean backup
If you don't have a confirmed-clean backup, ask your host if they retain older snapshots and restore the most recent one from before the first sign of suspicious activity.

Run a full malware scan
Use a reputable security plugin (e.g., Wordfence, Sucuri, or MalCare) and also run a server-level scan if your host provides that option.

Check for unknown admin users
After deleting them, review all remaining users' roles and reset their passwords, especially for editors and authors who might have been overlooked.

YOU'VE COMPLETED THE WORKBOOK

Keep this somewhere accessible. Review the monthly tracker on the 1st of each month. A fortified WordPress site is not a one-time task, it's a habit.

"There is no standard recipe to secure a website, but your hosting and your daily habits are the frontline."