WPSecureStack

# WordPress Security Checklist

wpsecurestack.com

50-Point hardening guide covering server, core, plugins, themes, and user access. Print this out and tick each item. **Bold items marked CRITICAL** should be done first.

## ■ SERVER & HOSTING SECURITY

- [ ] 1 CRITICAL Use a managed WordPress hosting provider with built-in firewalls
- [ ] 2 CRITICAL Keep PHP version up to date (7.4 minimum, 8.1+ recommended)
- [ ] 3 CRITICAL Enable HTTPS / SSL certificate on your domain
- [ ] 4 Disable PHP execution in uploads and wp-content folders
- [ ] 5 Restrict server directory listing (Options -Indexes in .htaccess)
- [ ] 6 Use a Web Application Firewall (WAF) such as Cloudflare or Sucuri
- [ ] 7 Enable server-level brute-force protection (fail2ban or equivalent)
- [ ] 8 Limit xmlrpc.php access or disable it completely
- [ ] 9 Block access to readme.html and license.txt files
- [ ] 10 Enable automatic server-level malware scanning

## ■■ WORDPRESS CORE

- [ ] 11 CRITICAL Keep WordPress core updated to the latest stable version
- [ ] 12 CRITICAL Enable automatic minor/security updates in wp-config.php
- [ ] 13 Remove unused default themes (Twenty-Twenty series, etc.)
- [ ] 14 Delete the readme.html file from the WordPress root folder
- [ ] 15 Change the default database table prefix (wp_ → custom prefix)
- [ ] 16 Disable the built-in file editor (Appearance > Editor)
- [ ] 17 Turn off WordPress debug mode on live/production sites
- [ ] 18 Remove the WordPress version number from page source
- [ ] 19 Restrict REST API access to authenticated users where possible
- [ ] 20 Review and harden your wp-config.php file (see our snippets guide)

## ■ PLUGINS & THEMES

- [ ] 21 CRITICAL Delete every plugin and theme you are not actively using
- [ ] 22 CRITICAL Update all plugins and themes to their latest versions
- [ ] 23 Only install plugins from wordpress.org or trusted commercial sources
- [ ] 24 Check plugin update frequency — avoid plugins not updated in 2+ years
- [ ] 25 Install a reputable security plugin (Wordfence, iThemes, Solid Security)
- [ ] 26 Install an activity log plugin to track all user and admin changes
- [ ] 27 Use a plugin vulnerability scanner (WPScan or Patchstack)
- [ ] 28 Avoid nulled (pirated) themes and plugins — they contain backdoors
- [ ] 29 Review plugin permissions — remove ones that request admin access
- [ ] 30 Use a staging environment to test updates before going live

## ■ USER ACCESS & LOGIN

- [ ] 31 CRITICAL Change the default 'admin' username to something unique
- [ ] 32 CRITICAL Use strong passwords (12+ characters, mix of letters, numbers, symbols)
- [ ] 33 CRITICAL Enable Two-Factor Authentication (2FA) for all admin accounts
- [ ] 34 Limit login attempts (3–5 tries before temporary lockout)
- [ ] 35 Change the default WordPress login URL (/wp-admin → custom URL)
- [ ] 36 Implement IP allowlisting for wp-admin if you have a static IP
- [ ] 37 Remove or disable inactive admin and editor user accounts
- [ ] 38 Assign users the lowest role needed (don't give Editor when Author suffices)
- [ ] 39 Force password resets after a security incident
- [ ] 40 Log out idle sessions automatically after 30–60 minutes

## ■ BACKUPS & MONITORING

- ☐ 41 CRITICAL Take daily automated backups and store them off-site (not just on the server)
- ☐ 42 CRITICAL Test your backup restore process at least once every 3 months
- ☐ 43 Set up uptime monitoring (UptimeRobot, Pingdom, or similar)
- ☐ 44 Enable email or SMS alerts for failed logins and admin changes
- ☐ 45 Schedule weekly malware scans using a trusted security plugin
- ☐ 46 Monitor your Google Search Console for security warnings
- ☐ 47 Keep a changelog — document every plugin/theme update with a date
- ☐ 48 Store at least 30 days of backups (daily) and 12 weeks (weekly)
- ☐ 49 Verify backup files are not stored in a publicly accessible folder
- ☐ 50 Maintain a separate backup of your database independent of file backups

---

**MY SCORE** Items Completed: _____ / 50 Date Reviewed: _____

| Score | Rating | What to do |
|---|---|---|
| 40 – 50 | ■ Excellent | Do a monthly review to stay on top |
| 30 – 39 | ■■ Good | Fix remaining items within 2 weeks |
| 20 – 29 | ■ Fair | Address CRITICAL items this week |
| Below 20 | ■ At Risk | Contact us immediately for a security audit |

---

**Emmanuel Tatyabala | Co-Founder, WPSecureStack**
emmanuel@wpsecurestack.com | WhatsApp: +256 785 832 643
wpsecurestack.com/resources