WordPress Security Audit Checklist

Use this on every site takeover or security review — GoTechWizard · May 2026

■ Critical ■ High ■ Medium ■ If access / Ongoing

1. USERS & ACCESS

☐	Export full user list, sort by role (Admin first) *Users > All Users > export*	Critical
☐	Get client to name every admin and editor account *Anyone unnamed gets demoted*	Critical
☐	Demote unrecognised accounts to Subscriber (do NOT delete) *Keeps audit trail intact*	Critical
☐	Change any default usernames: admin, administrator, webmaster	Critical
☐	Force password reset on ALL remaining accounts *Emergency Password Reset plugin*	Critical
☐	Enforce stronger password requirements via plugin *Password Policy Manager*	High
☐	Set 60 or 90-day password expiry policy	High
☐	Enable two-factor authentication — mandatory for Admin + Editor *WP 2FA plugin*	High
☐	Kill ALL active sessions after cleanup *WP-CLI: wp user session destroy --all*	Critical

2. PLUGINS & THEMES

☐	Remove the File Manager plugin immediately — no exceptions *Use cPanel or SFTP instead*	Critical
☐	Update ALL plugins to latest versions *Dashboard > Updates*	Critical
☐	Disable all unused/inactive plugins	Critical
☐	Delete all deactivated plugins *Deactivated != gone*	High
☐	Check CVEs for every installed plugin *WPScan or wpvulndb.com*	High
☐	Identify plugins replaceable with code *Reduces attack surface*	Medium
☐	Convince client to remove plugins not truly needed *Convenience vs risk conversation*	Medium

☐	Update active theme to latest version	High
☐	Delete ALL inactive/unused themes *Even default themes*	Medium
☐	Confirm active theme has an update path *Abandoned themes are a risk*	Medium

3. WORDPRESS CORE

☐	Update WordPress core to latest stable release *Dashboard > Updates*	Critical
☐	Verify core file integrity *WP-CLI: wp core verify-checksums*	Critical
☐	Remove version number from generator meta tag *Via functions.php*	High
☐	Hide WP version from RSS feeds and REST API	High

4. LOGIN & AUTHENTICATION

☐	Change login URL away from default wp-login.php *WPS Hide Login plugin*	High
☐	Enable login rate limiting and IP banning *Limit Login Attempts Reloaded*	High
☐	Block xmlrpc.php — disable XML-RPC unless required *.htaccess or plugin*	High
☐	Identify which countries client serves, block all others *Cloudflare or Wordfence rules*	High

5. WORDPRESS CONFIGURATION

☐	Disable file editing via wp-config.php *define('DISALLOW_FILE_EDIT', true)*	High
☐	Rotate security salts — assume compromised on inherited sites *api.wordpress.org/secret-key*	High
☐	Change database table prefix away from wp_ *Via phpMyAdmin + wp-config update*	Medium
☐	Restrict PHP execution in uploads/ directory *.htaccess: deny execute in uploads*	High

6. MALWARE & SECURITY SCANNING

☐	Run full malware scan *Wordfence or Sucuri*	Critical

☐	Verify core checksum — confirm no core files tampered *WP-CLI: wp core verify-checksums*	Critical
☐	Set up Wordfence with logging, alerting, and firewall rules	High
☐	Configure email alerts for failed logins and file changes	High

7. SERVER-LEVEL HARDENING

☐	Set up Cloudflare on the domain *Update nameservers, enable proxied DNS*	High
☐	Enable Imunify360 at server level *Hosting-level protection*	If access
☐	Configure CSF (ConfigServer Security & Firewall) *Server-level firewall*	If access
☐	Install and configure fail2ban *Blocks repeated failed auth attempts*	If access
☐	Lock down PHP: disable dangerous functions, restrict open_basedir *php.ini or hosting panel*	If access
☐	Confirm hosting environment is solid — good server = easier management	High

8. BACKUP & RECOVERY

☐	Set up automated off-site backups *UpdraftPlus + remote destination*	Medium
☐	Test that a restore actually works *Untested backup = no backup*	Medium
☐	Confirm backup frequency matches content update frequency	Medium

9. PERFORMANCE & CACHING

☐	Install a caching plugin *LiteSpeed Cache, W3 Total Cache*	Medium
☐	Verify caching is working and not causing issues	Medium

10. ONGOING MAINTENANCE

☐	Review Wordfence alerts weekly	Ongoing
☐	Apply plugin and theme updates as released	Ongoing
☐	Audit user list every 6 months or on staff change	Ongoing
☐	Test backup restores quarterly	Ongoing

☐	Review Cloudflare analytics for suspicious traffic patterns	Ongoing
☐	Check CVEs for installed plugins on each update cycle	Ongoing

AUDIT NOTES

Client: _____ Site URL: _____ Date: _____ Audited by: _____

Notes / observations: