Gearbly
Precision Tech. Human Ability.

THE GEARBLY FORTRESS PROTOCOL

The 50-Point Server Security Checklist for High-Performance WordPress Agencies

Version: 1.0 | **Author:** Gearbly Engineering Team

Most "hacked" WordPress sites aren't breached through the login page; they are breached through insecure server configurations. This checklist is the exact protocol we use at **Gearbly** to secure high-traffic infrastructure on CloudPanel, CyberPanel, and VPS environments.

Phase 1: The Iron Gate (Server Level)

Before you even install WordPress, the environment must be hardened.

- [ ] **Disable Root Login:** Create a new `sudo` user. Never log in as `root`.
- [ ] **SSH Key Authentication Only:** Disable password authentication in `/etc/ssh/sshd_config`.
- [ ] **Change Default SSH Port:** Move SSH from Port 22 to a random port (e.g., 2200-2299) to stop bot scanners.
- [ ] **Configure UFW (Firewall):** Deny all incoming traffic by default; allow only HTTP (80), HTTPS (443), and your Custom SSH Port.
- [ ] **Install Fail2Ban:** Configure it to ban IPs after 3 failed login attempts.
- [ ] **Disable Unused Ports:** Close FTP ports (21) if you are using SFTP (which is more secure).

Phase 2: The Application Shield (WordPress Level)

WordPress is secure, but default settings are a liability.

- [ ] **Change Database Prefix:** Never use `wp_`. Change it to something random like `gb_7x9_`.
- [ ] **Disable XML-RPC:** If you don't use the mobile app or Jetpack, disable this in `.htaccess` or Nginx config to stop DDoS attacks.

- [ ] **Disable File Editing:** Add `define('DISALLOW_FILE_EDIT', true);` to your `wp-config.php`.
- [ ] **Hide WP Version:** Remove the generator meta tag so hackers don't know which version you run.
- [ ] **Limit Login Attempts:** Install a lightweight plugin to block brute force attacks on `/wp-admin`.

Phase 3: The Safety Net (Backups & Maintenance)

Security is not a state; it is a process.

- [ ] **Off-Site Backups:** Do not store backups on the same server. Push them to AWS S3, Google Drive, or a separate storage VPS.
- [ ] **Automated Updates:** Enable auto-updates for minor WordPress versions.
- [ ] **Uptime Monitoring:** Set up an external ping (like UptimeRobot) to alert you if the server goes dark.
- [ ] **Cron Job Optimization:** Switch from `wp-cron` to System Cron for better performance and reliability.

⚠ Warning: The "Complexity Gap"

Securing a server is technical work. One wrong command in the SSH terminal can lock you out of your own server permanently.

Don't want to risk it? Let the Gearbly Engineering Team handle your infrastructure. We provide managed migration and security hardening services so you can sleep knowing your data is locked behind our "Iron Gate."

Book a Security Audit with Gearbly →