WordPress Enterprise Hardening

50-Point Enterprise security Hardening Checklist

1. Core & Environment Hardening

- **WP-Config Protection:** Move wp-config.php one level above the document root directory to prevent accidental public disclosure.
- **Disable File Editing:** Define DISALLOW_FILE_EDIT as true in wp-config.php to prevent dashboard-level file modification.
- **Restrict File Permissions:** Ensure all directories are set to 755 and all files to 644. wp-config.php should be restricted to 400 or 600.
- **Disable XML-RPC:** Block xmlrpc.php requests entirely using Nginx or a security plugin to mitigate brute-force and amplification attacks.
- **Enforce SSL/TLS:** Configure force SSL for both logins and admin sessions using FORCE_SSL_ADMIN.

2. Authentication & Access Management

- **Two-Factor Authentication (2FA):** Mandate 2FA for all administrator, editor, and author level accounts.
- **Custom Login URL:** Move the default login path from wp-login.php / wp-admin to a custom randomized URL.
- **Limit Login Attempts:** Enforce IP lockouts after 5 consecutive failed login attempts.
- **Username Enumeration Block:** Disable author archive scans (e.g. ?author=1) to prevent attackers from harvesting usernames.
- **Strong Password Policy:** Audit and enforce minimum entropy requirements for all dashboard users.

3. Database & System Hardening

- **Custom Prefix:** Avoid using the default wp_ prefix. Set a unique, alphanumeric prefix during database creation.
- **Restricted DB User Permissions:** Grant the WP database user only the minimum SQL privileges required: SELECT, INSERT, UPDATE, DELETE. Revoke DROP, ALTER, and GRANT in production.
- **Disable Debug Display:** Turn off WP_DEBUG_DISPLAY in production and log errors privately using WP_DEBUG_LOG.

4. Server & Header Hardening

- **Directory Browsing:** Disable directory indexes globally in Nginx configuration (e.g. autoindex off;).
- **Security Headers:** Enforce Content Security Policy (CSP), X-Frame-Options (prevent clickjacking), X-Content-Type-Options, and Strict-Transport-Security (HSTS).

- **Upload Directory Protection:** Disable PHP script execution inside /wp-content/uploads/ using Nginx rules.

5. Plugin & Theme Management

- **Minimization:** Review and uninstall inactive plugins and themes. Leftover code represents unnecessary attack surface.
- **Vulnerability Scanning:** Schedule automated vulnerability scans mapping active plugins against CVE databases (WPScan, CVE list).
- **Auto-updates for Security Patches:** Enable auto-updates exclusively for minor/security WordPress core releases and trusted plugins.