
🔐 WordPress Security Checklist (Step-by-Step)

🧱 1. Foundation & Server Hardening

- Use a reputable hosting provider with built-in security features.
- Enable HTTPS with a valid SSL/TLS certificate.
- Disable directory indexing on the server.
- Set secure file permissions:
    - wp-config.php → 400 or 440
    - /wp-admin/ → restricted access
    - /wp-content/uploads/ → allow uploads only
- Disable XML-RPC if not needed.

🔄 2. Keep Everything Updated

Update WordPress core immediately when new versions are released.

- Update all plugins and themes weekly after testing in staging website.
- Remove unused plugins/themes to reduce attack surface.

🔑 3. Strengthen Authentication

- Enforce strong passwords for all users.
- Enable multi-factor authentication (MFA) for admins and editors.
- Limit login attempts.
- Change the default login URL.
- Disable “admin” as a username.

🛡️ 4. WordPress Hardening

- Disable file editing in the dashboard (define('DISALLOW_FILE_EDIT', true);).
- Move wp-config.php one directory above the web root if possible.
- Add security keys and salts.

- Restrict access to /wp-admin/ by IP when possible.

🔍 5. Monitoring & Detection

- Enable real-time malware scanning.
- Set up uptime monitoring.
- Log all admin activity.
- Monitor file changes.

📦 6. Backup Strategy

- Schedule daily backups (database + files).
- Store backups off-site (cloud storage).
- Test restore procedures monthly.

🌐 7. Network & Firewall Protection

- Use a Web Application Firewall (WAF).
- Block known malicious IPs.
- Enable DDoS protection (via CDN or host).

🧪 8. Regular Audits

- Perform quarterly security audits.
- Conduct penetration testing annually.
- Review user roles and permissions monthly.
