WordPress Security Self-Audit Checklist

20-Point WordPress Hardening Audit

☐ Is hosting security reputable?
☐ Is WordPress core updated?
☐ Are plugins updated weekly?
☐ Are unused plugins deleted?
☐ Are themes legitimate and maintained?
☐ Are admin passwords 16+ characters?
☐ Is MFA enabled?
☐ Is login URL hardened?
☐ Are login attempts limited?
☐ Is a security scanner active?
☐ Is a firewall configured?
☐ Is XML-RPC reviewed?
☐ Is wp-config hardened?
☐ Are file permissions restrictive?
☐ Is dashboard file editing disabled?
☐ Are user roles minimized?
☐ Are backups automated?
☐ Has restore been tested?
☐ Is WooCommerce checkout secured?
☐ Is monthly monitoring routine scheduled?

Scoring:

17–20 = Strong WordPress security maturity
12–16 = Moderate exposure remains
0–11 = High hack susceptibility