
WordPress Security Audit – Pedro Ornstein

Overview

This security audit outlines the process I followed to assess and harden the security posture of a WordPress website I previously owned and managed: `blockzag.com` (decommissioned in 2024). The site was used for testing growth hacks, traffic strategies, and marketing funnels — making it a relevant candidate for assessing common plugin-based vulnerabilities.

Objective

Identify key security weaknesses and implement best practices to reduce risk exposure and improve overall site resilience.

Audit Summary

Category	Before Audit	After Audit
Plugins Updated	No	Yes
SSL / HTTPS	No	Enforced
Two-Factor Auth (2FA)	Disabled	Enabled
Firewall	None	Wordfence

| Brute Force Protection | None | Active |

| Admin URL Obfuscation | Default | Changed |

| Backup Strategy | Manual | Scheduled |

Step-by-Step Actions Taken

1. Vulnerability Assessment

* Scanned plugins/themes for known CVEs using tools like WPScan and Security Ninja.

* Removed 4 outdated plugins including: Slider Revolution, Contact Form 7, and Insert Headers and Footers.

2. Secure Login Hardening

* Installed and configured Wordfence Security.

* Enabled Two-Factor Authentication (2FA) for all admin accounts.

* Changed default login URL from `/wp-login.php` to a custom slug.

* Limited login attempts to 3 via `.htaccess` configuration.

3. HTTPS + SSL Enforcement

* Installed Really Simple SSL.

* Redirected all HTTP traffic to HTTPS.

* Verified certificate installation via SSL Labs.

4. Backups + Recovery

* Set up UpdraftPlus for automated daily backups stored in Google Drive.

* Documented a full site restoration test in staging.

5. File & Permission Management

- Changed file permissions:

 * wp-config.php → 600

 * wp-content/ → 755

* Disabled PHP execution in uploads directory.

Results

* Site performance improved by 15% (via GTMetrix).

* Passed all critical checks on SecurityHeaders.com.

* Logged and mitigated first brute-force login attempt within 48 hours post-implementation.

Lessons Learned

* Popular plugins increase attack surface; fewer is better.

* Many default WordPress installs skip basic SSL enforcement.

* Small changes (e.g., changing admin URL) significantly reduce bot login attempts.

Tools Used

* Wordfence
* UpdraftPlus
* Really Simple SSL
* WPScan
* Security Ninja
* GTMetrix / SSL Labs / Security Headers

Status

Project Completed — June 2025

Available for client or recruiter review.
