WordPress Incident Response

Standard Operating Procedures for Compromised WordPress Deployments

Phase 1: Detection & Identification

Identify if the system has been compromised. Look for anomalies: unrecognized administrative users, file integrity mismatches, sudden spike in outgoing spam emails, or user reports of redirects to external advertising sites.

- Run file checks: git diff (if tracked) or compare files against the official WordPress repository checksums using WP-CLI: wp core verify-checksums.
- Examine Nginx access and error logs for suspicious request patterns (e.g. POST requests targeting /wp-content/uploads/ or odd admin parameters).

Phase 2: Isolation & Containment

Stop active attacks and prevent the breach from spreading or leaking further data.

- **Go Offline:** Put the website in maintenance mode immediately. Return a 503 Service Unavailable header using Nginx to keep SEO ranking intact while denying visitor access.
- **Lock Out Dashboard:** Block access to /wp-login.php and /wp-admin/ at the server level, or restrict access exclusively to your security analysts' IP addresses.
- **Isolate the Environment:** If running multiple sites on the same VPS, isolate the compromised directory to prevent cross-site file infection.

Phase 3: Clean & Eradication

Completely remove malware payloads, backdoors, and database entries.

- **Reinstall Core:** Delete all core files and folders (excluding wp-content and wp-config.php) and replace them with a fresh, clean download of the exact core version.
- **Clean Plugins & Themes:** Delete the existing plugins and themes entirely. Download fresh copies directly from the official repositories. Do NOT trust existing folder contents.
- **Backdoor Search:** Inspect wp-config.php and the database (especially wp_options and user tables) for malicious injections, cron jobs, or rogue admin accounts.

Phase 4: Recovery & Post-Incident Hardening

Safely restore normal website operations and patch the initial entry point.

- **Reset Credentials:** Force reset all passwords for database users, FTP/SSH accounts, and WordPress administrators.

- **Update Authentication Keys:** Regenerate the security keys/salts in wp-config.php to invalidate all existing user sessions.
- **Find Initial Vector:** Conduct a thorough root-cause analysis. Check plugin version CVE status to identify how the attacker gained entry, and patch it immediately.