Lockora Security Audit

lockora-audit.com/sample-report
Prepared by G. Schad

Security audit report — aurora-co.com

WordPress 6.4.2 · 17 plugins · Lockora Security Audit v0.4.2 · sample report (fictional demo site)

78

Score 78 / 100

Up 6 since the previous scan (72). Weighted by how often each check is involved in real compromises.

3	7	24
critical	warnings	passed

This is a demonstration. aurora-co.com is a fictional site used to show the report format. The findings are representative of the issues Lockora most commonly detects on real WordPress sites. Remediation types: **Reversible toggle** is a switch inside the plugin that can be turned back off; **Action in Lockora** is a button that makes one explicit change when clicked; **Guided review** means the plugin shows the evidence and you decide; **Manual fix** is guidance for you, your developer or your host.

Critical — act today

CRITICAL

Known vulnerability match: Contact Form 7 5.8.2 installed; CVE-2023-6449 fixed in 5.8.4

Updates and platform · /wp-content/plugins/contact-form-7

WHAT

The installed Contact Form 7 version allows an unrestricted file upload via the [file] form tag: a crafted filename such as cv.pdf.phtml can bypass sanitization and land in the uploads directory with an executable extension.

WHY IT MATTERS

On hosts that execute .phtml as PHP this is unauthenticated remote code execution from a public contact form. Automated scanners actively probe for this version.

WHAT TO DO

Update the plugin from Plugins > Updates, then block PHP execution inside wp-content/uploads at the web server. Vulnerability matching uses the optional Wordfence Intelligence API key; without one Lockora still flags the plugin as behind the current release.

Manual fix · https://lockora-audit.com/blog/contact-form-7-security-vulnerabilities

CRITICAL

Authentication keys and salts: 3 of 8 keys = "put your unique phrase here"

`Configuration and secrets · wp-config.php`

WHAT

Three of the eight authentication keys and salts in wp-config.php were never replaced with unique values, a common leftover from one-click installers.

WHY IT MATTERS

These keys sign session cookies. Predictable keys make forged authentication cookies feasible, undermining every login protection on the site.

WHAT TO DO

Use the plugin's Rotate keys action to generate eight fresh high-entropy values, or paste new ones yourself. Rotation logs out all active sessions.

Action in Lockora · https://lockora-audit.com/blog/wordpress-wp-config-php-security

CRITICAL

Inactive Administrator: created 2023-02-11; last activity 26 months ago; 4 Administrators on a 3-person team

`Accounts · user "webtemp7"`

WHAT

An Administrator account exists that matches no current staff, vendor or service pattern and has been dormant for over two years. The site also has more Administrators than its team size suggests.

WHY IT MATTERS

Dormant privileged accounts are a favourite persistence mechanism after a compromise and widen the attack surface for credential stuffing.

WHAT TO DO

Downgrade the account, delete it (reassigning its content), or confirm it is known. Lockora lists the evidence and never deletes users itself.

Guided review · https://lockora-audit.com/blog/wordpress-user-roles-permissions-security

Warnings — act this week

WARNING

XML-RPC: POST /xmlrpc.php → 200 OK; system.multicall enabled

`Public exposure · /xmlrpc.php`

WHAT

The legacy XML-RPC endpoint is publicly reachable and accepts batched authentication attempts via system.multicall.

WHY IT MATTERS

One HTTP request can carry hundreds of password guesses, bypassing login throttles that only watch wp-login.php. The endpoint can also be abused for pingback reflection DDoS.

WHAT TO DO

If nothing on the site uses XML-RPC, switch on the Disable XML-RPC toggle in Lockora. It is reversible.

Reversible toggle · https://lockora-audit.com/blog/xmlrpc-php-security-disable-rate-limit

WARNING

Author enumeration / login protection: Two Administrator usernames discoverable; no login-protection or 2FA plugin detected

`Accounts · /?author=1, /wp-json/wp/v2/users`

WHAT	Two Administrator usernames are discoverable from public author archives and the REST users route, and no login-protection or two-factor plugin was detected.
WHY IT MATTERS	Known usernames plus an unthrottled login form is a complete brute-force path.
WHAT TO DO	Switch on the REST user routes toggle, set display names that differ from login names, and add lockouts and two-factor authentication.

Reversible toggle · https://lockora-audit.com/blog/how-to-secure-wordpress-login-page

WARNING

debug.log reachability: GET → 200 OK; 1.2 MB

`Public exposure · /wp-content/debug.log`

WHAT	Debug logging writes to the default location inside wp-content and the web server serves the file to anyone who asks for it.
WHY IT MATTERS	The log contains absolute file paths, plugin internals and sometimes database queries, which attackers use to pick working exploits faster.
WHAT TO DO	Set WP_DEBUG_LOG to a path outside the web root or turn debug logging off in production, delete the exposed file, and deny direct access to *.log at the web server.

Manual fix · https://lockora-audit.com/blog/wordpress-wp-config-php-security

WARNING

readme.html / generator tag: GET → 200; <meta name="generator" content="WordPress 6.4.2">

`Public exposure · /readme.html`

WHAT	The stock readme.html is reachable and every page carries a generator meta tag naming the exact WordPress version.
WHY IT MATTERS	Version information lets mass scanners skip straight to the exploits that apply.
WHAT TO DO	Switch on the Remove generator tag toggle and delete or block readme.html at the web server.

Reversible toggle

Passed — a sample of the 24 clean checks

PASSED **Core file checksums: 1,412 files verified against WordPress.org hashes; 0 modified**

Integrity · WordPress core

WHAT Every core file matches the official checksums for this version.

WHAT TO DO No action. Export the file list as CSV or TXT if needed.

None

PASSED **wp-content anomaly scan: 0 anomalies**

Integrity · wp-content

WHAT No executables in uploads, no unexpected PHP outside code directories, no backup or secret-like files.

WHAT TO DO No action.

None

PASSED **HTTPS and security headers: HSTS, X-Content-Type-Options, X-Frame-Options, Referrer-Policy present**

Configuration and secrets · Site-wide

WHAT The site redirects to HTTPS and sends the basic browser-hardening headers.

WHAT TO DO No action.

None

PASSED **SSL certificate expiry / PHP version: Certificate expires 2026-11-01 (61 days); PHP 8.2 supported**

Updates and platform · Server

WHAT Certificate renewal is not due yet and the PHP version is supported per WordPress.org Serve Happy data.

WHAT TO DO No action.

None

PASSED

Automatic updates / mu-plugins: Minor releases auto-update; wp-content/mu-plugins absent

Updates and platform · WordPress core

WHAT

Security releases install without waiting for a person and no must-use plugin directory exists.

WHAT TO DO

No action.

None
