

Oakwood Bakery — One-Off Website Health Check (Sample Report)

One-Off Website Health Check • A private report for your business

CLIENT NAME	WEBSITE DOMAIN	SERVICE PLAN	INFRASTRUCTURE
Oakwood Bakery Ltd	www.oakwoodbakery.example	One Off Health Check	LiteSpeed Server

ABOUT THIS ASSESSMENT

- This report is a snapshot of www.oakwoodbakery.example's condition at the time of testing: 14 Oct 2026, 15:14. Website conditions can change afterwards.
- Some checks assess the wider website or WordPress installation (e.g. plugin updates, backups); others examine a specific page or component only (e.g. homepage performance testing) — each finding below says which.
- This assessment does not replace a comprehensive security penetration test, a full SEO audit, or ongoing website monitoring.
- A backup tool being detected and running indicates a backup is likely being taken — it doesn't confirm a backup completed successfully or that it can be restored.
- Every check in this report is automated; none of these findings involved a manual or expert review unless stated otherwise.
- Your health score (68/100) is calculated from confirmed technical signals only — software updates, SSL, backups, security hardening, known vulnerabilities and server errors — weighted by severity. Optional services and improvement suggestions don't affect it.

OVERALL HEALTH STATUS

Needs Attention

68/100

www.oakwoodbakery.example is mostly fine, but a few confirmed issues need attention.

1 high-priority issue needs prompt attention.

KEY FINDINGS

- 1

Example Share Buttons has 1 known security issue

HIGH
- 2

2 PHP errors logged, invisible to visitors

MEDIUM
- 3

3 plugin/theme updates waiting

MEDIUM

WHAT'S WORKING WELL

- ✔

WordPress core is up to date.
- ✔

SSL certificate is valid and not close to expiring.
- ✔

Uptime has been reliable this period (99.97%).
- ✔

No broken links found across 24 pages checked.
- ✔

The server is running a supported PHP version.
- ✔

A recent backup is in place, based on timestamp alone — this doesn't confirm the backup is restorable.
- ✔

Email anti-spoofing protection (SPF/DKIM/DMARC) is fully configured and enforced.

⚠️ WHAT NEEDS ATTENTION

- HIGH** Example Share Buttons has 1 known security issue
- MEDIUM** 3 plugin/theme updates waiting
- MEDIUM** 2 security hardening checks failed: XML-RPC Interface Disabled, Directory Listing Prevented
- MEDIUM** 3 scheduled WordPress tasks overdue

MEDIUM 2 PHP errors logged, invisible to visitors

MEDIUM 1 plugin no longer actively maintained

LOW 1 protective browser security header missing: Content-Security-Policy (restricts where scripts can load from)

WHAT WE CHECKED

✅ WordPress, PHP & server

● ALL CURRENT

Why it matters: An out-of-date platform is the single biggest reason WordPress sites get hacked.

- WordPress is up to date, running version 6.7.1.
- PHP 8.3.14 is supported until 31 Dec 2027.
- Hosted on LiteSpeed behind Cloudflare.

❌ Plugins & themes

● NEEDS ATTENTION

Why it matters: Outdated or vulnerable plugins and themes are a frequent factor in WordPress site compromises.

- 9 plugins installed, 8 switched on.
- 2 themes installed.
- 3 plugin/theme updates are waiting to be installed.
- Example Contact Forms (1.9.2 → 1.9.5), Example Page Builder (3.24.0 → 3.25.2), Example Image Compressor (3.16.1 → 3.16.3).
- 1 known security issue found on plugin/theme currently switched on: Example Share Buttons 2.1.3 (SAMPLE-ADVISORY-2026-0142, Medium/CVSS 5.4) — patched in 2.1.4.
- 1 plugin hasn't been updated by its developer in over a year.

⚠️ Security

● NEEDS ATTENTION

Why it matters: Many break-ins exploit a handful of well-known gaps — closing them reduces risk, though it can't eliminate it.

- 16 of 18 security hardening checks passed.
- Failed: XML-RPC Interface Disabled, Directory Listing Prevented. XML-RPC is a precautionary check, not an automatic fail — some integrations rely on it.
- 2 WordPress administrator accounts detected.
- SSL certificate is valid, renewing in 187 days.
- 2 of 3 recommended protective headers are switched on.
- Missing: Content-Security-Policy (restricts where scripts can load from).

✅ Backups

● UP TO DATE

Why it matters: A backup is the difference between a bad day and losing the site completely.

- Latest backup was taken on 13 Oct 2026 (via UpdraftPlus).
- Backups are copied off-site.
- This confirms a backup file exists and is recent — it doesn't confirm the backup can be successfully restored. Restoration should be test-checked periodically.

⚠️ Homepage speed

● COULD BE FASTER

Why it matters: Based on the homepage only, not every page on the site — a slow homepage can lose visitors before they see what you offer.

- Tested URL: <https://www.oakwoodbakery.example/>
- Homepage desktop speed score: 93/100 (good).
- Homepage mobile speed score: 72/100 (needs improvement).
- Largest Contentful Paint (LCP) — how long the main content takes to appear — is rated GOOD on desktop and NEEDS IMPROVEMENT on mobile.
- These ratings are based on real-user Core Web Vitals (CrUX field) data, not a one-off lab test.

⚠️ Uptime, errors & scheduled tasks

● ERRORS LOGGED

Why it matters: Downtime, silent errors and stalled scheduled tasks cost sales and trust — usually before anyone notices.

- 99.97% uptime this period.
- 2 distinct PHP errors logged (352 occurrences): a deprecated function notice in the active theme and an undefined array key warning in a plugin.
- Neither error currently breaks a page or shows up to visitors — this is the kind of hidden fault a basic uptime check won't catch.
- 3 scheduled WordPress tasks are overdue (oldest: `woocommerce_cleanup_sessions`, 2h overdue) — these fail silently too, with no visible error on the site itself.

✔ Domain, email & links

● ALL CLEAR

Why it matters: These are quiet failures — nothing crashes, but customers quietly have a worse experience or your emails don't arrive.

- Domain name renews on 13 Oct 2028 (123-reg).
- Email anti-spoofing protection is fully set up — SPF and DKIM are valid, and DMARC is enforced (policy: quarantine).
- No broken links found across 24 pages checked.

⚠ Database

● COULD BE TIDIED

Why it matters: A bloated database is one of the most common hidden causes of a sluggish site.

- Database size: 312 MB across 48 tables.
- Autoloaded options total 4.2 MB across 612 rows (recommended under ~1 MB) — this entire block loads on every single page request, admin screens included.

📅 YOUR ACTION PLAN

Technical Issues

Confirmed problems with a clear, straightforward fix — included in a remediation quotation below.

ISSUE	PRIORITY	WHAT IT MEANS FOR YOUR BUSINESS	RECOMMENDED ACTION
Example Share Buttons has 1 known security issue	HIGH	The installed version (2.1.3) has a publicly disclosed Cross-Site Scripting (XSS) vulnerability — SAMPLE-ADVISORY-2026-0142, rated Medium severity (CVSS 5.4) in the vulnerability database. A patched release (2.1.4) is available. Exploitability on this installation depends on how the plugin's affected feature is used and what other safeguards are in place.	Update Example Share Buttons from 2.1.3 to the patched 2.1.4 release.
3 plugin/theme updates waiting	MEDIUM	Updates usually include security fixes — the longer they wait, the bigger the gap for something to go wrong.	Review compatibility and update: Example Contact Forms (1.9.2 → 1.9.5), Example Page Builder (3.24.0 → 3.25.2), Example Image Compressor (3.16.1 → 3.16.3).
1 plugin no longer actively maintained	MEDIUM	If a security problem is ever found, an unmaintained plugin won't get a fix — worth planning a replacement.	Review the 1 unmaintained plugin and plan a replacement.
2 security hardening checks failed: XML-RPC Interface Disabled, Directory Listing Prevented	MEDIUM	2 of the 18 standard security precautions we check for aren't in place yet: XML-RPC Interface Disabled, Directory Listing Prevented. These are server and WordPress configuration checks — a separate thing from the browser security headers below. XML-RPC is flagged as a precaution, not a confirmed problem — some integrations (e.g. Jetpack or a mobile publishing app) legitimately depend on it, so it's worth confirming nothing in use needs it before disabling. Directory Listing Prevented has no such trade-off.	Confirm nothing in use depends on XML-RPC before disabling it, and correct the directory listing exposure.
1 protective browser security header missing: Content-Security-Policy (restricts where scripts can load from)	LOW	These are extra locks on the front door — simple server-side settings that stop certain common attacks. This is a separate check from the security hardening checks above, examining live HTTP response headers rather than server/WordPress configuration.	Add the missing header: Content-Security-Policy (restricts where scripts can load from).

Requires Investigation

Confirmed problems where the cause isn't yet clear — diagnosis is needed before a fix can be scoped and quoted.

ISSUE	PRIORITY	WHAT IT MEANS FOR YOUR BUSINESS	RECOMMENDED ACTION
2 PHP errors logged, invisible to visitors (352 occurrences)	MEDIUM	These are a deprecation notice and an undefined array key warning — there's no evidence either is currently affecting site functionality. Left unreviewed, recurring notices like these can occasionally point to a deeper bug, so they're worth checking rather than ignoring indefinitely.	Review the server error log to identify the source of each error and confirm whether any user-facing functionality is at risk. Scope and cost depend on what's found.
3 scheduled WordPress tasks overdue	MEDIUM	Scheduled tasks like publishing posts, sending emails, running backups or clearing caches can silently stop running without breaking the site visibly — visitors won't notice, but things quietly stop happening.	Investigate why scheduled WordPress tasks aren't running on time (common causes include low traffic triggering WP-Cron, a plugin conflict, or server-level cron misconfiguration) and restore reliable execution. Findings determine whether this is quick to fix or needs further work.

Improvement Opportunities

Optional optimisations — not part of the remediation quotation, priced separately on request.

ISSUE	PRIORITY	WHAT IT MEANS FOR YOUR BUSINESS	RECOMMENDED ACTION
Homepage speed on mobile is below the 'good' threshold (mobile speed score 72/100, based on real-user CrUX field data — not a Lighthouse lab test; mobile LCP rated needs improvement)	LOW	Real visitors on mobile are measured as waiting longer than recommended for the homepage to load or its main content to appear, which can cost visitors and may affect search ranking. The exact cause depends on what's actually slowing it down, so we recommend investigating rather than assuming a specific fix.	Investigate what's slowing the homepage down on mobile before assuming a fix.
The site is loading a large amount of settings data on every page	LOW	This adds overhead to every page load, admin screens included — the actual performance impact depends on server-side caching and configuration, but it's unnecessary weight worth trimming.	Clean up the largest autoloaded options to reduce page load overhead.

✓ KEEP YOUR WEBSITE HEALTHY AFTER THIS CHECK

Your website health check provides a snapshot of its condition at the time of assessment. However, website performance, security, software and availability can change over time.

DevEdge Website Support provides ongoing monitoring, maintenance and preventative care to help identify problems early and keep your website running reliably.

WHAT'S INCLUDED (DEPENDING ON YOUR SUPPORT PLAN)

- ✓ Website uptime and availability monitoring
- ✓ Security and vulnerability monitoring
- ✓ Regular website health assessments
- ✓ WordPress, plugin and theme updates
- ✓ Scheduled backups and backup verification
- ✓ Technical support and maintenance

This covers ongoing maintenance going forward — it doesn't retroactively include fixing problems this report already found; see "What happens next" below for those.

See the Website Support plans below to explore your options.

→ WHAT HAPPENS NEXT

OPTION 1 — REMEDIATION

Tailored Remediation Quotation

Where findings need fixing, DevEdge reviews the specific issues above — including the one marked **High** — and provides a tailored quotation before any work is booked in. Routine items (like pending updates) are usually quick and low-cost; anything requiring investigation or compatibility testing is scoped and quoted separately once we know what's involved.

Items marked **Requires Investigation** (the PHP errors and scheduled task failures) are diagnosed first, with cost confirmed once scoped. **Improvement Opportunities** (mobile speed, database cleanup) are optional and quoted separately on request. No remediation work begins without your approval.

OPTION 2 — WEBSITE SUPPORT (ONGOING)

Your £99 check fee comes off any plan below if you join within 30 days — £33 off each of your first 3 months if you pay monthly, or the full £99 off upfront if you pay annually.

☆ RECOMMENDED

Essential Website Support

£49/month

3-month minimum, then monthly, 30 days' notice to cancel

- ✓ WordPress, plugin and theme updates
- ✓ Security and vulnerability monitoring
- ✓ Scheduled backups and backup verification
- ✓ Monthly health summary email

Standard Website Support

£139/month

3-month minimum, then monthly, 30 days' notice to cancel

- ✓ Everything in Essential
- ✓ Website uptime and availability monitoring
- ✓ Regular website health assessments
- ✓ Priority email response (next business day)

Pro Website Support

£249/month

3-month minimum, then monthly, 30 days' notice to cancel

- ✓ Everything in Standard
- ✓ Priority technical support and maintenance
- ✓ Same-day emergency response
- ✓ Quarterly website strategy call

Routine maintenance — ongoing updates and standard security monitoring — is covered across all three plans above. Significant pre-existing problems found in a health check may need separate remediation work; joining Website Support doesn't include unlimited free repairs to issues that already exist.

Joining adds the plan to your account — we'll be in touch to get everything scheduled.

✉ [Reply to talk it through](#)

ASSESSMENT COVERAGE & METHODOLOGY

This assessment ran 18 checks in total: 8 passed, 7 needed attention, 2 were flagged for investigation, 0 could not be fully verified, 0 did not apply to this site, 0 weren't run this time, and 1 was reported for information only. Informational: Administrator access.

Every check in this report is automated, run against the DevEdge Connect plugin installed on the site, publicly available domain/DNS/email records, and (for homepage performance) Google PageSpeed Insights. No check in this report involved a manual security review, penetration test or SEO audit. Where a check was inconclusive or didn't apply to this site, that's noted in its own section above rather than being counted as either a pass or a failure.

CHECK	RESULT
WordPress core version	Passed
PHP version	Passed
Plugin/theme updates	Attention Required
Known vulnerabilities	Attention Required
Abandoned plugins	Attention Required
Security hardening checks	Attention Required
Administrator access	Informational
SSL certificate	Passed
Browser security headers	Attention Required
Backup health	Passed
Homepage speed	Attention Required
Uptime monitoring	Passed
Error logs	Requires Investigation
Scheduled task (WP-Cron) health	Requires Investigation
Domain renewal	Passed
Email deliverability	Passed
Broken links	Passed
Database autoload size	Attention Required