Fenix WP

DELIVERY REPORT NO. 2026-001

Site cleaned and delivered

Sample Bakery (example) · bakery.example.com

PLAN	STARTED	DELIVERED	GUARANTEE UNTIL
Complete Cleanup	Sep 16, 2026	Sep 16, 2026	Oct 16, 2026

01 Summary

Site clean

The site was rebuilt from official sources, the Japanese spam and the redirect to a gambling site were removed, and every entry point found was closed. The hack started through an outdated forms plugin, which has been updated.

02 What was found

TYPE	WHERE	ACTION
Backdoor	`wp-content/uploads/2024/03/cache.php`	Removed
Backdoor	`wp-content/uploads/2024/05/image.php`	Removed
Backdoor	`wp-includes/class-wp-cache.php` (fake file)	Removed
Persistent file	`wp-content/mu-plugins/wp-cache-helper.php`	Removed
Redirect	`.htaccess`, rule for visitors coming from Google	Removed
Ghost administrator	`wp_users`, user wpadmin2	Deleted
SEO spam	1,284 Japanese posts in `wp_posts`	Deleted
Entry point	Outdated forms plugin	Updated

03 Checklist performed

01 Forensic backup — DONE

Full copy of the files and database before any change, stored off the server.

→ 850 MB copy stored off the server.

02 Inventory — DONE

WordPress and PHP versions, plugins and themes with their versions, administrator users, cron jobs and other sites on the same account.

03 WordPress core — DONE

Check against the official checksums and reinstall a clean core on the same version.

→ WordPress 6.6.2 reinstalled; 4 core files had been modified.

04 Plugins and themes — DONE

Reinstalled from official sources. Pirated (nulled), inactive and abandoned plugins are removed.

→ 14 plugins reinstalled; 2 inactive ones removed.

05 Uploads folder — DONE

Removal of any executable file and PHP execution blocked in `wp-content/uploads`.

06 Persistence points — DONE

Review of `wp-config.php`, `.htaccess`, `index.php`, `mu-plugins`, drop-ins, `.user.ini`, files outside the public folder and the server crontab.

07 Database — DONE

Cleanup of `wp_options`, posts and pages with injected scripts, SEO spam and unknown users.

08 Custom code and store — NOT APPLICABLE

Manual review of the custom theme and plugins, the checkout (card skimming), the orders and every site in the network or account.

09 Hardening — DONE

Every password rotated (WordPress, hosting, FTP and database), new security keys, sessions closed, file editor disabled, permissions, updates and 2FA.

10 Google and SEO — DONE

SEO cleanup: Search Console (owners, sitemaps and manual actions), spam pages removed from Google and a review request for the warning.

→ Review request sent through Search Console on Sep 16, 2026.

11 Validation — DONE

Test of the main pages, forms and checkout, compared with the previous state.

12 Clean backup and delivery — DONE

Backup of the cleaned site, PDF report and guidance.

04 What was changed

- Passwords of every WordPress administrator.
- Hosting panel and FTP password.
- Database password, already updated in `wp-config.php`.
- Security keys (salts), with every session closed.

05 What's left for you

These tasks don't depend on me and are part of the guarantee conditions.

- [ ] Change the passwords of email and other services linked to the site.
- [ ] Run an up-to-date antivirus on the computers that access the dashboard.
- [ ] Don't install pirated (nulled) plugins or themes.
- [ ] Keep WordPress, plugins and themes up to date.

06 Guarantee

The guarantee is valid until **Oct 16, 2026**. If the site gets hacked again in that period, I clean it again at no cost, provided that the tasks in item 05 were done, nobody changed the site outside what we agreed and the server is not compromised at the system level.

Extended support: not purchased. Until the guarantee ends, you can add 30 more days for US$ 50.

If you notice anything odd on the site during the guarantee, just message me on WhatsApp.