TechTune Performance

Security case study — ttperformance.net

Sector	Automotive performance (tuning)
Platform	WordPress (Salient)
Scope	File + Database
Attack family	n/a (clean)
Entry vector	n/a
Verdict	CLEAN Clean (vulnerabilities only)

> **No compromise at file or database level — two unpatched vulns to fix**

The problem

TechTune Performance needed a definitive answer on whether their WordPress site was compromised. The job was to scan a full database export and a complete wp-content file tree — roughly 30,000 files, 12,000 of them PHP — and separate any genuine malware from the many legitimate code patterns that look alarming to a naive scanner.

What I did

- Scanned the full file system and database and cleared every one of the 156 eval/base64 pattern hits as legitimate plugin code (security tools, code-snippet plugins by design, backup gzip, page-builder base64).
- Verified the must-use plugin, the uploads directory, and the htaccess files were all genuine, and mapped every recent file modification back to a logged, legitimate bulk plugin update — meaning no anomalous, injected file.
- Confirmed the database was clean of stored malware, with the only security-tool issues being two unpatched theme vulnerabilities, not backdoors.
- Documented the real, lower-severity findings honestly — a default ‘Admin’ account, admin logins from non-owner IPs, overlapping migration plugins — and stated the scope limits (no wp-config or long-term server logs).

The result

I gave the client a clean verdict they could trust precisely because it was evidence-backed rather than assumed — every suspicious-looking hit was run down and explained. Their real exposure

was narrowed to two unpatched Salient vulnerabilities and a handful of hygiene items, turning an open-ended “are we hacked?” worry into a short, concrete to-do list.