Tax Store Campbelltown

Security case study — taxstorecampbelltown.com.au

Sector	Accounting / tax (AU)
Platform	WordPress
Scope	Database
Attack family	Backdoor persistence via rogue admins
Entry vector	Undetermined (DB-only scope)
Verdict	CRITICAL Critical

> **Two rogue admin accounts created within 48h of export**

The problem

This accounting firm's site had two administrator accounts that didn't belong to anyone on the team — one named to look like a “security monitor” service and the other simply “bot” — both created within the 48 hours before the database export, both holding full administrator rights. The naming pattern matched documented WordPress persistence techniques designed to survive a cursory review of the Users list.

What I did

- Confirmed the two unauthorised admin accounts against the raw user and capability tables, with their exact registration timestamps and full admin capability flags.
- Checked the rest of the database thoroughly — options, post content, post metadata, comments, and scheduled tasks — and confirmed those areas were clean of injected scripts, spam, or known malicious patterns.
- Was explicit that no file-level data was in scope, so web-shells and tampered configuration files remained outstanding rather than cleared.
- Noted supporting oddities (a malformed page GUID, a third-party admin email) worth the owner's confirmation.

The result

The client got a precise, evidence-anchored finding — two backdoor-style admin accounts to remove immediately — alongside an honest boundary on what a database-only scan could and

couldn't clear. That framing let them act on the real risk now while planning the file-level follow-up needed for a full all-clear.