Corporate Headshots Melbourne

Security case study — corporateheadshotsmelbourne.com.au

Sector	Photography studio (AU)
Platform	WordPress
Scope	File + Database, plus public-surface vulnerability assessment
Attack family	oEmbed cache SEO-spam injection
Entry vector	Undetermined; unverified admin flagged
Verdict	CRITICAL Critical

> **oEmbed cache SEO-spam injection; files clean; hardening gaps mapped**

The problem

This studio's site looked normal to visitors, but its contact page had been quietly poisoned: twelve malicious oEmbed cache entries injected into the post metadata were serving hidden casino, dating, and Russian-language spam to search engines through WordPress's built-in embed rendering — hijacking the site's search reputation while staying invisible to human visitors. A separate public-surface review also found the site leaking through weak hardening.

What I did

- Located and documented the twelve poisoned oEmbed cache rows on the contact page and confirmed the injection was isolated to cache metadata, not live content.
- Cleared the file system honestly: every plugin, theme, must-use plugin, upload, and htaccess file checked out, with all the eval/base64 hits traced back to legitimate plugin code.
- Flagged an administrator account that couldn't be verified against the known team as the suspected injection vector, alongside redundant duplicate admins.
- Delivered a companion public-surface vulnerability report: directory listing left open on the uploads folder, all six recommended security headers missing (an F grade), and recent CVEs on confirmed plugins to verify and patch.

The result

The studio got both halves of the picture — a specific, low-collateral cleanup (purge the poisoned cache rows, confirm the suspect admin) and a prioritised hardening list to close the gaps that let it

happen. Because the file system was proven clean, remediation stayed surgical rather than a full rebuild, saving the client time and disruption.