Pylomoshop

Security case study — pylomoshop.com

Sector	E-commerce (Shopify)
Platform	Shopify
Scope	Theme file audit
Attack family	n/a (clean) — app-level injection surface flagged
Entry vector	n/a
Verdict	CLEAN Clean (advisory findings only)

> **No active malware — licensed theme; top risk is an app injection surface**

The problem

The owner needed certainty about whether their Shopify theme was compromised or backdoored. The 191-file theme export had to be checked not just for active malware but for the quieter risks — a pirated theme phoning home, an app with an open injection surface, or undisclosed tracking — that a quick look would miss.

What I did

- Scanned all 191 theme files and confirmed the theme was a legitimately licensed copy (verified through the vendor's intact, design-mode-only telemetry), with no skimmer, backdoor, or obfuscated payload.
- Identified the real top risk: a page-builder app that renders store metafields into every page unsanitized — a script-injection surface that sits outside the theme files and would be the likeliest silent-reinfection vector.
- Flagged, with awareness rather than alarm, undisclosed competitor-tool evasion code and legitimate-but-unlisted tracking that belonged in the privacy policy.
- Cleared the base64 and eval hits as inert CSS and confirmed the settings and provenance were clean.

The result

The client got what a clean bill of health should actually look like: a confident “no active malware” verdict backed by evidence, plus a forward-looking risk map so they knew where a future

compromise would most likely come from (the app injection surface) rather than a false sense that nothing needed watching.