Passive security audit

https://cladco.co.uk/

D 53/100 Security grade

This store scored **D (53/100)** — At risk — several serious issues need fixing. We ran 11 passive checks and found 1 critical, 5 medium, 1 low, 4 info. Every finding below includes the exact command to fix it.

Start here — fix these first

1. CRITICAL Appears exposed to SessionReaper (CVE-2025-54236) if unpatched
2. MEDIUM Content-Security-Policy is report-only (not enforced)
3. MEDIUM Cookies set without the Secure flag
4. MEDIUM GraphQL introspection enabled
5. MEDIUM Non-production subdomains exposed in Certificate Transparency logs

All findings

Critical · 1

Appears exposed to SessionReaper (CVE-2025-54236) if unpatched INFERRED

Store appears to be running Magento 2.x. If it is 2.4.8-p2 or earlier without the APSB25-88 emergency hotfix (VULN-32437), an unauthenticated improper-input-validation flaw in the Commerce REST API allows customer-session takeover and, under certain configurations, remote code execution. This is actively exploited in the wild — verify the exact patch level urgently. CVE-2025-54236 is on CISA's Known Exploited Vulnerabilities catalog — it is being exploited in the wild right now, so treat patching as urgent, not theoretical.

EVIDENCE `form_key=present · mage_init=present · page_wrapper=present · section_data=present · observed https://cladco.co.uk/`

How to fix — Apply Adobe's APSB25-88 emergency hotfix (VULN-32437) immediately, then rebuild. Actively exploited — treat as urgent, not routine.

1. Apply the APSB25-88 isolated hotfix (VULN-32437) for your release line — it closes this without a full upgrade — then rebuild.

```
bin/magento setup:upgrade && bin/magento cache:flush
```

2. If there is any sign of exploitation, assume session/admin compromise: invalidate all sessions and rotate admin credentials and integration tokens.

```
bin/magento admin:user:unlock; # then flush the session store to force re-authentication
```

3. Optional: move to a patched release on your line. Use your edition's metapackage and the exact fixed version from the advisory.

```
composer require magento/product-<your-edition>-edition:<fixed-version> --no-update && composer update
```

https://helpx.adobe.com/security/products/magento/apsb25-88.html

Medium · 5

Content-Security-Policy is report-only (not enforced)

CONFIRMED

Only a Content-Security-Policy-Report-Only header is set — violations are reported but NOT blocked, so an injected inline skimmer still executes. Magento ships CSP in report-only by default; the storefront must be switched to restrict (enforced) mode to actually stop card skimmers.

EVIDENCE Content-Security-Policy=absent · Content-Security-Policy-Report-Only=font-src www.paypalobjects.com fonts.gstatic... · observed https://cladco.co.uk/

How to fix — Switch Magento_Csp from report-only to enforced (restrict) mode for the storefront.

1. Enforce the storefront CSP (0 = restrict/enforced).

```
bin/magento config:set
system/csp/mode/storefront/report_only 0
```

2. Whitelist legitimate inline scripts/domains via csp_whitelist.xml first to avoid breaking the storefront, then flush.

```
bin/magento cache:flush config full_page
```

https://developer.adobe.com/commerce/php/development/security/content-security-policies/

Cookies set without the Secure flag

CONFIRMED

Cookies are set over HTTPS without Secure, so they can be transmitted over a downgraded/plaintext connection.

EVIDENCE affected_cookies=wp_ga4_user_id, wp_ga4_customerGroup · observed https://cladco.co.uk/

How to fix — Set Secure on the affected cookies.

1. Magento cookie flags: set web/cookie configuration and ensure the store is served exclusively over HTTPS.

```
bin/magento config:set web/cookie/cookie_httponly 1
```

2. Enforce Secure + SameSite at the edge for cookies the app does not manage.

```
proxy_cookie_flags ~ secure samesite=lax;
```

GraphQL introspection enabled

CONFIRMED

The GraphQL schema is fully introspectable in production, handing an attacker the complete type/field map — including custom modules — to plan targeted queries.

EVIDENCE query={__schema{queryType{name} types{name}}} · endpoint=/graphql · observed https://cladco.co.uk/graphql?query=%7B__schema%7BqueryType...

How to fix — Disable GraphQL introspection in production.

1. Set the deployment mode to production (disables introspection by default).

```
bin/magento deploy:mode:set production
```

2. If a custom middleware/plugin toggles it, ensure introspection is gated to non-production only, then flush cache.

```
bin/magento cache:flush
```

https://developer.adobe.com/commerce/webapi/graphql/

Non-production subdomains exposed in Certificate Transparency logs

INFERRED

Public CT logs list 2 non-production-looking subdomain(s) for this domain (e.g. test.apps.cladco.co.uk, test.cladco.co.uk). Staging/dev/UAT hosts frequently run a copy of production data without a password, WAF, or up-to-date patches — a common back door. Confirm each is not publicly reachable.

EVIDENCE source=crt.sh (Certificate Transparency) · total_flagged=2 · risky_subdomains=test.apps.cladco.co.uk, test.cladco.co.uk

How to fix — Lock down or take offline every non-production host.

1. Confirm which of these resolve and respond, then put them behind auth / an IP allowlist, or take them offline.
2. Never run production data on an unprotected staging host; scrub PII from non-prod databases.
3. Front non-prod with the same WAF/CDN as production so they are not a soft target.

https://crt.sh/?q=%25.cladco.co.uk

Older critical CVEs on this branch — verify your patch level

INFERRED

The store appears to be running Magento 2.x, but the exact patch level could not be determined. This branch has had critical, now-fixed vulnerabilities — CosmicSting (CVE-2024-34102, APSB24-40); TrojanOrder (CVE-2022-24086, APSB22-12). A store kept reasonably current already has these patches; if yours is NOT on the latest patch they are critical (unauthenticated RCE / data theft), and 2 are on CISA's Known Exploited Vulnerabilities catalog (actively exploited in the wild). Confirm your exact patch level.

EVIDENCE `form_key=present · mage_init=present · older_cves=CVE-2024-34102, CVE-2022-24086 · page_wrapper=present · observed https://cladco.co.uk/`

How to fix — Confirm the store is on the latest patch for its release line.

1. Check the running version against the latest patch for your line.

```
bin/magento --version
```

2. If behind, apply the latest security patches (isolated hotfixes exist for each of these), then rebuild.

```
composer update && bin/magento setup:upgrade &&
bin/magento cache:flush
```

https://experienceleague.adobe.com/docs/commerce-operations/release/planning/lifecycle-policy.html

Low · 1

Referrer-Policy not set

CONFIRMED

No Referrer-Policy. Full URLs (including cart/checkout tokens in query strings) may leak to third parties.

EVIDENCE `Referrer-Policy=absent · observed https://cladco.co.uk/`

How to fix — Set a strict referrer policy.

1. nginx: add to the server block.

```
add_header Referrer-Policy "strict-origin-when-cross-
origin" always;
```

Info · 4

Appears to be running Magento 2.x

INFERRED

Platform inferred from passive signals. Treat the version as approximate — verify the exact patch level against the deployment.

EVIDENCE `form_key=present · mage_init=present · page_wrapper=present · section_data=present · observed https://cladco.co.uk/`

Permissions-Policy not set

CONFIRMED

No Permissions-Policy. Powerful browser features are not explicitly restricted for embedded third-party content.

EVIDENCE `Permissions-Policy=absent · observed https://cladco.co.uk/`

How to fix — Declare a least-privilege Permissions-Policy.

1. nginx: restrict sensitive features.

```
add_header Permissions-Policy "geolocation=(),
camera=(), microphone=()" always;
```

Static assets indicate version 2.4.3 or older

INFERRED

The tiny_mce_4 static path was retired after 2.4.3; its presence indicates an older, likely end-of-support branch. This narrows the version inferred from page markers alone — verify the exact patch level.

EVIDENCE source=gwillem/magento-version-identification; Adob... · implies=2.4.3 or older · discriminator=TinyMCE 4 admin bundle · observed https://cladco.co.uk/static/adminhtml/Magento/backend/en_U...

Static assets indicate version 2.4.4 or newer

INFERRED

Magento bundled TinyMCE 4 through 2.4.3 and upgraded to TinyMCE 5 in 2.4.4; the tiny_mce_5 static path exists only on 2.4.4 and later. This narrows the version inferred from page markers alone — verify the exact patch level.

EVIDENCE source=gwillem/magento-version-identification; Adob... · implies=2.4.4 or newer · discriminator=TinyMCE 5 admin bundle · observed https://cladco.co.uk/static/adminhtml/Magento/backend/en_U...