CookieInspector

HOW TO FIX · REMEDIATION GUIDE · EXPERIMENTAL

Consent setup remediation for cookieinspector-demo-shop.vercel.app

The site displays a consent banner but it does not offer a reject-all option and tracking from several third parties runs before consent, so update the banner and stop third-party scripts until consent is given.

SITE	https://cookieinspector-demo-shop.vercel.app/
SCAN	8A3071F7-F2C2-4F3C-A551-C2D56018C3AB · 2026-10-31 · scanned from main
CONSENT PLATFORM	none detected
CURRENT SCORE	**71 / 100** risk (lower is better) · NonCompliant
EXPECTED AFTER FIXES	**35–39**

SUMMARY

Fix pre-consent tracking

A consent banner is present but appears to be a custom or unrecognised implementation and is not blocking trackers; third-party tracking requests to hosts such as google-analytics.com, connect.facebook.net, www.facebook.com, ad.doubleclick.net and googleads.g.doubleclick.net are executed before the user can refuse, and cookies from doubleclick.net and facebook.com are set prior to consent. Remediate by restoring a clear reject/deny control on the banner or switching to a supported CMP, and ensure all third-party tracking scripts are prevented from loading until explicit consent is recorded.

What is working

CONFIRMED

- A consent banner is visible to visitors.
- Tracking activity is limited to a known set of third-party hosts that can be targeted for blocking.

What produces the score

ROOT CAUSE

- The consent banner is a custom or unrecognised CMP and lacks a reject-all control and blocking integration.
- Tracking scripts are injected directly into the page (theme or custom code) rather than being controlled by a CMP or tag manager, so they execute before consent.
- No mechanism is present to delay or conditionally load scripts that set cookies at hosts such as doubleclick.net and facebook.com.

What happens before the visitor decides

TIME	EVENT	CONSENT STATE
0.16 s	connect.facebook.net contacted (Tracking).	before consent
0.21 s	www.googletagmanager.com contacted (Tag manager).	allowed before consent
0.28 s	www.google-analytics.com contacted (Tracking).	before consent
0.30 s	connect.facebook.net contacted (Tracking).	before consent
0.31 s	www.facebook.com contacted (Tracking).	before consent
0.48 s	ad.doubleclick.net contacted (Tracking).	before consent
11.59 s	Visitor clicks accept.	granted

Rows marked *allowed before consent* are not violations. The tag manager container, the consent platform and denied Consent Mode pings have to reach the browser before the visitor answers, because they are what applies the answer afterwards.

EVIDENCE

What loaded before anyone answered

Third-party hosts contacted before the consent decision, in the order they were first reached. Bold rows are the ones counted as tracking.

HOST	FIRST SEEN	CLASS	REQUESTS
connect.facebook.net	0.16 s	Tracking	1
www.googletagmanager.com	0.21 s	Tag manager	2
www.google-analytics.com	0.28 s	Tracking	2
connect.facebook.net	0.30 s	Tracking	1
www.facebook.com	0.31 s	Tracking	1
ad.doubleclick.net	0.48 s	Tracking	2
www.google.com	0.48 s	Tracking	2
www.google.com	0.48 s	Tracking	3
googleads.g.doubleclick.net	0.49 s	Tracking	1

Cookies written before consent

COOKIE	SET BY
test_cookie	doubleclick.net
fr	facebook.com

DIAGNOSIS

Load the homepage in a fresh browser session and confirm the banner appears but there is no reject/deny option.

Open the network panel and reload; observe requests to google-analytics.com, connect.facebook.net, www.facebook.com, ad.doubleclick.net and googleads.g.doubleclick.net occurring before interacting with the banner.

Search the theme templates and site header for hardcoded script tags that reference those hosts and for any CMP code; if none of the scripts are loaded from your tag manager container then they are injected by theme or plugin code.

What the score is made of

- Consent banner detected (Unknown CMP).
- Consent banner does not expose a reject-all option.
- Consent banner is not blocking access before consent.
- 2 third-party cookies observed before consent.
- 3 tracking scripts detected.
- 2 high severity issues detected.
- 2 medium severity issues detected.
- Marketing trackers detected.
- Third-party activity occurred before consent despite the consent banner.

FIX 1

Add a Reject-All control to the banner

Visitors must be able to deny marketing and tracking cookies up front; the current banner lacks that control so consent cannot be declined.

Steps

- If you use a commercial CMP, open its console and enable the global 'reject all' or 'deny all' option and save/publish the policy so the banner shows both Accept and Reject buttons.
- If no CMP is used and the banner is rendered by your theme or custom code, edit the theme template or banner script to add a visible 'Reject all' button that records a denial in the same storage the banner uses (cookie/localStorage) and triggers the site's consent state handler.
- Ensure the reject action sets an explicit consent state (deny for marketing/statistics categories) and persists it so subsequent page loads honour the refusal.

FIX 2

Prevent third-party scripts running before consent

Tracking requests to google-analytics.com, connect.facebook.net, www.facebook.com, ad.doubleclick.net and googleads.g.doubleclick.net are executed before consent, so those scripts must be blocked until consent is granted.

Steps

- Search the site code and theme header for any hardcoded script tags or inline code that load or initialize Google Analytics, Facebook SDK, DoubleClick or Google Ads and remove those direct script tags from the page.
- If you manage tags through a tag manager, migrate each removed script into the tag manager and configure each tag with a trigger that requires explicit marketing or analytics consent before firing.
- If you do not use a tag manager, wrap each third-party script injection in a runtime check that reads the banner consent state and only appends the external script element after the user has given the matching category consent.
- For the Facebook hosts (connect.facebook.net, www.facebook.com) and doubleclick/googleads hosts, ensure the initialization code is deferred and not executed on page load; only inject their SDKs after the user accepts the relevant category.

FIX 3

Remove or delay cookies set before consent

Cookies from doubleclick.net and facebook.com are present before consent, which indicates scripts are creating persistent identifiers; these must be prevented or cleared until consent.

Steps

- After preventing the scripts from loading (previous fix), add a short startup script in the theme that checks for any existing cookies from doubleclick.net or facebook.com and removes client-accessible cookies set by those domains where possible.
- Confirm that cookie removal only runs when the banner denies consent or on first load before consent is provided, and that cookies are not recreated until explicit consent is given and the approved scripts run.
- Test in a private browser to verify that after these changes no requests to those hosts occur and no related cookies are set prior to accepting the banner.

FIX 4

Switch to a supported CMP or integrate blocking API

An unrecognised or custom banner is not effectively stopping tracking; a supported CMP provides a blocking API and consent management integrations which simplify compliance.

Steps

- Evaluate deploying a recognised CMP (or enable your existing CMP integration) that offers automatic blocking for common vendors and provides a documented API to query consent state.
- Configure the CMP to block marketing and analytics categories by default and to expose a callback or JS API that your tag manager or theme can use to conditionally load tags and scripts only after consent.
- Replace the current banner script with the CMP's published snippet or enable the CMP plugin for your platform and test end-to-end: banner shows Accept/Reject, CMP records state, and third-party requests occur only after acceptance.

VERIFICATION

Check it before you publish

- Load the site in a fresh private window and confirm the banner presents both accept and reject options before interacting further.
- With network logging enabled, reload and confirm there are no requests to google-analytics.com, connect.facebook.net, www.facebook.com, ad.doubleclick.net or googleads.g.doubleclick.net before accepting consent.
- Accept consent and confirm the expected tracking requests appear; then reload a fresh session and choose Reject to confirm tracking requests do not occur and cookies from doubleclick.net and facebook.com are not set.

Pages included in this scan

- https://cookieinspector-demo-shop.vercel.app/

Reference

Cookie policy	not found
Privacy policy	not found
Findings raised	BANNER_NON_BLOCKING, CMP_PRESENT, CMP_PRESENT_NOT_EFFECTIVE, CMP_REJECT_MISCONFIG, COOKIES_BEFORE_CONSENT, THIRD_PARTY_API_CALLS, THIRD_PARTY_PRE_CONSENT
Scanner build	eabedd098003