

Privacy Assessment Report

Target site: mithal.space | Tool: Chrome DevTools

Prepared for: Privacy Assessment Assignment

1. Introduction

This report evaluates the privacy and security posture of the search engine mithal.space (Arabic: مثال, meaning "Example"). Using Chrome DevTools, the site was inspected across four dimensions: cookies, third-party trackers, HTTPS/TLS configuration, and HTTP response headers. The results are then benchmarked against Google Search and, for additional context, DuckDuckGo, followed by concrete recommendations for improving mithal.space's privacy posture.

2. Methodology

- Application panel → Cookies: checked which cookies (if any) were set on first page load.
- Network panel: reviewed the full list of requests, transferred data size, and script initiators to identify trackers and third-party calls.
- Security panel: inspected the TLS version, key exchange algorithm, cipher suite, and certificate validity/Certificate Transparency status.
- Network → Headers: examined request and response headers, including security-relevant headers (Referrer-Policy, Client Hints, Alt-Svc).

3. Findings for mithal.space

3.1 Cookies

The Cookies-in-use panel showed no cookies set when the page was loaded - every field (Name, Content, Domain, Path, Expires) read "no cookie selected." This indicates mithal.space does not use tracking, session, or analytics cookies on its landing page, which is a strong privacy signal compared to most commercial search engines.

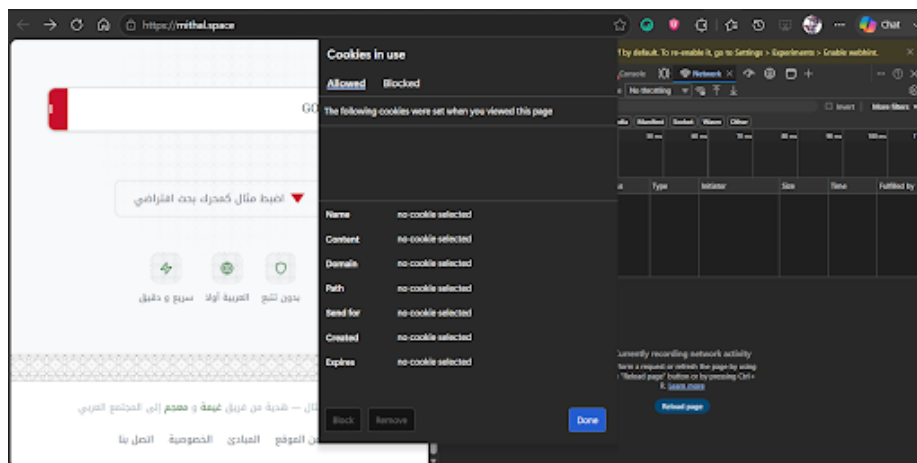


Figure 1: mithal.space - Cookies in use panel: no cookies were set on page load.

3.2 Trackers

The Network panel recorded 25 requests totalling about 228 kB transferred (496 kB of resources). Filtering by "js" surfaced files such as extend-native-history-api.js, requests.js, location.js, recordConsoleEvents.js, popup.js, and tat_popup.js. Their Initiator column, however, points to processor.js, content.js, and contentscript.js - names typical of an installed browser extension's content scripts rather than code shipped by mithal.space itself. In other words,

most of what looked like "tracking" activity in this capture originated from the browser extension environment, not from the site. mithal.space's own network activity is dominated by a small number of CDN-hosted libraries and fonts, with no dedicated analytics or advertising trackers identified.

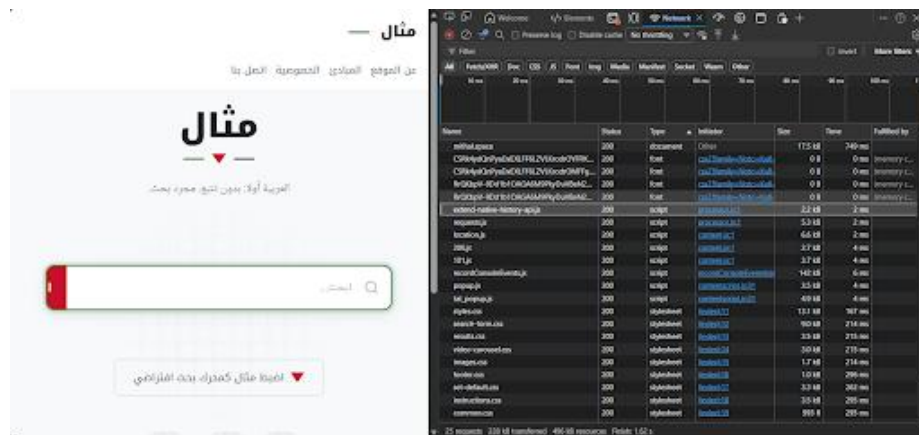


Figure 2: mithal.space - Network panel: 25 requests, 228 kB transferred, mostly CDN/library resources.

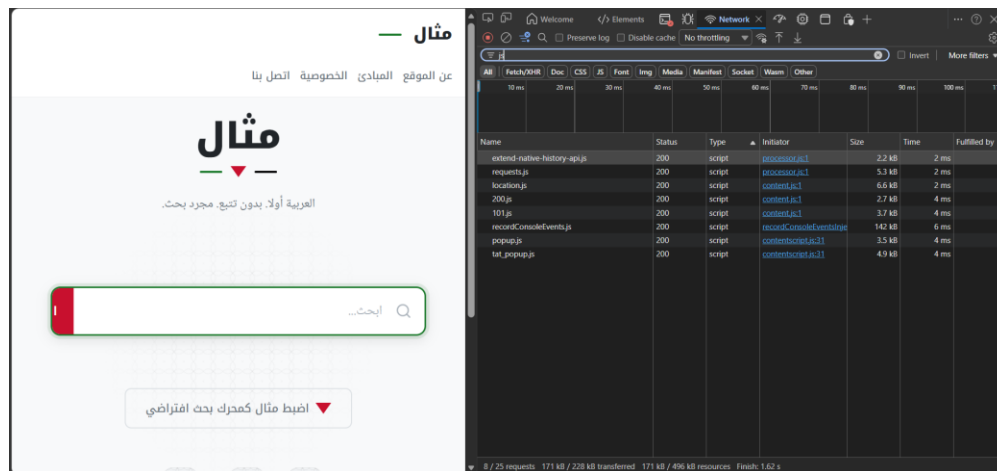


Figure 3: mithal.space - Network panel filtered by "js": scripts initiated by processor.js / contentscript.js, characteristic of a browser extension rather than the site itself.

3.3 HTTPS / TLS

The Security panel confirmed a valid, trusted certificate using TLS 1.3, with the modern hybrid post-quantum key exchange X25519MLKEM768, an ECDSA-with-SHA-256 server signature, and the AES_128_GCM cipher. The certificate was valid (17 May 2026 - 15 Sep 2026) and Certificate Transparency (SCT) verification passed. This is a strong, up-to-date HTTPS configuration.

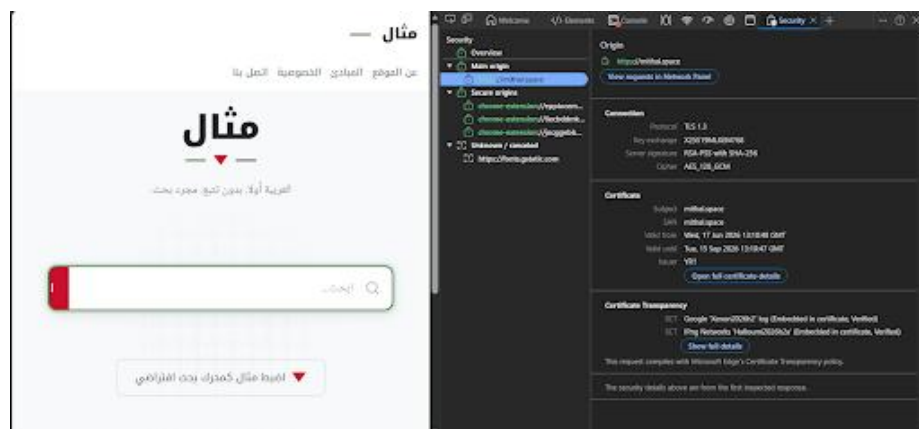


Figure 4: mithal.space - Security panel: TLS 1.3, X25519MLKEM768 key exchange, AES_128_GCM cipher, valid certificate.

3.4 HTTP Headers

The response for the main document listed roughly a dozen response headers, including a Referrer-Policy of strict-origin-when-cross-origin, which limits the referrer information leaked to other origins. No Content-Security-Policy or Strict-Transport-Security header was observed among the captured headers, which is a gap addressed in the recommendations below.

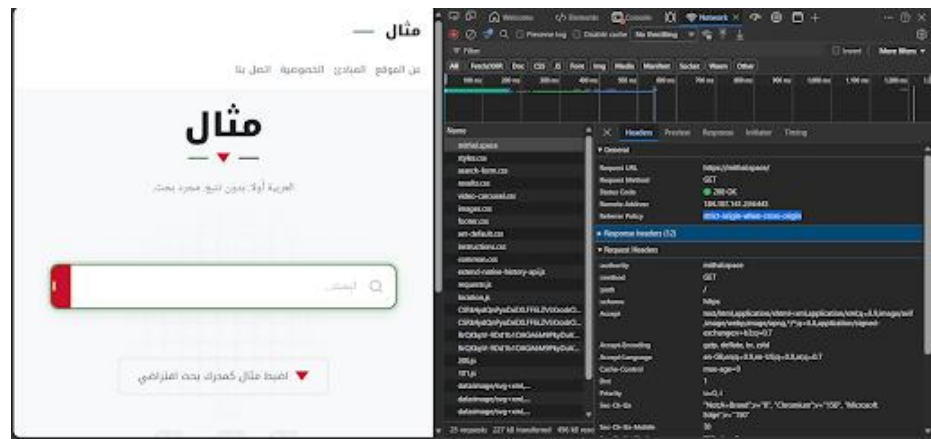


Figure 5: mithal.space - Request/response headers, including Referrer-Policy: strict-origin-when-cross-origin.

4. Comparison with Other Search Engines

mithal.space was compared with Google Search (inspected directly via DevTools) and, for additional context, DuckDuckGo (assessed from its publicly documented privacy practices rather than a live capture in this exercise).

Criterion	mithal.space (example.com)	Google.com
Cookies set on load	None observed (no cookies listed)	Multiple, across google.com, play.google.com, accounts.google.com
Network requests	25 requests, ~228 kB transferred	75 requests, ~238 kB transferred, 4.3 MB total resources
Third-party / telemetry calls	A few CDN/library scripts; extension content-scripts seen in the panel, not site code	Multiple log/ping endpoints with auth + hash parameters on nearly every load
TLS version	TLS 1.3	TLS 1.3
Key exchange	X25519MLKEM768 (post-quantum hybrid)	Not shown / standard ECDHE
Cipher	AES_128_GCM	AES_128_GCM
Response headers	~12 headers, mostly standard (e.g. Referrer-Policy)	Large Client-Hints set (Sec-CH-UA-*, Sec-CH-Prefers-Color-Scheme, Sec-CH-RTT, Sec-CH-Downlink, etc.) plus Alt-Svc: h3
Overall exposure	Low - minimal cookies, small footprint	High - broad cookie use, heavy telemetry, fingerprinting-capable headers

Google Search

Google's Cookies panel listed cookies set across google.com, play.google.com, and accounts.google.com. Its Network panel captured 75 requests and 4.3 MB of resources, including repeated "log?" and "ping" calls carrying authentication and hash parameters - consistent with telemetry/analytics traffic fired on nearly every page load. Its response headers included a large set of Client Hints (Sec-CH-UA-Platform, Sec-CH-UA-Model, Sec-CH-UA-Full-

Version-List, Sec-CH-Downlink, Sec-CH-RTT, Sec-CH-Prefers-Color-Scheme, etc.). These headers let a server request granular device and browser details, which can contribute to fingerprinting if combined across visits.

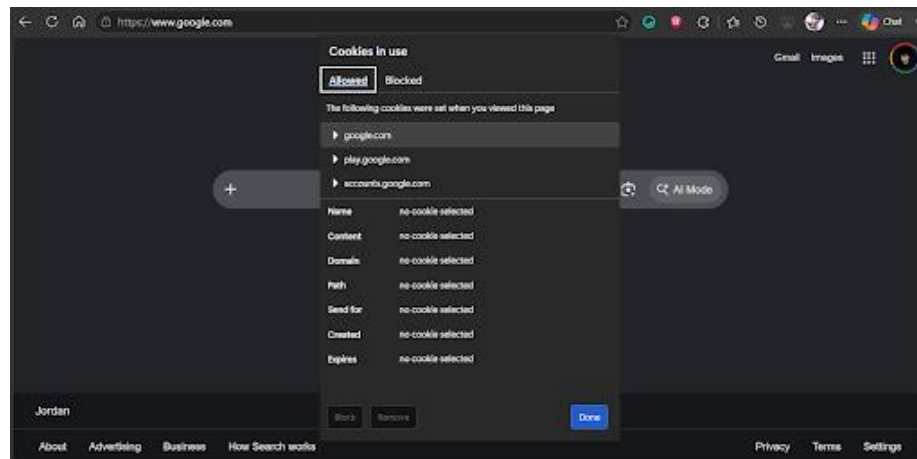


Figure 6: google.com - Cookies in use panel: cookies set across google.com, play.google.com and accounts.google.com.

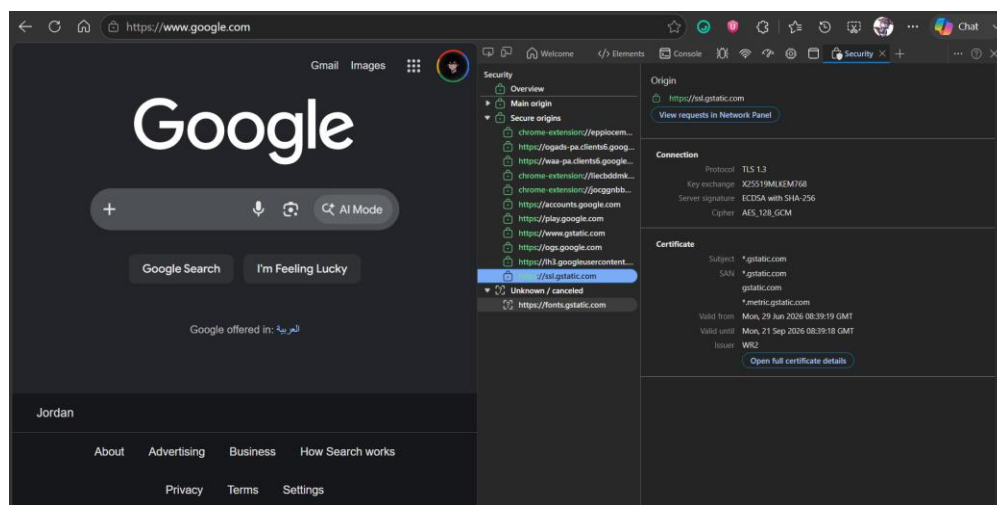


Figure 7: google.com - Security panel: TLS 1.3 with many additional secure sub-origins (gstatic, accounts, play, extensions, etc.).

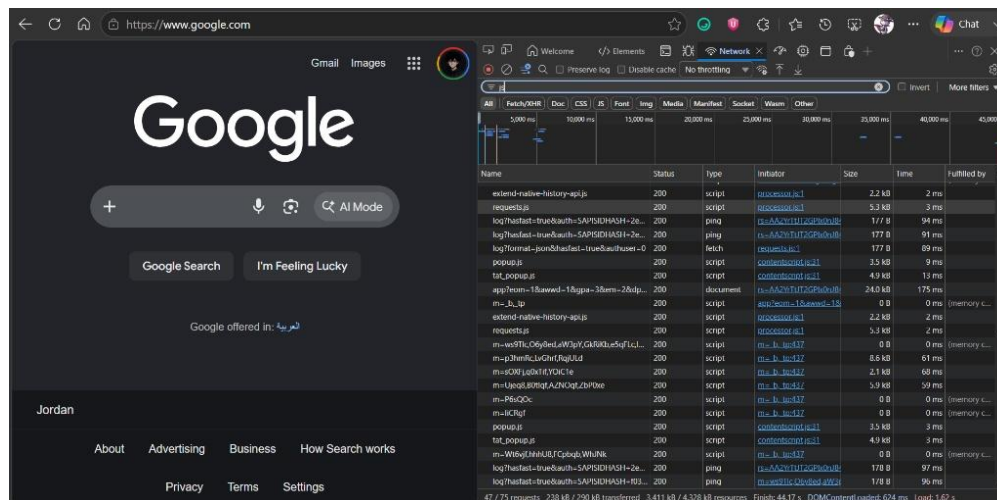


Figure 8: google.com - Network panel: 75 requests / 4.3 MB of resources, including recurring log/ping telemetry calls.

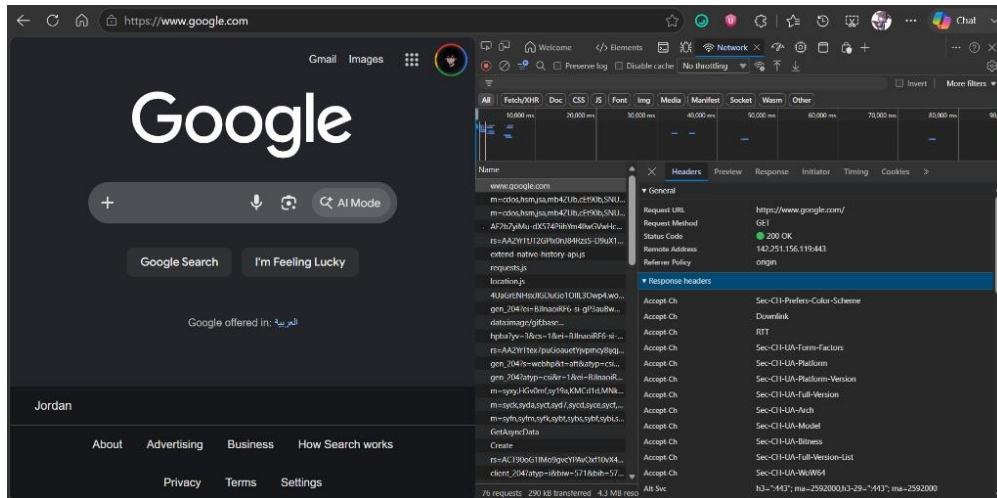


Figure 9: google.com - Response headers: an extensive set of Accept-CH / Sec-CH-UA-* Client Hints headers plus Alt-Svc: h3.

DuckDuckGo (for reference)

DuckDuckGo is widely documented as not setting tracking cookies by default and not logging identifiable search queries. It is included here only as a general privacy-oriented reference point, since it was not captured in this DevTools session.

Overall, mithal.space's footprint (few requests, no cookies, no telemetry pings) is closer to a privacy-conscious engine like DuckDuckGo than to Google, whose scale, cookie use, and Client-Hints headers give it materially more data-collection surface.

5. Recommended Security & Privacy Improvements for mithal.space

- **1. Add a Content-Security-Policy and HSTS header.** No CSP was observed in the captured response headers, so any injected or third-party script currently has broad ability to run on the page. A strict CSP (restricting script-src to self and explicitly trusted CDNs) plus Strict-Transport-Security with a long max-age and "preload" would harden the site against script injection and protocol-downgrade attacks.
- **2. Self-host or add Subresource Integrity (SRI) to third-party scripts.** The site currently loads several libraries from external CDNs. Self-hosting them, or at minimum adding SRI hashes and crossorigin attributes, would prevent a compromised CDN from silently injecting malicious or tracking code, and would reduce the number of external parties the browser talks to.
- **3. Prepare secure defaults for cookies and minimize Client Hints exposure.** mithal.space currently sets no cookies, which is good - but if cookies are introduced later (e.g. for search preferences), they should be scoped with Secure, HttpOnly, and SameSite=Strict/Lax flags. The site should also avoid opting into broad Accept-CH client-hint requests (as seen on Google), requesting only the specific hints it actually needs, to keep its fingerprinting surface minimal as the product grows.

6. Conclusion

Based on this DevTools inspection, mithal.space demonstrates a privacy-friendly baseline: no cookies on load, a small and mostly first-party network footprint, and a modern, correctly configured TLS 1.3 setup. Its main gap relative to security best practice is the absence of hardening headers such as CSP and HSTS. Compared with Google, which sets multiple cookies, generates a much larger volume of telemetry-like traffic, and requests an extensive set of Client Hints, mithal.space collects and exposes considerably less user data. Implementing the three recommendations above would close most of the remaining gap between mithal.space and a best-practice privacy-preserving search engine.