

BrainIdeasFused — Security Audit

A small surface, by design. Summary of the app's security posture.

01

No authentication vulnerabilities

BrainIdeasFused is a public tool with no auth layer — no logins, passwords, tokens, or sessions to compromise. There is no privileged surface to escalate into and no credential store to breach, which removes an entire class of common attack vectors by design.

02

No data persistence risks

Fusion inputs and outputs are processed in-request and not persisted against any user. There is no user database to leak, no history to exfiltrate, and no long-lived PII at rest beyond an explicitly opted-in waitlist email.

03

No third-party data sharing

Snippets are sent only to the model provider strictly to generate the requested brief. Nothing is shared with analytics vendors, ad networks, or data brokers — there is no tracking pipeline wired into the app.

04

Claude API usage scoped to session

Every fusion opens a fresh, uniquely-identified Claude session with no cross-request memory. The Emergent Universal Key stays server-side in environment variables and is never exposed to the browser, so model access can't be replayed or abused from the client.