AI-Assisted Security Audit

Executive summary — June 2026

Version 1.11.0

June 2026

This document is provided for informational purposes only. It is not investment, legal, or tax advice. Trading digital assets involves substantial risk of loss. Past performance is not indicative of future results.

Scope

This summary describes the March 2026 security review of the Smooth Brains web application, API, and live execution path. It is written for institutional allocators and technical due diligence teams. Detailed findings live in the full report available on request; this page states posture and remediations at a high level.

Architecture in plain terms

Component	Role
Web application	User onboarding, performance pages, wallet connection, settings
Application API	Authenticated requests for account state, execution preferences, and operational data
Database	User profiles, execution state, audit logs - hosted on managed Postgres with row-level access controls
Job queue	Background tasks for notifications, reconciliation, and scheduled checks
Execution path	Signs orders on Hyperliquid under user-granted trade-only delegation

Smooth Brains does not store user private keys or withdrawal credentials.

Review methodology

An independent security reviewer (automated and manual pass) examined:

– Authentication and session handling

– Authorisation on account-scoped API routes (preventing cross-user data access)

– Database policies ensuring users read only their own rows

– Input validation on execution and settings endpoints

– Secret handling in deployment configuration

Summary of findings (March 2026)

Severity	Count	Status
Critical	0	-
High	0 open	Remediated or accepted with compensating control

Severity	Count	Status
Medium	Several	Remediated or scheduled
Low / informational	Several	Documented

No critical or open high-severity issues remained at publication. Medium items addressed included tightening account-scoped access on sensitive routes, hardening webhook validation, and clarifying error responses that could leak internal identifiers.

Live execution controls

– Fail closed on stop placement or confirmation failure

– Kill switch and drawdown circuit breaker available to operators

– Non-custodial model - compromise of platform servers does not directly drain user wallets without separate wallet compromise

Ongoing practices

– Dependency and vulnerability monitoring on deploy

– Separate production secrets from repository code

– Role-limited access to production database and hosting dashboard

What this audit does not cover

– Smart contract audit of Hyperliquid itself (third-party venue)

– User device or browser security

– Social engineering against individual users

Disclaimer

A point-in-time audit summary. Not a guarantee against future vulnerabilities. Not financial advice.