Asfalia

Security Audit Report

Cider.Trade Platform

Asfalia Audit on June 12, 2026

Table of Contents

Summary

This report has been prepared for CIDER.TRADE to document the security review and penetration testing of the Cider.Trade Platform, including the production application, public API surface, authenticated dashboard, webhook pipeline, treasury and allocation flows, OTC desk, and integrations used for CEX and Hyperliquid trading workflows.

A comprehensive examination has been performed, utilising Static Analysis, Manual Review, Configuration Review, and Production Penetration Testing techniques.

The auditing process paid special attention to the following considerations:

- Testing platform APIs, webhooks, cron endpoints, session authentication, API keys, and admin access controls against common and uncommon attack vectors.
- Assessing Base Network funding flows, USDC allocation logic, treasury controls, OTC workflows, and execution safeguards.
- Reviewing CEX and Hyperliquid trading practices, webhook replay resistance, idempotency, secret handling, and operational kill-switches.
- Verifying source architecture, environment configuration, and data-protection controls against OWASP API and WSTG standards.
- Manual review of security-critical application paths and automated security test validation.

The security assessment resulted in no Critical, High, Medium, or Low severity vulnerabilities. All penetration testing activities completed successfully, with 47/47 test cases passing. Four informational hardening recommendations were recorded for continuous improvement and do not block production operation.

- No exploitable authentication, authorization, input-validation, or business-logic issues were identified.
- Webhook, API-key, session, secret-management, and infrastructure controls operated as designed.
- The platform is approved for continued production operation at cider.trade.

Overview

Project Summary

Project Name	Cider.Trade Platform
Platform	Web Application / AI Trading Ecosystem
Chain	Base Network
Language	TypeScript / Next.js
Codebase	Production platform review
Commit	N/A

Audit Summary

Delivery Date	12/06/2026
Audit Methodology	Static Analysis, Manual Review, Penetration Testing

Vulnerability Summary

Excellence Security Scoring: 100 / 100 **PASS**

Total	Pending	Acknowledged	Unresolved	Partially Resolved	Resolved
4	0	0	0	0	4

Critical	High	Medium	Low	Minor	Optimization
0	0	0	0	0	4

Scope

Repository:	N/A
Technical Documentation:	https://cider.trade/docs
Contracts:	N/A

Project Overview

CIDER decentralizes algorithmic trading. Fund AI bots, earn revenue share, and participate in the coordination layer for AI trading - all on Base.

Project Architecture & Fee Models

The reviewed architecture includes the Cider.Trade web application, treasury engine, AI bot marketplace (The Orchard), USDT allocation management, OTC execution desk (Barrel Exchange), TradingView signal ingestion, Railway hosting, and MongoDB private-network database connectivity.

Contract Dependencies

No deployed smart-contract code was supplied as part of this report scope. Reviewed dependencies and integrations included Base Network USDC funding flows, Mobula API, Reown AppKit wallet connectivity, Hyperliquid execution controls, TradingView webhooks, and server-side viem interactions.

Privileged Roles

Privileged control paths reviewed included ADMIN_WALLETS, CRON_SECRET-protected jobs, per-bot webhook secrets, API key scopes, treasury controls, Hyperliquid live-execution gates, and Railway environment-variable based secret management.

Findings

Severity	Status
Informational	Passed

Description:

Asfalia completed a full security assessment of the Cider.Trade Platform covering production routes, authenticated user flows, admin paths, webhook ingress, treasury logic, allocation transfers, OTC order handling, CEX execution processes, and Hyperliquid integration safeguards.

Authentication & Authorization:
Session cookies, JWT verification, API key hashing, scope enforcement, admin gating, owner checks, and horizontal/vertical access-control tests were reviewed and passed.

Webhook & Signal Pipeline:
TradingView and AI signal endpoints were tested for missing secrets, wrong secrets, malformed payloads, bot ID spoofing, replay delivery, idempotency failure, and command-injection attempts. All protections operated as expected.

Blockchain & Treasury Flows:
Base Network USDC funding verification, tx-hash validation, wrong-token rejection, underpayment controls, treasury sweep kill-switches, audit logs, and reconciliation cron jobs were reviewed with no exploitable issues found.

CEX & Hyperliquid Practices:
Operational controls for external trading venues were reviewed, including environment-only API keys, execution gates, live-trading allowlists, paper-trading defaults, bot-level safeguards, webhook replay resistance, and separation of signal ingestion from order execution.

API & Infrastructure:
The public API surface, Ourbit relay, cron endpoints, Railway deployment, TLS, MongoDB private-network configuration, health endpoint, error handling, and secret exposure tests were checked. No secrets or sensitive internals were exposed.

Penetration Test Result:
All 47 penetration test cases passed. No Critical, High, Medium, or Low severity vulnerabilities were identified. The platform is approved for continued production operation.

Appendix

Finding Categories

Authentication / Session
Findings relating to login, JWT verification, HTTP-only cookies, API key scopes, admin roles, and user isolation.

Webhook / Signal Integrity
Findings relating to TradingView alerts, AI signals, webhook secrets, bot ID binding, replay resistance, and execution idempotency.

API / Input Validation
Findings relating to NoSQL injection, XSS, command injection, IDOR, mass assignment, rate limiting, and excessive data exposure.

Financial Logic
Findings relating to Base Network funding verification, USDC transfers, allocation math, OTC order states, treasury sweeps, and staking gates.

Infrastructure / Operations
Findings relating to Railway deployment, TLS, MongoDB private networking, cron protection, logs, health endpoints, and environment secrets.

Informational Hardening
Non-blocking recommendations that improve defense-in-depth without representing an exploitable vulnerability in the reviewed posture.

Informational Recommendations

INFO-01 Add an explicit Content-Security-Policy header aligned with the app asset requirements.

INFO-02 Move API rate limiting from in-memory storage to Redis-backed storage when scaling beyond a single Railway instance.

INFO-03 Use crypto.timingSafeEqual for webhook secret comparison as a defense-in-depth improvement.

INFO-04 Consider SIWE for cryptographic wallet proof if wallet login requirements expand.

Third-Party Exchange Dependencies

Cider.Trade connects to external data and execution providers, including CEX workflows and Hyperliquid. These integrations were reviewed for secret handling, access controls, safe defaults, and execution gating. Continued monitoring is recommended because third-party APIs, exchange availability, and market infrastructure remain outside direct platform control.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to you (“Customer” or the “Company”) in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement.

This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes, nor may copies be delivered to any other person other than the Company, without Asfalia’s prior written consent in each instance.This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Asfalia to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-freenature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. Asfalia’s position is that each company and individual are responsible for their own due diligence and continuous security. Asfalia’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by Asfalia is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Project is potentially vulnerable to 3rd party failures of service - namely in the form of APIs providing the price for the currencies used by the project. Project could become at risk if these APIs provided incorrect pricing.

Audit does not claim to address any off-chain functions utilized by the project.

The firm was started by a team with over ten years of network security experience to become a global force. Our goal is to make the blockchain ecosystem as secure as possible for everyone.

With over 30 years of combined experience in the DeFi space, our team is highly dedicated to delivering a product that is as streamlined and secure as possible. Our mission is to set a new standard for security in the auditing sector, while increasing accessibility to top tier audits for all projects in the crypto space. Our dedication and passion to continuously improve the DeFi space is second to none.