softstack

Penetration Test Report

CUSTOMER	Edel Finance
TARGET	*.edel-api.xyz (Development)
DATE	18.10.2026

Made in Germany by softstack GmbH

Table of Contents

1. Disclaimer 4

2. About the Project and Company 5

3. Executive Summary 6

4. Scope & Methodology 8

5. Target Infrastructure & Architecture 10

6. API Endpoint Map 12

7. Vulnerability Findings 16

7.1 Backend dependencies pinned to versions with known CVEs 18

7.2 Cross-user prompt injection through counterpartyOrderId in MCP trade history 19

7.3 Origin reachable outside Cloudflare, with rate limiting keyed on a client-controlled header 20

7.4 Managed challenge blocks programmatic API clients but not browser navigation 20

7.5 Demo origin exposes an unauthenticated /api/dev proxy with wildcard CORS 21

7.6 clientOrderId is stored and reflected verbatim as orderId 21

7.7 User enumeration on POST /v1/auth/login/init 22

7.8 TLS 1.0 and 1.1 still enabled at the Cloudflare edge 23

7.9 Missing security headers on the admin (Next.js) responses 23

7.10 Containers run as root 24

7.11 GitHub Actions are not pinned to commit SHAs 24

7.12 Withdrawal confirmation validates the identifier after running upstream gates 25

7.13 IMDS hop limit allows containers to reach instance metadata 25

7.14 Missing HSTS header on API responses 26

7.15 Origin provider and internal trace identifiers disclosed in response headers 26

7.16 Missing security headers on API application responses 27

7.17 Cloudflare managed challenge is applied inconsistently across the admin host 27

7.18 Cloudflare bot gate on the API host is satisfied by a browser-like User-Agent 28

7.19 autoClose take-profit and stop-loss are not validated against side and entry 28

7.20 API documentation and OpenAPI specification exposed on the origin 29

7.21 Large public payload served without throttling 29

7.22 MCP hardening gaps in response handling and rate limiting 30

7.23 Infrastructure hardening gaps in the Terraform configuration 30

7.24 400 "unknown account id" returned for a valid, owned account 31

7.25 OpenAPI specification does not match live responses 31

7.26 Lenient validation on the public candles.limit parameter 32

7.27 KYC skip and affiliate self-referral need verification where KYC is enforced 32
8. Re-Test Results **34**
9. Positive Security Controls **37**
10. Complete Test Inventory **38**
11. Risk Summary Matrix **40**
12. Appendices **41**
13. About the Auditor **43**
14. Glossary **44**

1. Disclaimer

The audit makes no statements or warrantees about utility of the code, safety of the code, suitability of the business model, investment advice, endorsement of the platform or its products, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only.

The information presented in this report is confidential and privileged. If you are reading this report, you agree to keep it confidential, not to copy, disclose or disseminate without the agreement of the client. If you are not the intended receptor of this document, remember that any disclosure, copying or dissemination of it is forbidden.

Version History

Version	Date	Description
0.1	05.10.2026	Creation of the report
0.2	06.10.2026	Setup of the pentest environment
1.0	08.10.2026 - 13.10.2026	Testing phase
1.1	17.10.2026	Re-test after remediation
2.0	18.10.2026	Final report

2. About the Project and Company

Company	Titan Labs Limited
Address	c/o Little Bay Corporate Services Limited, 3rd Floor, Ritter House, P.O. Box 3198, Road Town, Tortola, VG1110, British Virgin Islands
Website	https://www.edel.finance/

Edel Finance builds open finance infrastructure for tokenized equities. Its thesis is that tokenization changes more than who owns an asset: once equities move on-chain they become programmable, liquidity becomes portable, and the market stops behaving like a set of separate venues and starts behaving like a single system. Edel positions itself as the operating layer for that system, connecting access, assets, liquidity, exposure and the settlement networks underneath into one programmable stack.

The company delivers this through four connected products. EdelEQUITIES offers round-the-clock trading and custody of tokenized equities with institutional-grade settlement on the Canton Network. EdelMARKETS provides the execution, settlement and market-making infrastructure for those assets across public liquidity networks, and extends into perpetual futures for programmable markets. EdelRUNWAY gives tokenized issuers structured financing rails to raise, deploy and manage capital on-chain. EdelVAULTS, built on Ethereum, packages risk-defined exposure, looping and yield strategies on top of the tokenized equity markets.

The platform is built around the Canton Network, where Edel operates its own validator and where tokenized equity trading and settlement are already live, alongside partners including Base, Ethereum, LayerZero, Kraken and xStocks. Access is programmatic as much as graphical: a REST API and a CCXT-compatible layer serve traders and integrators, a ticket-gated WebSocket stream carries market and account events, a Model Context Protocol server lets AI agents operate accounts under scoped keys, and an internal dashboard gives operators market, bot and withdrawal controls. Edel Finance is operated by Titan Labs Limited, registered in the British Virgin Islands.

3. Executive Summary

softstack GmbH carried out an owner-authorized penetration test of the Edel Finance perpetual futures backend between 8 and 13 October 2026. Testing covered the development environment only, [redacted]. The team worked with access to the backend source tree and to a seeded development trading account, which allowed every network observation to be traced back to the code path that produced it.

The assessment produced 27 findings: 2 High, 5 Medium, 17 Low and 3 Informational. There were no Critical findings and no broken access control. The money path, from deposit through order placement, fill and position close, reconciled correctly throughout. Object-level authorization held on every account-scoped route and on batch order operations, bearer token validation behaved correctly, and the commands that move value failed closed when their dependencies were unavailable. For a trading venue, these are the controls that matter most, and they were sound.

[redacted]

All findings were remediated or formally accepted during the remediation window. The re-test on 17 October 2026 confirmed 25 findings fixed and 2 accepted as residual risk, with no finding left in an open state.

2	5	17	3
HIGH	MEDIUM	LOW	INFORMATIONAL

Key Risk Areas

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

Immediate Action Items

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]
5. [redacted]
6. [redacted]
7. [redacted]

Re-Test Update (October 17, 2026)

A full re-test was performed on 17 October 2026 against the same development environment. Every finding was re-verified, either against the merged remediation commit or, for the findings that live in the Cloudflare zone configuration rather than in code, against the live edge.

- 25 of 27 findings fixed and verified, including both High findings
- 2 findings formally accepted as residual risk, both relating to the deliberate scope of the Cloudflare managed challenge
- 0 findings remain open
- 23 remediation pull requests were merged into the backend between 11 and 18 October 2026

4. Scope & Methodology

Target	[redacted]
Hosts in scope	[redacted]
Out of scope	[redacted]
Test type	Grey-box, owner-authorized, source-assisted
Credentials provided	[redacted]
Test period	8 - 13 October 2026
Re-test date	17 October 2026
Methodology	OWASP Testing Guide v4, OWASP API Security Top 10, PTES
Report version	2.0 (Re-Test)

Testing Phases

Phase	Description	Tools
1. Reconnaissance	Host and surface enumeration, DNS and certificate inspection, TLS configuration review, and identification of the hosting and edge providers behind each host	DNS enumeration, TLS scanners, certificate transparency
2. Surface mapping	Reconstruction of the REST, WebSocket, MCP and admin surfaces from the committed OpenAPI and AsyncAPI contracts and from route and tool code, cross-checked against live responses	OpenAPI and AsyncAPI contracts, route and tool source, HTTP client
3. Authentication and authorization	Bearer token validation, object-level authorization on account-scoped routes and batch operations, WebSocket ticket scope, MCP API-key isolation, and the operator and bot shared-secret header planes	Headless browser, HTTP client, manual review

Phase	Description	Tools
4. Business logic and money path	Deposit, order placement, fill, position close and withdrawal flows, including reduce-only handling, leverage limits, self-trade prevention, idempotency and the withdrawal state machine	Seeded development account, HTTP client, manual review
5. Input validation and fuzzing	Schema-driven fuzzing of the documented operations and targeted testing of identifiers that cross user and system boundaries	Property-based API fuzzing, manual payload crafting
6. Infrastructure and supply chain	Dependency advisory review, container image inspection, infrastructure-as-code review and CI workflow review	Dependency and container advisory scanners, manual IaC review
7. Edge behaviour	Measurement of how the Cloudflare managed challenge responds to different client types and routes, and whether the origin is reachable outside the edge	Headless browser, HTTP client
8. Re-test	Verification of each remediation against its merged commit, and re-verification of the edge and transport findings against the live development hosts	Merge commit review, HTTP client, TLS client

5. Target Infrastructure & Architecture

Infrastructure Components

Component	Technology	Version	Details
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Network Topology

Asset	IP Addresses	Purpose
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Subdomains Discovered (6)

[redacted]

6. API Endpoint Map

The following 83 API endpoints were identified across the tested surfaces and exercised during the engagement.

Public (no authentication)

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Accounts and positions

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Orders, withdrawals, realtime and keys

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

CCXT compatibility layer (v2)

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

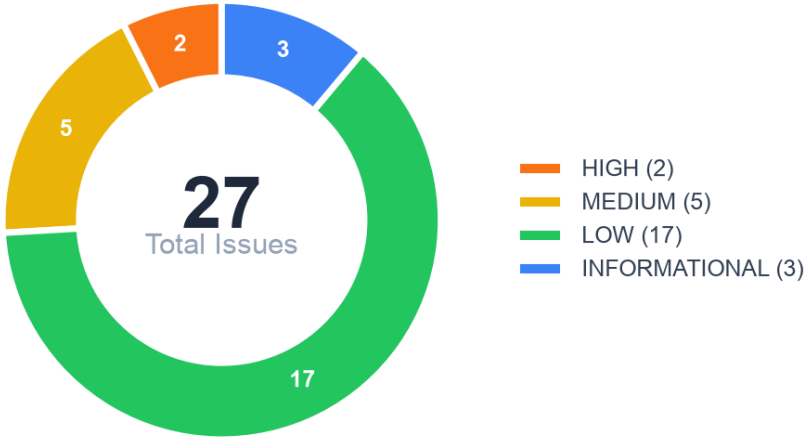
Internal control plane

Method	Path	Auth	Description
[redacted]	[redacted]	[redacted]	[redacted]

7. Vulnerability Findings

Findings Overview

Findings are classified by severity: Critical, High, Medium, Low, and Informational.



No	ID	Title	Severity	CVSS	Status
7.1	H-01	Backend dependencies pinned to versions with known CVEs	HIGH	9.5	FIXED
7.2	H-02	Cross-user prompt injection through counterpartyOrderId in MCP trade history	HIGH	7.3	FIXED
7.3	M-01	Origin reachable outside Cloudflare, with rate limiting keyed on a client-controlled header	MEDIUM	7.3	FIXED
7.4	M-02	Managed challenge blocks programmatic API clients but not browser navigation	MEDIUM	5.3	FIXED
7.5	M-03		MEDIUM	6.5	FIXED

No	ID	Title	Severity	CVSS	Status
		Demo origin exposes an unauthenticated /api/dev proxy with wildcard CORS			
7.6	M-04	clientOrderId is stored and reflected verbatim as orderId	MEDIUM	6.5	FIXED
7.7	M-05	User enumeration on POST /v1/auth/login/init	MEDIUM	5.3	FIXED
7.8	L-01	TLS 1.0 and 1.1 still enabled at the Cloudflare edge	LOW	3.7	FIXED
7.9	L-02	Missing security headers on the admin (Next.js) responses	LOW	4.3	FIXED
7.10	L-03	Containers run as root	LOW	4.4	FIXED
7.11	L-04	GitHub Actions are not pinned to commit SHAs	LOW	6.6	FIXED
7.12	L-05	Withdrawal confirmation validates the identifier after running upstream gates	LOW	4.3	FIXED
7.13	L-06	IMDS hop limit allows containers to reach instance metadata	LOW	4.4	FIXED
7.14	L-07	Missing HSTS header on API responses	LOW	3.1	FIXED
7.15	L-08	Origin provider and internal trace identifiers disclosed in response headers	LOW	3.7	FIXED
7.16	L-09	Missing security headers on API application responses	LOW	3.1	FIXED
7.17	L-10	Cloudflare managed challenge is applied inconsistently across the admin host	LOW	3.1	ACKNOWLEDGED
7.18	L-11	Cloudflare bot gate on the API host is satisfied by a browser-like User-Agent	LOW	3.7	ACKNOWLEDGED
7.19	L-12	autoClose take-profit and stop-loss are not validated against side and entry	LOW	2.7	FIXED

No	ID	Title	Severity	CVSS	Status
7.20	L-13	API documentation and OpenAPI specification exposed on the origin	LOW	5.3	FIXED
7.21	L-14	Large public payload served without throttling	LOW	5.3	FIXED
7.22	L-15	MCP hardening gaps in response handling and rate limiting	LOW	3.7	FIXED
7.23	L-16	Infrastructure hardening gaps in the Terraform configuration	LOW	n/a	FIXED
7.24	L-17	400 "unknown account id" returned for a valid, owned account	LOW	n/a	FIXED
7.25	I-01	OpenAPI specification does not match live responses	INFORMATIONAL	n/a	FIXED
7.26	I-02	Lenient validation on the public candles.limit parameter	INFORMATIONAL	n/a	FIXED
7.27	I-03	KYC skip and affiliate self-referral need verification where KYC is enforced	INFORMATIONAL	n/a	FIXED

7.1 Backend dependencies pinned to versions with known CVEs

H-01 HIGH CVSS 9.5 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

[redacted]

RECOMMENDATION

- [redacted]

7.2 Cross-user prompt injection through counterpartyOrderId in MCP trade history

H-02 HIGH CVSS 7.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

- [redacted]

7.3 Origin reachable outside Cloudflare, with rate limiting keyed on a client-controlled header

M-01 MEDIUM CVSS 7.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

- [redacted]
- [redacted]

7.4 Managed challenge blocks programmatic API clients but not browser navigation

M-02 MEDIUM CVSS 5.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

[redacted]

RECOMMENDATION

[redacted]

7.5 Demo origin exposes an unauthenticated /api/dev proxy with wildcard CORS

M-03 MEDIUM CVSS 6.5 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.6 clientOrderId is stored and reflected verbatim as orderId

M-04 MEDIUM CVSS 6.5 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

- [redacted]
- [redacted]

7.7 User enumeration on POST /v1/auth/login/init

M-05 MEDIUM CVSS 5.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.8 TLS 1.0 and 1.1 still enabled at the Cloudflare edge

L-01 LOW CVSS 3.7 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.9 Missing security headers on the admin (Next.js) responses

L-02 LOW CVSS 4.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.10 Containers run as root

L-03 LOW CVSS 4.4 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

- [redacted]
- [redacted]

7.11 GitHub Actions are not pinned to commit SHAs

L-04 LOW CVSS 6.6 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

- [redacted]

- [redacted]

7.12 Withdrawal confirmation validates the identifier after running upstream gates

L-05 LOW CVSS 4.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.13 IMDS hop limit allows containers to reach instance metadata

L-06 LOW CVSS 4.4 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

[redacted]

7.14 Missing HSTS header on API responses

L-07 LOW CVSS 3.1 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.15 Origin provider and internal trace identifiers disclosed in response headers

L-08 LOW CVSS 3.7 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

[redacted]

RECOMMENDATION

[redacted]

7.16 Missing security headers on API application responses

L-09 LOW CVSS 3.1 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.17 Cloudflare managed challenge is applied inconsistently across the admin host

L-10 LOW CVSS 3.1 ACKNOWLEDGED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.18 Cloudflare bot gate on the API host is satisfied by a browser-like User-Agent

L-11 LOW CVSS 3.7 ACKNOWLEDGED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.19 autoClose take-profit and stop-loss are not validated against side and entry

L-12 LOW CVSS 2.7 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

PROOF OF CONCEPT

[redacted]

RECOMMENDATION

[redacted]

7.20 API documentation and OpenAPI specification exposed on the origin

L-13 LOW CVSS 5.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.21 Large public payload served without throttling

L-14 LOW CVSS 5.3 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.22 MCP hardening gaps in response handling and rate limiting

L-15 LOW CVSS 3.7 FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

7.23 Infrastructure hardening gaps in the Terraform configuration

L-16 LOW FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.24 400 "unknown account id" returned for a valid, owned account

L-17 LOW FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.25 OpenAPI specification does not match live responses

I-01 INFORMATIONAL FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.26 Lenient validation on the public candles.limit parameter

I-02 INFORMATIONAL FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]

7.27 KYC skip and affiliate self-referral need verification where KYC is enforced

I-03 INFORMATIONAL FIXED

TARGET

[redacted]

DESCRIPTION

[redacted]

RECOMMENDATION

[redacted]



8. Re-Test Results (October 17, 2026)

25	2	0
FIXED	ACCEPTED RISK	STILL VULNERABLE

Detailed Re-Test Results

ID	Finding	Original Severity	Re-Test Status	Evidence
H-01	Backend dependencies pinned to versions with known CVEs	HIGH	FIXED	[redacted]
H-02	Cross-user prompt injection through counterpartyOrderId in MCP trade history	HIGH	FIXED	[redacted]
M-01	Origin reachable outside Cloudflare, with rate limiting keyed on a client-controlled header	MEDIUM	FIXED	[redacted]
M-02	Managed challenge blocks programmatic API clients but not browser navigation	MEDIUM	FIXED	[redacted]
M-03	Demo origin exposes an unauthenticated /api/dev proxy with wildcard CORS	MEDIUM	FIXED	[redacted]
M-04	clientOrderId is stored and reflected verbatim as orderId	MEDIUM	FIXED	[redacted]
M-05	User enumeration on POST /v1/auth/login/init	MEDIUM	FIXED	[redacted]
L-01	TLS 1.0 and 1.1 still enabled at the Cloudflare edge	LOW	FIXED	[redacted]
L-02	Missing security headers on the admin (Next.js) responses	LOW	FIXED	[redacted]

ID	Finding	Original Severity	Re-Test Status	Evidence
				[redacted]
L-03	Containers run as root	LOW	FIXED	[redacted]
L-04	GitHub Actions are not pinned to commit SHAs	LOW	FIXED	[redacted]
L-05	Withdrawal confirmation validates the identifier after running upstream gates	LOW	FIXED	[redacted]
L-06	IMDS hop limit allows containers to reach instance metadata	LOW	FIXED	[redacted]
L-07	Missing HSTS header on API responses	LOW	FIXED	[redacted]
L-08	Origin provider and internal trace identifiers disclosed in response headers	LOW	FIXED	[redacted]
L-09	Missing security headers on API application responses	LOW	FIXED	[redacted]
L-10	Cloudflare managed challenge is applied inconsistently across the admin host	LOW	ACKNOWLEDGED	[redacted]
L-11	Cloudflare bot gate on the API host is satisfied by a browser-like User-Agent	LOW	ACKNOWLEDGED	[redacted]
L-12	autoClose take-profit and stop-loss are not validated against side and entry	LOW	FIXED	[redacted]
L-13	API documentation and OpenAPI specification exposed on the origin	LOW	FIXED	[redacted]
L-14	Large public payload served without throttling	LOW	FIXED	[redacted]

ID	Finding	Original Severity	Re-Test Status	Evidence
L-15	MCP hardening gaps in response handling and rate limiting	LOW	FIXED	[redacted]
L-16	Infrastructure hardening gaps in the Terraform configuration	LOW	FIXED	[redacted]
L-17	400 "unknown account id" returned for a valid, owned account	LOW	FIXED	[redacted]
I-01	OpenAPI specification does not match live responses	INFORMATIONAL	FIXED	[redacted]
I-02	Lenient validation on the public candles.limit parameter	INFORMATIONAL	FIXED	[redacted]
I-03	KYC skip and affiliate self-referral need verification where KYC is enforced	INFORMATIONAL	FIXED	[redacted]

Re-Test Methodology

- [redacted]

Conclusion

[redacted]

9. Positive Security Controls

The following security mechanisms were tested and found to be properly implemented:

- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]
- ✓ [redacted]

10. Complete Test Inventory

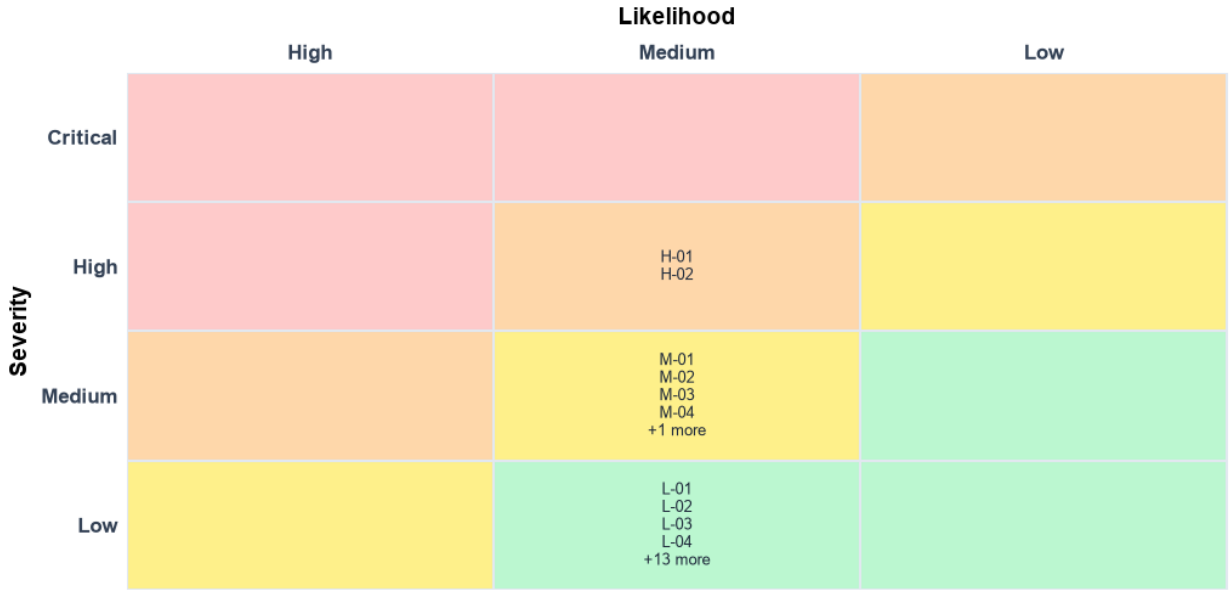
36 distinct tests were performed across 8 phases.

Phase	Category	Test	Result
Reconnaissance	DNS and certificates	[redacted]	[redacted]
Reconnaissance	TLS	[redacted]	[redacted]
Reconnaissance	Secrets	[redacted]	[redacted]
Surface mapping	REST	[redacted]	[redacted]
Surface mapping	Documentation	[redacted]	[redacted]
Surface mapping	API contract	[redacted]	[redacted]
Surface mapping	Internal routes	[redacted]	[redacted]
Authentication	Bearer tokens	[redacted]	[redacted]
Authentication	Account enumeration	[redacted]	[redacted]
Authorization	Object-level access	[redacted]	[redacted]
Authorization	Realtime	[redacted]	[redacted]
Authorization	MCP	[redacted]	[redacted]
Authorization	Account resolution	[redacted]	[redacted]
Authorization	Admin	[redacted]	[redacted]
Business logic	Money path	[redacted]	[redacted]
Business logic	Risk limits	[redacted]	[redacted]
Business logic	Withdrawals	[redacted]	[redacted]
Business logic	Orders	[redacted]	[redacted]
Business logic	KYC and affiliates	[redacted]	[redacted]
Input validation	Identifiers	[redacted]	[redacted]
Input validation	Public parameters	[redacted]	[redacted]
Input validation	Payload size	[redacted]	[redacted]
		[redacted]	[redacted]

Phase	Category	Test	Result
Supply chain	Dependencies		
Supply chain	CI	[redacted]	[redacted]
Infrastructure	Containers	[redacted]	[redacted]
Infrastructure	Instance metadata	[redacted]	[redacted]
Infrastructure	Logging and encryption	[redacted]	[redacted]
Edge	Managed challenge	[redacted]	[redacted]
Edge	Managed challenge	[redacted]	[redacted]
Edge	Bot gate	[redacted]	[redacted]
Edge	Origin exposure	[redacted]	[redacted]
Edge	Response headers	[redacted]	[redacted]
Edge	Security headers	[redacted]	[redacted]
Edge	Cross-origin	[redacted]	[redacted]
AI agent surface	MCP	[redacted]	[redacted]
AI agent surface	MCP	[redacted]	[redacted]

11. Risk Summary Matrix

Risk is assessed as the combination of **Severity** (potential impact) and **Likelihood** (ease of exploitation).



12. Appendices

A. Tools Used

Tool	Purpose
Headless Chromium (Playwright)	Measuring Cloudflare challenge behaviour across navigation, in-page fetch and proxy paths, and exercising authenticated browser flows
Schema-driven API fuzzer	Property-based fuzzing of the documented REST operations against the committed OpenAPI contract
nmap	Service and port exposure checks against the in-scope hosts
sslscan / OpenSSL s_client	TLS protocol version and cipher suite enumeration, including the re-test of legacy TLS support
OSV and Trivy	Dependency and container image advisory review against the committed lockfile
curl	Request and response inspection, header collection and edge behaviour comparison between client types
Manual source review	Tracing each observation to the route, contract or infrastructure-as-code definition that produced it

B. Software Inventory (14 Components)

Component	Version	Layer	Confidence
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Component	Version	Layer	Confidence
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

13. About the Auditor

Established in 2017 under the name Chainsulting, and rebranded as softstack GmbH in 2023, softstack has been a trusted name in Web3 Security space. Within the rapidly growing Web3 industry, softstack provides a comprehensive range of offerings that include software development, cybersecurity, and consulting services. Softstack's competency extends across the security landscape of prominent blockchains like Solana, Tezos, TON, Ethereum and Polygon. The company is widely recognized for conducting thorough code audits aimed at mitigating risk and promoting transparency.

The firm's proficiency lies particularly in assessing and fortifying smart contracts of leading DeFi projects, a testament to their commitment to maintaining the integrity of these innovative financial platforms. To date, softstack plays a crucial role in safeguarding over $100 billion worth of user funds in various DeFi protocols.

Underpinned by a team of industry veterans possessing robust technical knowledge in the Web3 domain, softstack offers industry-leading smart contract audit services. Committed to evolving with their clients' ever-changing business needs, softstack's approach is as dynamic and innovative as the industry it serves.

Check our website for further information: https://softstack.io

14. Glossary

Term	Definition
API	Application Programming Interface
BOLA	Broken Object Level Authorization
CCXT	CryptoCurrency eXchange Trading library
CI	Continuous Integration
CORS	Cross-Origin Resource Sharing
CSP	Content Security Policy
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DAML	Digital Asset Modelling Language
HSTS	HTTP Strict Transport Security
IDOR	Insecure Direct Object Reference
IMDS	Instance Metadata Service
IaC	Infrastructure as Code
JWT	JSON Web Token
KYC	Know Your Customer
MCP	Model Context Protocol
NATS	Neural Autonomic Transport System (messaging platform)
OWASP	Open Worldwide Application Security Project
PTES	Penetration Testing Execution Standard
RBAC	Role-Based Access Control
REST	Representational State Transfer
SHA	Secure Hash Algorithm
TLS	Transport Layer Security

Term	Definition
TP/SL	Take Profit / Stop Loss
WAF	Web Application Firewall
XFF	X-Forwarded-For
XSS	Cross-Site Scripting