QCC TOKEN & SALE

QuickCamCoin v1.0 · Audit.

A line-by-line review of the QCC token and sale contracts. Three static-analysis tools were run against the codebase. **1,177 lines** were read end-to-end. **509 detector candidates** were reviewed against the source by hand.

0 FINDINGS SUMMARY

FINDINGS RETAINED AFTER REVIEW

Across Critical · High · Medium · Low · Informational. All engine candidates were categorized and excluded during triage.

LINES REVIEWED

1,177

across **4 production contracts**. All source read end-to-end.

CODE MATURITY

12 of 16

Strong or **Sound**. Two moderates are design decisions, not weaknesses.

COMMIT	SCANNED	SCOPE	ENGINES	DURATION
594d5ee	2026-05-06	4 contracts	Slither · Aderyn · Semgrep	4 weeks

How this audit happened

5-STEP WORKFLOW

1. **Scope lock** — Identify 4 production .sol files and dependencies.
2. **Tool sweep** — Slither, Aderyn, Semgrep against full compilation unit.
3. **Read pass** — Hand-read every contract end-to-end, top to bottom.
4. **Triage** — Read each candidate against the source. Categorize as retained or excluded.
5. **Report** — Score maturity. Write findings + review matrix.

01 FINDINGS BY SEVERITY

Zero across every tier.

Critical and **High** would block deployment. **Medium** and **Low** are issues to fix. **Informational** are best-practice notes. None present at any level.

✓ CLEAN	✓ CLEAN	✓ CLEAN	✓ CLEAN	✓ CLEAN
0	**0**	**0**	**0**	**0**
CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
Immediate risk of loss	Must fix before deployment	Should fix or document	Quality / minor impact	Best-practice notes only

02 TRIAGE FUNNEL

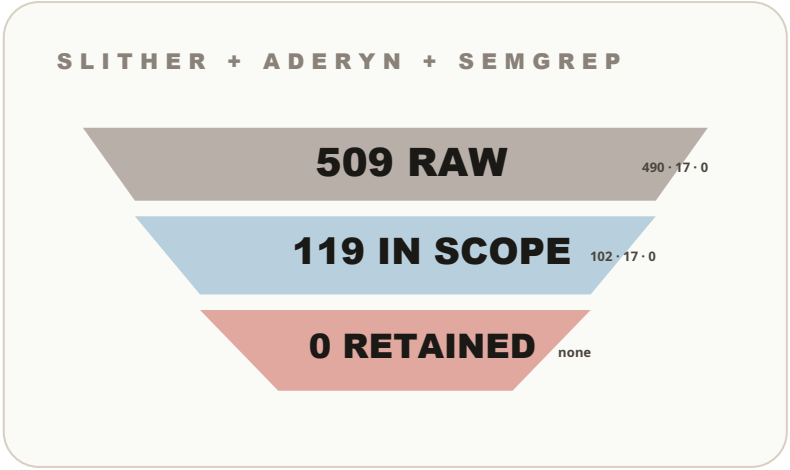
509 candidates in. Zero bugs out.

Static analyzers flag every pattern that *might* be a problem. We read each one against the actual code to see if it's real. Most are not.

Each survivor is a retained finding.

Scanner output is mostly false positives, intentional design choices, or stylistic preferences. Items retained after manual review are what reached the report.

Raw	all detector hits
In scope	inside the 4 prod files
Retained	findings kept after review



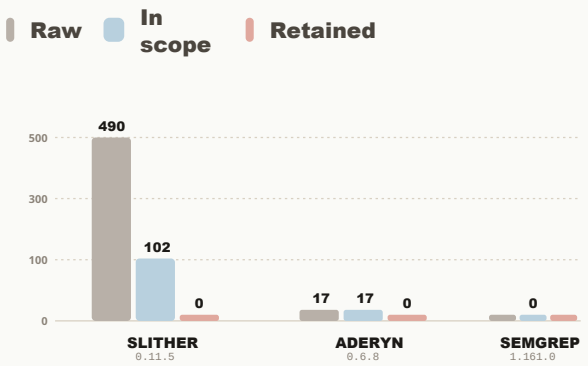
> **Every public/payable entry holds nonReentrant. The price feed has all three Chainlink freshness checks. The upgrade path is role-gated end-to-end.**
>
> — REVIEW MATRIX, CONDENSED

Three engines. One source of truth.

Each engine catches different patterns. Running all three plus a hand-review gives broader coverage than any single tool.

Findings by engine

Raw vs. in-scope vs. retained. Slither found more candidates; all dropped after review.



Code quality scorecard

16 craftsmanship categories, modeled on Trail of Bits's Code Maturity rubric.

Access Controls	STRONG
Data Handling	STRONG
Authentication	STRONG
Error Handling	STRONG
Upgradeability	STRONG
Testing	STRONG
Arithmetic	SOUND
Complexity Mgmt.	SOUND
Configuration	SOUND
Documentation	SOUND
Transaction Order	SOUND
Front-Run Resist.	SOUND
Auditing (Events)	MODERATE
Decentralization	MODERATE
Cryptography	N/A
Memory Safety	N/A

04 WHAT WE LOOKED AT

Six attack classes. All reviewed.

Common patterns that have affected other crypto projects, read against the QCC source as part of the manual review.

1

Reentrancy

Can an attacker call back mid-execution to drain funds?

✓ NONREENTRANT ON EVERY ENTRY

2

Oracle staleness

Can a stale ETH/USD price mint QCC at a stolen rate?

✓ 3 CHAINLINK FRESHNESS CHECKS

3

Upgrade hijack

Could a bad actor swap in a malicious version?

✓ UUPS GATED BY ADMIN ROLE

4

Access control

Are privileged setters truly gated? Sale callable directly?

✓ RBAC + ONLYTOKEN DELEGATION

5

Caps & slippage

Can someone buy more than their share or settle at a stolen price?

✓ PER-USER + PER-TIER + MIN-OUT

6

Tokenomics drift

Are burns and treasury flows bounded over time?

✓ MONOTONIC + CAPPED SCHEDULES

05 SCOPE

Four production contracts.

All source read end-to-end. OpenZeppelin and Chainlink dependencies treated as trusted libraries.

IN-SCOPE SOURCE

contracts/QuickCamCoinUpgradeable.sol	587 LoC
contracts/QCCSaleUpgradeable.sol	560 LoC
contracts/Proxy.sol	22 LoC
contracts/IQCCToken.sol	8 LoC

1,177

LINES OF SOLIDITY