# QCC Security Audit — Summary

Prepared for Promanager by Bitspur (auditor)

Independent smart-contract security review

## Contents



## QuickCamCoin (QCC) — security audit summary

**Verdict:** PASS

*No publicly-exploitable vulnerabilities identified. All engine candidates were reproduced against the source and dropped after triage.*

### Findings by severity

| Critical | High | Medium | Low | Informational |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |

### Scope

- `contracts/QuickCamCoinUpgradeable.sol`
- `contracts/QCCSaleUpgradeable.sol`
- `contracts/Proxy.sol`
- `contracts/IQCCToken.sol`

*1177 lines in scope*

### Provenance

- **Client:** Promanager
- **Auditor:** Bitspur
- **Scanned (UTC):** 2026-05-06T23:45:01Z

*Independent security review of source code. Not a CPA attestation; not legal or investment advice.*

### Tools used (multi-engine scan)

***Raw*** *= total detector hits across the whole build (incl. OZ / Chainlink / mocks).* ***In scope*** *= subset inside the four production scope files.* ***Retained*** *= survivors of manual triage. Everything else is on the* ***Results*** *page under* Triaged.

| Engine | Version | Raw | In scope | Retained | Note |
|---|---|---|---|---|---|
| slither | 0.11.5 | 490 | 102 | 0 | 490 detector-level results across the full compilation unit (including OZ internals). 102 in-scope to project contracts. None retained — all dropped per triage rubric (style, intentional rounding, intentional centralization, mitigated reentrancy, etc.). |
| aderyn | 0.6.8 | 17 | 17 | 0 | All 17 issues dropped. The 2 high-severity items (Ether-locked, unsafe-casting) are confirmed false positives against test/proxy contracts; the 15 low-severity items are centralization noise on privileged setters or style preferences. |
| semgrep | 1.161.0 | 0 | 0 | 0 | The public p/solidity rule pack returned HTTP 404 from semgrep.dev/c/p/solidity (registry change), so the substitute p/security-audit pack was used and ran cleanly with zero matches on the in-scope Solidity sources. Slither and Aderyn cover the same patterns the unavailable solidity pack would have targeted. |

## Code maturity

Per-category maturity ratings, modeled on the Trail of Bits Code Maturity scorecard. Reflects what the audit observed in source and tests, not just whether the engines flagged something.

| Category | Rating | Note |
|---|---|---|
| Access Controls | **Strong** | RBAC + Ownable across all privileged entry points; privilege graph traced end-to-end; setSaleContract requires non-zero address. |
| Arithmetic | **Sound** | Tiered-pricing math uses intentional ceiling rounding favorable to the protocol; precision loss is bounded; no unchecked/asm arithmetic. |
| Auditing (Events) | **Moderate** | Three setters (token.sol:167,182,203) emit no events. Privileged-only, so observability gap rather than exploit. Recommended in a future minor revision. |
| Authentication | **Strong** | onlyToken delegation pattern means QCCSale's mutating surface is unreachable except via the role-gated token contract. |
| Complexity Management | **Sound** | Token/sale split exists to stay under 24KB; the price-tier loop is bounded; UUPS adds upgrade-time complexity which is offset by storage gaps. |
| Configuration | **Sound** | Initializer-based bootstrapping; named roles + threshold list; all setters role-gated. |
| Cryptography | **Not Applicable** | Inherits OZ ERC20Permit (EIP-2612). No custom signing or key handling. |

| Category | Rating | Note |
|---|---|---|
| Data Handling | **Strong** | Slippage protection (minQccAmount), per-user / per-tier purchase caps, ETH refund on partial fills, MaxSupplyExceeded enforced on the sale path. |
| Decentralization | **Moderate** | Centralization is intentional and documented: admin/operational/pauser/minter roles can pause, set thresholds, withdraw ETH, and upgrade. Trust in role-holders is required by design. |
| Documentation | **Sound** | Inline NatSpec is sparse on both production contracts; this audit report serves as the primary documentation supplement. Recommended for a future revision. |
| Error Handling | **Strong** | Custom errors used throughout both contracts; revert reasons are unambiguous. |
| Maintenance / Upgradeability | **Strong** | UUPS with ___gap reserves on both contracts, _disableInitializers in constructors, _authorizeUpgrade gated by admin role / owner. |
| Memory Safety | **Not Applicable** | Solidity 0.8.x; no inline assembly outside of OZ ERC1967 storage-slot patterns. |
| Testing | **Strong** | Multiple Hardhat test files (V331, edge cases, coverage enhancement, burn schedule, upgrade verification) plus a harness contract for unreachable-path coverage. |
| Transaction Ordering | **Sound** | nonReentrant on every public/payable entry point on both contracts; partial CEI ordering in _processPurchase is mitigated by the dual-side reentrancy lock. |
| Front-Running Resistance | **Sound** | Slippage parameter on buyQCC bounds adverse pricing; tier prices are deterministic from on-chain state and the Chainlink feed. |

*Scale: Strong · Sound · Moderate · Weak · Missing · Not Applicable*

*Independent security review of source code. Not a CPA attestation; not legal or investment advice.*