QuantAMM V1 Audit Report

Prepared by Cyfrin

Version 1.0

Lead Auditors

0kage

May 1, 2025

Contents

1 About Cyfrin

Cyfrin is a Web3 security company dedicated to bringing industry-leading protection and education to our partners and their projects. Our goal is to create a safe, reliable, and transparent environment for everyone in Web3 and DeFi. Learn more about us at cyfrin.io.

2 Disclaimer

The Cyfrin team makes every effort to find as many vulnerabilities in the code as possible in the given time but holds no responsibility for the findings in this document. A security audit by the team does not endorse the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the solidity implementation of the contracts.

3 Risk Classification

	Impact: High	Impact: Medium	Impact: Low
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4 Protocol Summary

5 Audit Scope

The scope of this audit included changes introduced in the following pull requests.

- PR 53
- PR 54
- PR 55
- PR 56
- PR 57
- PR 58

6 Executive Summary

Over the course of 3 days, the Cyfrin team conducted an audit on the QuantAMM V1 smart contracts provided by QuantAMM. In this period, a total of 0 issues were found.

This audit focused on a targeted review of recent updates to the QuantAMM protocol, specifically evaluating the code changes introduced in a set of pull requests (PRs). The scope was limited to reviewing specific diffs associated with PRs merged since the last audited codebase, rather than performing a full protocol or system-wide audit.

Key Findings:

- **PR 53**: Adjusted Hardhat configuration to modify optimizer runs – No issues found.
- **PR 54**: Introduced intermediate covariance and gradient state functions – Logic and tests validated as sound.

- **PR 55**: Implemented event emissions for CalculateWeightsRequest and CalculateWeightsResponse – Functionality verified.

- **PR 56**: Changed update_interval variable type to uint40 – No issues found.

- **PR 57**: Flattened weights and multipliers; revised WeightsUpdated event – No concerns raised.

- **PR 58**: Enabled manual setting of target weights; suggested an update to NatSpec documentation – Implementation confirmed.

All changes were reviewed for logical integrity and associated test coverage, both of which were found to be adequate and aligned with the intended functionality. No issues were identified during this diff audit.

Summary

Project Name	QuantAMM V1
Repository	QuantAMM-V1
Commit	3cfe58cf30c6...
Audit Timeline	Apr 23rd - Apr 25th
Methods	Manual Review, Stateful Fuzzing

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Informational	0
Gas Optimizations	0
Total Issues	0

Summary of Findings

-