



SHERLOCK

SHERLOCK SECURITY REVIEW FOR



Prepared for:

Gitcoin

Prepared by:

Sherlock

Lead Security Expert:

0x52

Dates Audited:

March 27 - March 31, 2023

Prepared on:

April 17, 2023

Introduction

Allo Protocol is a set of smart contracts that enable the democratic allocation and distribution of funds through the power of Quadratic Funding.

Scope

[contracts @ 36dc33762c396660c0a84f6ef7d790f632638e81](#)

- [contracts/contracts/payoutStrategy/IPayoutStrategy.sol](#)
- [contracts/contracts/payoutStrategy/MerklePayoutStrategy/MerklePayoutStrategyFactory.sol](#)
- [contracts/contracts/payoutStrategy/MerklePayoutStrategy/MerklePayoutStrategyImplementation.sol](#)
- [contracts/contracts/program/ProgramFactory.sol](#)
- [contracts/contracts/program/ProgramImplementation.sol](#)
- [contracts/contracts/projectRegistry/ProjectRegistry.sol](#)
- [contracts/contracts/round/IRoundFactory.sol](#)
- [contracts/contracts/round/IRoundImplementation.sol](#)
- [contracts/contracts/round/RoundFactory.sol](#)
- [contracts/contracts/round/RoundImplementation.sol](#)
- [contracts/contracts/settings/AlloSettings.sol](#)
- [contracts/contracts/utils/MetaPtr.sol](#)
- [contracts/contracts/votingStrategy/IVotingStrategy.sol](#)
- [contracts/contracts/votingStrategy/QuadraticFundingStrategy/QuadraticFundingVotingStrategyFactory.sol](#)
- [contracts/contracts/votingStrategy/QuadraticFundingStrategy/QuadraticFundingVotingStrategyImplementation.sol](#)

Findings

Each issue has an assigned severity:

- Medium issues are security vulnerabilities that may not be directly exploitable or may require certain conditions in order to be exploited. All major issues should be addressed.
- High issues are directly exploitable security vulnerabilities that need to be fixed.



Issues found

Medium	High
0	0

Issues not fixed or acknowledged

Medium	High
0	0

Security experts who found valid issues

