WiseLending Security Audit

The audit engagement encompassed a specific list of contracts that were present in the commit hash of the repository that was in scope. The tables below detail certain meta-data about the target of the security assessment and a navigation chart is present at the end that links to the relevant findings per file.

Target

- Repository: **https://github.com/wise-foundation/lending-audit**
- Commit: 4470403c94e81c7e523364d77122bd30b045ae34
- Language: Solidity
- Network: Ethereum
- Revisions: 4470403c94, 663245f9d7

Findings Per File

File	Total Finding(s)
contracts/WrapperHub/AaveHub.sol (AHB)	2
contracts/WrapperHub/AaveEvents.sol (AES)	0
contracts/WrapperHub/AaveHelper.sol (AHR)	4
contracts/TransferHub/ApprovalHelper.sol (AHE)	1
contracts/Babylonian.sol (BNA)	1
contracts/TransferHub/CallOptionalReturn.sol (COR)	2
contracts/WiseLiquidation/Declarations.sol (DSN)	3
contracts/WiseOracleHub/Declarations.sol (DSO)	1
contracts/WrapperHub/Declarations.sol (DSI)	3
contracts/FeeManager/DeclarationsFeeManager.sol (DFM)	6
contracts/FeeManager/FeeManager.sol (FMR)	10

File	Total Finding(s)
contracts/FeeManager/FeeManagerEvents.sol (FME)	0
contracts/FeeManager/FeeManagerHelper.sol (FMH)	5
contracts/MainHelper.sol (MHR)	9
contracts/WiseOracleHub/OracleHelper.sol (OHR)	12
contracts/OwnableMaster.sol (OMR)	4
contracts/PoolManager.sol (PMR)	4
contracts/PositionNFTs.sol (PNF)	11
contracts/TransferHub/TransferHelper.sol (THR)	1
contracts/USDEquivalent.sol (USD)	4
contracts/WiseCore.sol (WCE)	3
contracts/WiseLending.sol (WLG)	4
contracts/WiseSecurity/WiseSecurity.sol (WSY)	9
contracts/WiseOracleHub/WiseOracleHub.sol (WOH)	7
contracts/WiseLiquidation/WiseLiquidation.sol (WLN)	0
contracts/WiseLowLevelHelper.sol (WLL)	4
contracts/WiseSecurity/WiseSecurityHelper.sol (WSH)	8
contracts/WiseLiquidation/WiseLiquidationHelper.sol (WLH)	0
contracts/WiseLendingDeclaration.sol (WLD)	6
contracts/WiseSecurity/WiseSecurityDeclarations.sol (WSD)	4

Audit Report Revisions

The execution of our static analysis toolkit identified **931 potential issues** within the codebase of which **759 were ruled out to be false positives** or negligible findings.

The remaining **172 issues** were validated and grouped and formalized into the **45 exhibits** that follow:

ID	Severity	Addressed	Title
AHR-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
AHR-02S	Informational	Partial	Redundant Variable Assignments
AHB-01S	Minor	Yes	Deprecated Native Asset Transfers
AHE-01S	Informational	Nullified	Inexistent Visibility Specifier
COR-01S	Informational	Nullified	Literal Equality of `bool` Variable
DSN-01S	Informational	Acknowledged	Illegible Numeric Value Representations
DSO-01S	Informational	Partial	Inexistent Visibility Specifiers
DSN-02S	Informational	Yes	Inexistent Visibility Specifiers
DSI-01S	Informational	Yes	Inexistent Visibility Specifiers
DSN-03S	Minor	Yes	Inexistent Sanitization of Input Addresses
DSI-02S	Minor	Yes	Inexistent Sanitization of Input Addresses
DFM-01S	Informational	Yes	Illegible Numeric Value Representations

ID	Severity	Addressed	Title
DFM-02S	Informational	Yes	Inexistent Visibility Specifiers
DFM-03S	Minor	Yes	Inexistent Sanitization of Input Addresses
FMR-01S	Informational	Partial	Data Location Optimizations
FMR-02S	Informational	Partial	Inexistent Event Emissions
FMR-03S	Informational	Acknowledged	Literal Equality of `bool` Variables
FMH-01S	Informational	Yes	Redundant Variable Assignments
MHR-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
OMR-01S	Informational	Partial	Inexistent Event Emissions
OMR-02S	Informational	Yes	Inexistent Visibility Specifier
OMR-03S	Minor	Yes	Inexistent Sanitization of Input Address
PMR-01S	Informational	Acknowledged	Literal Equality of `bool` Variable
PNF-01S	Informational	Acknowledged	Inexistent Event Emissions
PNF-02S	Informational	Acknowledged	Literal Equality of `bool` Variables
THR-01S	Informational	Nullified	Inexistent Visibility Specifiers
USD-01S	Informational	Acknowledged	Inexistent Event Emissions
USD-02S	Informational	Acknowledged	Inexistent Visibility Specifiers
USD-03S	Minor	Acknowledged	Inexistent Sanitization of Input Address

ID	Severity	Addressed	Title
WCE-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
WLG-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
WLG-02S	Minor	Yes	Deprecated Native Asset Transfers
WLD-01S	Informational	Acknowledged	Illegible Numeric Value Representation
WLD-02S	Informational	Partial	Inexistent Visibility Specifiers
WLD-03S	Minor	Yes	Inexistent Sanitization of Input Addresses
WLL-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
WOH-01S	Informational	Yes	Data Location Optimizations
WOH-02S	Informational	Acknowledged	Literal Equality of `bool` Variable
WSY-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
WSY-02S	Informational	Partial	Redundant Variable Assignments
WSD-01S	Informational	Yes	Illegible Numeric Value Representations
WSD-02S	Informational	Yes	Inexistent Visibility Specifiers
WSD-03S	Minor	Yes	Inexistent Sanitization of Input Address
WSH-01S	Informational	Acknowledged	Literal Equality of `bool` Variables
WSH-02S	Informational	Partial	Redundant Variable Assignments

Code Style

During the manual portion of the audit, we identified **60 optimizations** that can be applied to the codebase that will decrease the operational cost associated with the execution of a particular function and generally ensure that the project complies with the latest best practices and standards in Solidity.

Additionally, this section of the audit contains any opinionated adjustments we believe the code should make to make it more legible as well as truer to its purpose.

These optimizations are enumerated below:

ID	Severity	Addressed	Title
AHR-01C	Informational	Acknowledged	Ineffectual Usage of Safe Arithmetics
AHR-02C	Informational	Yes	Loop Iterator Optimizations
BNA-01C	Informational	Yes	Unclear Order of Operations
COR-01C	Informational	Yes	Redundant Return of Function
DFM-01C	Informational	Acknowledged	Non-Standard Revert Patterns
FMR-01C	Informational	Yes	Inefficient Iterator Data Types
FMR-02C	Informational	Yes	Inefficient Loop Limit Evaluations
FMR-03C	Informational	Acknowledged	Inefficient `mapping` Lookups
FMR-04C	Informational	Partial	Loop Iterator Optimizations
FMR-05C	Informational	Yes	Potentially Inefficient Array Shift Operation
FMH-01C	Informational	Yes	Ineffectual Usage of Safe Arithmetics

ID	Severity	Addressed	Title
FMH-02C	Informational	Acknowledged	Inefficient Integration of Internal Protocol
FMH-03C	Informational	Yes	Inefficient Loop Limit Evaluations
FMH-04C	Informational	Yes	Loop Iterator Optimizations
MHR-01C	Informational	Yes	Generic Typographic Mistake
MHR-02C	Informational	Yes	Ineffectual Usage of Safe Arithmetics
MHR-03C	Informational	Yes	Inefficient Iterator Data Type
MHR-04C	Informational	Yes	Loop Iterator Optimization
MHR-05C	Informational	Yes	Non-Uniform Invocation Style
MHR-06C	Informational	Acknowledged	Potentially Inefficient Array Shift Operation
MHR-07C	Informational	Partial	Weak Validation of Non-Zero Fees
OHR-01C	Informational	Yes	Ineffectual Usage of Safe Arithmetics
OHR-02C	Informational	Acknowledged	Inefficient Invocation of Chainlink Related Functions
OHR-03C	Informational	Acknowledged	Loop Iterator Optimization
OHR-04C	Informational	Yes	Non-Standard Error Style
OHR-05C	Informational	Yes	Non-Standard Revert Pattern
OHR-06C	Informational	Yes	Redundant Conditional Evaluation

ID	Severity	Addressed	Title
OHR-07C	Informational	Nullified	Unclear Order of Operations
OMR-01C	Informational	Acknowledged	Non-Standard Revert Patterns
PMR-01C	Informational	Yes	Generic Typographic Mistake
PMR-02C	Informational	Yes	Inefficient `mapping` Lookups
PMR-03C	Informational	Acknowledged	Repetitive Value Literals
PNF-01C	Informational	Yes	Loop Iterator Optimization
PNF-02C	Informational	Acknowledged	Non-Standard Caller Evaluation
PNF-03C	Informational	Yes	Unclear Order of Operations
USD-01C	Informational	Acknowledged	Variable Mutability Specifier (Immutable)
WCE-01C	Informational	Yes	Generic Typographic Mistakes
WCE-02C	Informational	Yes	Non-Uniform Invocation Style
WLG-01C	Informational	Yes	Ineffectual Usage of Safe Arithmetics
WLG-02C	Informational	Yes	Non-Uniform Invocation Style
WLD-01C	Informational	Yes	Generic Typographic Mistakes
WLL-01C	Informational	Acknowledged	Inefficient Conditional Structure
WLL-02C	Informational	Acknowledged	Inefficient `mapping` Lookups
WLL-03C	Informational	Acknowledged	Non-Standard Revert Patterns

ID	Severity	Addressed	Title
WOH-01C	Informational	Acknowledged	Ineffectual Usage of Safe Arithmetics
WOH-02C	Informational	Yes	Inefficient Iterator Data Types
WOH-03C	Informational	Yes	Loop Iterator Optimizations
WOH-04C	Informational	Nullified	Redundant Invocation of Constructor
WSY-01C	Informational	Partial	Generic Typographic Mistakes
WSY-02C	Informational	Partial	Ineffectual Usage of Safe Arithmetics
WSY-03C	Informational	Acknowledged	Inefficient `mapping` Lookups
WSY-04C	Informational	Yes	Loop Iterator Optimizations
WSY-05C	Informational	Acknowledged	Non-Standard Revert Pattern
WSY-06C	Informational	Yes	Non-Uniform Invocation Style
WSD-01C	Informational	Acknowledged	Repetitive Value Literal
WSH-01C	Informational	Yes	Generic Typographic Mistake
WSH-02C	Informational	Yes	Inefficient Code Structure
WSH-03C	Informational	Yes	Inefficient Loop Limit Evaluations
WSH-04C	Informational	Yes	Loop Iterator Optimizations
WSH-05C	Informational	Acknowledged	Non-Standard Revert Patterns

Manual Review

A **thorough line-by-line review** was conducted on the codebase to identify potential malfunctions and vulnerabilities in Wise's ecosystem sub-set.

As the project at hand implements a wide array of DeFi modules inclusive of lending / borrowing systems, intricate care was put into ensuring that the **flow of funds & assets within the system conforms to the specifications and restrictions** laid forth within the protocol's specification.

We validated that **all state transitions of the system occur within sane criteria** and that all rudimentary formulas within the system execute as expected. We **pinpointed multiple significant vulnerabilities** within the system which could have had **severe ramifications** to its overall operation; we urge the Wise team to promptly evaluate and remediate these vulnerabilities.

Additionally, the system was investigated for any other commonly present attack vectors such as re-entrancy attacks, mathematical truncations, logical flaws and **ERC / EIP** standard inconsistencies. The documentation of the project was satisfactory to a certain extent, however, we strongly recommend it to be expanded at certain complex points such as the intricate calculations in relation to the interest stepping algorithm which do not closely correlate with the `LASA` system's whitepaper definition.

A total of **83 findings** were identified over the course of the manual review of which **23 findings** concerned the behaviour and security of the system. The non-security related findings, such as optimizations, are included in the separate **Code Style** chapter.

The finding table below enumerates all these security / behavioural findings:

ID	Severity	Addressed	Title
AHB-01M	Informational	Acknowledged	Discrepant Behaviour of Paybacks
DSI-01M	Unknown	Yes	Inexplicable Capability of Reconfiguration
DFM-01M	Unknown	Acknowledged	Inexplicable Address Literals
DFM-02M	Medium	Yes	Insecure Assumption of NFT Acquisition
FMR-01M	Medium	Acknowledged	Inexistent Accommodation of Inexistent

ID	Severity	Addressed	Title
			Incentives
FMR-02M	Medium	Yes	Unsafe Incentive Owner Adjustment
MHR-01M	Major	Yes	Incorrect Early Return
OHR-01M	Informational	Yes	Misleading Function Name
OHR-02M	Medium	Yes	Incorrect Assessment of Latest Update Delta
OHR-03M	Medium	Yes	Incorrect Iteration Count Limitation
OHR-04M	Medium	Yes	Misconception of Chainlink Round IDs
OHR-05M	Medium	Acknowledged	Potentially Abnormally Low Heartbeat
PNF-01M	Unknown	Yes	Re-Entrant Creation of Positions
PNF-02M	Minor	Yes	Non-Standard Override of Default EIP-721 Functionality
PNF-03M	Minor	Yes	Potentially Insecure Position Creation Workflow
PNF-04M	Minor	Yes	Potentially Insecure Position Reservation Workflow
PNF-05M	Medium	Acknowledged	EIP-721 Deviation of Approval
PNF-06M	Major	Yes	Discrepancy in Zero ID Management
WLD-01M	Unknown	Yes	Inexplicable Capability of Reconfiguration
WLD-02M	Medium	Yes	Insecure Assumption of NFT Acquisition
WOH-01M	Medium	Yes	Improper Integration of Chainlink Oracles

ID	Severity	Addressed	Title
WSY-01M	Major	Yes	Incorrect Curve Pool Query
WSH-01M	Major	Yes	Incorrect Validation of Reservation

Compilation

The project is composed of barebones contracts without the utilization of a framework, however, a framework is most likely utilized to develop the system due to its sheer size.

All `pragma` versions within the project have been locked to `0.8.23`, the same version we utilized during our static analysis and code style evaluation of the codebase.

Post-Audit Conclusion

The Wise team iterated through all findings within the report and provided us with a revised commit hash to evaluate all exhibits on.

Severity	Identified	Alleviated	Partially Alleviated	Acknowledged
Unknown	4	3	0	1
Informational	98	50	12	36
Minor	12	11	0	1
Medium	10	7	0	3
Major	4	4	0	0

During the audit, we filtered and validated a total of **45 findings utilizing static analysis** tools as well as identified a total of **83 findings during the manual review** of the codebase. All the following non-critical exhibits have been fullly or partially alleviated.