SMART CONTRACT AUDIT REPORT

for

Roe Finance

Prepared By: Xiaomi Huang

PeckShield

September 18, 2022

Document Properties

Client	Roe Finance
Title	Smart Contract Audit Report
Target	Roe Finance
Version	1.0
Author	Shulin Bie
Auditors	Shulin Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	September 18, 2022	Shulin Bie	Final Release
1.0-rc	September 16, 2022	Shulin Bie	Release Candidate

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction **4**

1.1 About Roe Finance 4

1.2 About PeckShield 5

1.3 Methodology 5

1.4 Disclaimer 7

2 Findings **9**

2.1 Summary 9

2.2 Key Findings 10

3 Detailed Results **11**

3.1 Incompatibility with Deflationary/Rebasing Tokens 11

3.2 Fork-Compliant Domain Separator in AToken 13

3.3 Flashloan-assisted Lowered StableBorrowRate for Mode-Switching Users 15

3.4 Trust Issue of Admin Keys 17

4 Conclusion **19**

References **20**

1 | Introduction

Given the opportunity to review the design document and related smart contract source code of the `Roe Finance` protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About Roe Finance

`Roe Finance` is a decentralized non-custodial liquidity markets protocol that is developed on top of one of the largest DeFi protocols, i.e., `AAVE`. It builds upon the biggest derivative opportunity embedded in `Uniswap` and aims to solve the impermanent loss for liquidity providers. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of Roe Finance

Item	Description
Target	Roe Finance
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	September 18, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Note that the `Roe Finance` protocol assumes a trusted price oracle with timely market price feeds for supported assets and the oracle itself is not part of this audit. Additionally, in this audit, `LendingPool.sol.0x2` is used as `LendingPool` contract.

- https://github.com/RoeFinance/RoeMarkets.git (7a6eeda)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/RoeFinance/RoeMarkets.git (a933ee6)

1.2 About PeckShield

PeckShield Inc. [8] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

Likelihood

1.3 Methodology

To standardize the evaluation, we define the following terminology based on OWASP Risk Rating Methodology [7]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

To evaluate the risk, we go through a list of check items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the

Table 1.3: The Full List of Check Items

Category	Check Item
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [6], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logics	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the `Roe Finance` implementation. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logic, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	2	■ ■
Low	2	■ ■
Informational	0	
Total	4	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities that need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 2 medium-severity vulnerabilities and 2 low-severity vulnerabilities.

Table 2.1: Key Roe Finance Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Incompatibility with Deflationary/Rebasing Tokens	Business Logic	Confirmed
PVE-002	Low	Fork-Compliant Domain Separator in AToken	Business Logic	Confirmed
PVE-003	Medium	Flashloan-assisted Lowered StableBorrowRate for Mode-Switching Users	Time and State	Confirmed
PVE-004	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Incompatibility with Deflationary/Rebasing Tokens

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `LendingPool`
- Category: Business Logic [5]
- CWE subcategory: CWE-841 [3]

Description

In the `Roe Finance` protocol, the `LendingPool` contract is designed to be the main entry for interaction with borrowing/lending users. In particular, one entry routine, i.e., `deposit()`, accepts asset transfer-in and mints the corresponding `AToken` to represent the depositor's share in the lending pool. Naturally, the contract implements a number of low-level helper routines to transfer assets into or out of the protocol. These asset-transferring routines work as expected with standard ERC20 tokens: namely the vault's internal asset balances are always consistent with actual token balances maintained in individual ERC20 token contract.

```
  function deposit(
    address asset,
    uint256 amount,
    address onBehalfOf,
    uint16 referralCode
  ) external override whenNotPaused {
      DataTypes.ReserveData storage reserve = _reserves[asset];

      ValidationLogic.validateDeposit(reserve, amount);

      address aToken = reserve.aTokenAddress;

      reserve.updateState();
      reserve.updateInterestRates(asset, aToken, amount, 0);

      IERC20(asset).safeTransferFrom(msg.sender, aToken, amount);
```

```

        bool isFirstDeposit = IAToken(aToken).mint(onBehalfOf, amount, reserve.liquidityIndex);

        if (isFirstDeposit) {
            _usersConfig[onBehalfOf].setUsingAsCollateral(reserve.id, true);
            emit ReserveUsedAsCollateralEnabled(asset, onBehalfOf);
        }

        emit Deposit(asset, msg.sender, onBehalfOf, amount, referralCode);
    }
```

Listing 3.1: `LendingPool::deposit()`

However, there exist other ERC20 tokens that may make certain customizations to their ERC20 contracts. One type of these tokens is deflationary tokens that charge a certain fee for every `transfer()` or `transferFrom()`. (Another type is rebasing tokens such as `YAM`.) As a result, this may not meet the assumption behind these low-level asset-transferring routines. In other words, the above operations, such as `deposit()`, may introduce unexpected balance inconsistencies when comparing internal asset records with external ERC20 token contracts.

One possible mitigation is to measure the asset change right before and after the asset-transferring routines. In other words, instead of expecting the amount parameter in `transfer()` or `transferFrom()` will always result in full transfer, we need to ensure the increased or decreased amount in the pool before and after the `transfer()` or `transferFrom()` is expected and aligned well with our operation. Though these additional checks cost additional gas usage, we consider they are necessary to deal with deflationary tokens or other customized ones if their support is deemed necessary.

Another mitigation is to regulate the set of ERC20 tokens that are permitted into `Roe Finance`. In `Roe Finance` protocol, it is indeed possible to effectively regulate the set of tokens that can be supported. Keep in mind that there exist certain assets (e.g., `USDT`) that may have control switches that can be dynamically exercised to suddenly become one.

Recommendation If current codebase needs to support deflationary tokens, it is necessary to check the balance before and after the `transfer()`/`transferFrom()` call to ensure the book-keeping amount is accurate. This support may bring additional gas cost. Also, keep in mind that certain tokens may not be deflationary for the time being. However, they could have a control switch that can be exercised to turn them into deflationary tokens. One example is the widely-adopted `USDT`.

Status This issue has been confirmed by the team.

3.2 Fork-Compliant Domain Separator in AToken

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: High
- Target: AToken
- Category: Business Logic [5]
- CWE subcategory: CWE-841 [3]

Description

The AToken token contract strictly follows the widely-accepted ERC20 specification. In the meantime, we notice the support of EIP-2612 with the permit() function that allows for approvals to be made via secp256k1 signatures. Interestingly, we notice the state variable DOMAIN_SEPARATOR is initialized once inside the initialize() function (lines 81-89).

```
64      function initialize(
65          ILendingPool pool,
66          address treasury,
67          address underlyingAsset,
68          IAaveIncentivesController incentivesController,
69          uint8 aTokenDecimals,
70          string calldata aTokenName,
71          string calldata aTokenSymbol,
72          bytes calldata params
73      ) external override initializer {
74          uint256 chainId;
75
76          //solium-disable-next-line
77          assembly {
78              chainId := chainid()
79          }
80
81          DOMAIN_SEPARATOR = keccak256(
82              abi.encode(
83                  EIP712_DOMAIN,
84                  keccak256(bytes(aTokenName)),
85                  keccak256(EIP712_REVISION),
86                  chainId,
87                  address(this)
88              )
89          );
90
91          ...
92    }
```

Listing 3.2: AToken::initialize()

The DOMAIN_SEPARATOR is used in the permit() function and should be unique to the contract and chain in order to prevent replay attacks from other domains. However, when analyzing this permit() routine, we realize the current implementation needs to be improved by recalculating the value of DOMAIN_SEPARATOR inside the permit() function, for the very purpose of preventing cross-chain replay attacks. Specifically, when there is a chain-level hard-fork, because of the pre-computed DOMAIN_SEPARATOR, a valid signature for one chain could be replayed on the other.

```
    function permit(
        address owner,
        address spender,
        uint256 value,
        uint256 deadline,
        uint8 v,
        bytes32 r,
        bytes32 s
    ) external {
        require(owner != address(0), 'INVALID_OWNER');
        //solium-disable-next-line
        require(block.timestamp <= deadline, 'INVALID_EXPIRATION');
        uint256 currentValidNonce = _nonces[owner];
        bytes32 digest =
        keccak256(
            abi.encodePacked(
            '\x19\x01',
            DOMAIN_SEPARATOR,
            keccak256(abi.encode(PERMIT_TYPEHASH, owner, spender, value,
                currentValidNonce, deadline))
            )
        );
        require(owner == ecrecover(digest, v, r, s), 'INVALID_SIGNATURE');
        _nonces[owner] = currentValidNonce.add(1);
        _approve(owner, spender, value);
    }
```

Listing 3.3: AToken::permit()

Recommendation Recalculate the value of DOMAIN_SEPARATOR inside the permit() function.

Status The issue has been confirmed by the team.

3.3 Flashloan-assisted Lowered StableBorrowRate for Mode-Switching Users

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `LendingPool`
- Category: Business Logic [5]
- CWE subcategory: CWE-837 [2]

Description

By design, the `Roe Finance` protocol supports both variable and stable borrow rates. The variable borrow rate follows closely the market dynamics and can be changed on each user interaction (either borrow, deposit, withdraw, repayment or liquidation). The stable borrow rate instead will be unaffected by these actions. However, implementing a fixed stable borrow rate model on top of a dynamic reserve pool is complicated and the protocol provides the rate-rebalancing support to work around dynamic changes in market conditions or increased cost of money within the pool.

In the following, we show the code snippet of `swapBorrowRateMode()` which allows users to swap between stable and variable borrow rate modes. It follows the same sequence of convention by firstly validating the inputs (Step I), secondly updating relevant reserve states (Step II), then switching the requested borrow rates (Step III), next calculating the latest interest rates (Step IV), and finally performing external interactions, if any (Step V).

```
    function swapBorrowRateMode(address asset, uint256 rateMode) external override whenNotPaused {
        DataTypes.ReserveData storage reserve = _reserves[asset];

        (uint256 stableDebt, uint256 variableDebt) = Helpers.getUserCurrentDebt(msg.sender, reserve);

        DataTypes.InterestRateMode interestRateMode = DataTypes.InterestRateMode(rateMode);

        ValidationLogic.validateSwapRateMode(
            reserve,
            _usersConfig[msg.sender],
            stableDebt,
            variableDebt,
            interestRateMode
        );

        reserve.updateState();

        if (interestRateMode == DataTypes.InterestRateMode.STABLE) {
```

```
            IStableDebtToken(reserve.stableDebtTokenAddress).burn(msg.sender, stableDebt);
            IVariableDebtToken(reserve.variableDebtTokenAddress).mint(
                msg.sender,
                msg.sender,
                stableDebt,
                reserve.variableBorrowIndex
            );
        } else {
            IVariableDebtToken(reserve.variableDebtTokenAddress).burn(
                msg.sender,
                variableDebt,
                reserve.variableBorrowIndex
            );
            IStableDebtToken(reserve.stableDebtTokenAddress).mint(
                msg.sender,
                msg.sender,
                variableDebt,
                reserve.currentStableBorrowRate
            );
        }

        reserve.updateInterestRates(asset, reserve.aTokenAddress, 0, 0);

        emit Swap(asset, msg.sender, rateMode);
    }
```

Listing 3.4: `LendingPool::swapBorrowRateMode()`

Our analysis shows this `swapBorrowRateMode()` routine can be affected by a flashloan-assisted sandwiching attack such that the new stable borrow rate becomes the lowest possible. Note this attack is applicable when the borrow rate is switched from variable to stable rate. Specifically, to perform the attack, a malicious actor can first request a flashloan to deposit into the reserve pool so that the reserve's utilization rate is close to 0, then invoke `swapBorrowRateMode()` to perform the variable-to-borrow rate switch and enjoy the lowest `currentStableBorrowRate` (thanks to the nearly 0 utilization rate in current reserve), and finally withdraw to return the flashloan. A similar approach can also be applied to bypass `maxStableLoanPercent` enforcement in `validateBorrow()`.

Recommendation Revise the current implementation to defensively detect sudden changes to a reserve utilization and block malicious attempts.

Status This issue has been confirmed be the team. The team does not plan to support `stable borrow rate` mode.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [1]

Description

In the `Roe Finance` protocol, there is a privileged `owner` account that plays a critical role in governing and regulating the system-wide operations (e.g., parameter setting and price oracle adjustment). Our analysis shows that the privileged account needs to be scrutinized. In the following, we examine the privileged account and the related privileged accesses in current contracts.

```
    function setAssetSources(address[] calldata assets, address[] calldata sources)
    external
    onlyOwner
    {
        _setAssetsSources(assets, sources);
    }

    function setFallbackOracle(address fallbackOracle) external onlyOwner {
        _setFallbackOracle(fallbackOracle);
    }
```

Listing 3.5: `AaveOracle`

Moreover, the `LendingPoolAddressesProvider` contract allows the privileged `owner` to configure protocol-wide contracts, including `LENDING_POOL`, `LENDING_POOL_CONFIGURATOR`, `POOL_ADMIN`, `EMERGENCY_ADMIN`, `LENDING_POOL_COLLATERAL_MANAGER`, `PRICE_ORACLE`, and `LENDING_RATE_ORACLE`. These contracts play a variety of duties and are also considered privileged.

```
    contract LendingPoolAddressesProvider is Ownable, ILendingPoolAddressesProvider {
        string private _marketId;
        mapping(bytes32 => address) private _addresses;

        bytes32 private constant LENDING_POOL = 'LENDING_POOL';
        bytes32 private constant LENDING_POOL_CONFIGURATOR = 'LENDING_POOL_CONFIGURATOR'
            ;
        bytes32 private constant POOL_ADMIN = 'POOL_ADMIN';
        bytes32 private constant EMERGENCY_ADMIN = 'EMERGENCY_ADMIN';
        bytes32 private constant LENDING_POOL_COLLATERAL_MANAGER = 'COLLATERAL_MANAGER';
        bytes32 private constant PRICE_ORACLE = 'PRICE_ORACLE';
        bytes32 private constant LENDING_RATE_ORACLE = 'LENDING_RATE_ORACLE';
        ...
    }
```

Listing 3.6: `LendingPoolAddressesProvider`

We emphasize that the privilege assignment may be necessary and consistent with the protocol design. However, it is worrisome if the privileged account is not governed by a `DAO`-like structure. Note that a compromised account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

Recommendation Promptly transfer the privileged account to the intended `DAO`-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been confirmed with the team. For the time being, it is planned to mitigate with a 2-day timelock to balance efficiency and timely adjustment.

4 Conclusion

In this audit, we have analyzed the Roe Finance design and implementation. Roe Finance is a decentralized non-custodial liquidity markets protocol that is developed on top of one of the largest DeFi protocols, i.e., AAVE. It builds upon the biggest derivative opportunity embedded in Uniswap and aims to solve the impermanent loss for liquidity providers. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

References

[1] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[2] MITRE. CWE-837: Improper Enforcement of a Single, Unique Action. https://cwe.mitre.org/data/definitions/837.html.

[3] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[4] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[5] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[6] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[7] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[8] PeckShield. PeckShield Inc. https://www.peckshield.com.