Assure DeFi®

THE VERIFICATION **GOLD STANDARD**

VERIFIED BY ASSURE DEFI ® INTEGRITY ✦ TRUST ✦ CREDIBILITY

Security Assessment

opTradeAI

Date: 02/03/2025

Audit Status: PASS

Audit Edition: Standard

ASSURE DEFI®

THE VERIFICATION **GOLD STANDARD**

Risk Analysis

Vulnerability summary

Classification	Description
🔴 High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
🟠 Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
🟡 Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
🟢 Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Secured.**

Insecure	**Poorly Secured**	**Secured**	**Well Secured**

Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the opTradeAI contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	https://etherscan.io/address/0x72b658Bd674f9c2B4954682f517c17D14476e417#code
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	● Compiler warnings. ● Race conditions and Reentrancy. Cross-function race conditions. ● Possible delays in data delivery. ● Oracle calls. ● Front running. ● Timestamp dependence. ● Integer Overflow and Underflow. ● DoS with Revert. ● DoS with block gas limit. ● Methods execution permissions. ● Economy model. ● Private user data leaks. ● Malicious Event log. ● Scoping and Declarations. ● Uninitialized storage pointers. ● Arithmetic accuracy. ● Design Logic. ● Cross-function race conditions. ● Safe Zeppelin module. ● Fallback function security. ● Overpowered functions / Owner privileges

AUDIT OVERVIEW

HIGH

No high severity issues were found.

MEDIUM

1. Division by Zero in Transfer Fee Calculation

Issue: Fee distribution for transfers uses sell fee ratios. If fees are removed via RemoveAllFees() while transferFee remains non-zero, this causes a division by zero resulting in an immediate revert, effectively causing a DOS on token transfers.

Recommendation: Set transferFee to zero when removing fees or add explicit checks to prevent division by zero in the fee distribution logic.

2. Centralization and Owner Privileges

Issue: The owner has extensive control over fee settings, trading activation, wallet updates, and transaction limits, creating a centralization risk if abused or compromised.

Recommendation: Introduce multi-signature governance, time-locks, or decentralized control mechanisms. Clearly document owner privileges and consider transitioning to a more decentralized admin model.

3. Inconsistent Fee Distribution for Transfers

Issue: Transfer fees are calculated using transferFee but distributed using sell fee ratios. This could lead to unintended fee allocation if fee parameters are adjusted independently.

Recommendation: Review and separate transfer fee parameters from sell fees, or clearly document the intended behavior to avoid confusion and ensure tokenomics align with design expectations.

LOW

1. Low-Level External Calls without Full Reversion

Issue: ETH transfers via low-level .call to external wallets (marketing and development) do not enforce reversion on failure. This might result in funds remaining in the contract if the call fails.

Recommendation: Check the success flags and either revert on failure or emit events for manual intervention. Alternatively, ensure the wallet addresses are EOAs to reduce potential issues with contract fallback functions.

2. Use of 0 Minimum Output in Swap Function

Issue: The swap function sets amountOutMin to 0, exposing the swap to potential front-running and adverse price impacts under volatile market conditions.

Recommendation: Consider implementing a minimum output threshold for swaps to mitigate risks from price slippage and front-running, especially during periods of high volatility.

INFORMATIONAL

1. Unused State Variables and Redundancies

Issue: An unused mapping (_holderLastTransferTimestamp) and redundant use of SafeMath (given Solidity 0.8+ includes built-in overflow checks) may indicate incomplete features or code clutter.

Recommendation: Remove unused variables and unnecessary SafeMath usage to improve code clarity, gas efficiency, and maintainability.

Technical Findings Summary

Findings

Vulnerability Level	Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
🔴 High	0					
🟠 Medium	3					
🟡 Low	2					
🟢 Informational	1					

Assessment Results

Score Results

Review	Score
Global Score	**85/100**
Assure KYC	Not completed
Audit Score	85/100

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the opTradeAI project, the project did meet the necessary criteria required to pass the security audit.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocating for the Project, and users relying on this report should not consider this as having any merit for financial opTradeAI in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment opTradeAI, nor should it be used to signal that any person reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audit completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment opTradeAIs provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any opTradeAIs, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The opTradeAIs may access, and depend upon, multiple layers of third parties.