

RITA AI Smart Contract Auditor

Unknown

0xCa127b33F6e606660D8AbA486A4b167fEd4b5612

Detailed Security Audit

Critical Functions Check

Issue Description	Checking Status
Compiler errors	Passed
Race conditions and Reentrancy, Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
Timestamp dependence	Passed
Integer Overflow and Underflow	Low Risk
Dos with Revert	Low Risk
Dos with block gas limit	Passed
Methods execution permissions	Passed
Economy model of the contract	High Risk
The impact of the exchange rate on the logic	Passed
Private user data leaks	Passed
Malicious Event log	Passed
Scoping and Declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Low Risk
Design Logic	Passed
Cross-function race conditions	Passed
Safe Open Zeppelin contracts implementation and usage	Passed
Fallback function security	Passed
Unsafe delegatecall usage	Passed
Unrestricted public functions	Passed
Potential infinite loops	Low Risk
High gas consumption operations	Passed
Unsafe send/transfer usage	Low Risk

Risky Functions Details

Function: economy

Critical economy model issue with fees (tax, liquidity, charity) detected, may lead to unexpected behavior or exploitation

Function: loops

Potential infinite loops detected, risking contract freezing or high gas costs

Function: send/transfer

Potential unsafe send/transfer usage detected, risking reentrancy or fund loss



This audit was conducted and prepared by RITA AI