OXSCANS

AI Generated at 06:44 PM, UTC

February 29, 2024

OVERVIEW

This audit has been perpared for '' to review the main aspects of the project to help investors make an informative decision during their research process

You will find a summarized review of the following key points:

- Contract's source code
- Owner wallets
- Tokenomics
- Team transparency and goals
- Website's age, code, security and UX
- Whitepaper and roadmap
- Social media and online presence

Table of Content

General Information

Name ◌

Info

General Information

Tokenomics

Contract Address	0xcda954A0C574d8C408F0b8c89a2B367d6A2D3354

General Analysis

Audit Review Process

1. Testing the smart contracts against both common and uncommon vulnerabilities
2. Assessing the codebase to ensure compliance with current best practices and industry standards
3. Ensuring contract logic meets the specifications and intentions of the client
4. Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
5. Thorough line-byline AI review of the entire codebase by industry

Token Transfer Stats

Transactions (Latest Mine Block)	Token holders	Compiler
1	0	v0.8.19

Smart Contract Stats

Functions	Events	Constructor
7	2	1

Detail Analysis

Threat Level

🔴 High	Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment
🟠 Medium	Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment
🟡 Low	Issues on this level are minor details and warning that can remain unfixed
🔵 Informational	Informational level is to offer suggestions for improvement of efficacy or secruity for fratures with risk free factor

Threat Level

🔴 High	2 threats found
🟠 Medium	0 threats found
🟡 Low	0 threats found
🔵 Informational	0 threats found

Detail Analysis

Vulnerability Check 🟢 19 Passed 🔴 2 Fail

🟢 Arbitrary Jump/Storage Write 🔴 Centralization of Control

🟢 Compiler Issues 🟢 Delegate Call to Untrusted Contract

🟢 Dependence on Predictable Variables 🟢 Ether/Token Theft

🟢 Flash Loans 🟢 Front Running 🟢 Improper Events

🔴 Improper Authorization Scheme 🟢 Integer Over/Underflow

🟢 Logical Issues 🟢 Oracle Issues 🟢 Outdated Compiler Version

🟢 Race Conditions 🟢 Reentrancy 🟢 Signature Issues 🟢 Sybil Attack

🟢 Unbounded Loops 🟢 Unused Code 🟢 Overall Contract Safety

Detail Analysis

Detail Analysis

🟢 19 Passed 🔴 2 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write	🟢	The contract does not employ low-level calls or assembly code that could lead to arbitrary jumps or storage writes.
Centralization of Control	🔴	The contract has a single point of control, as there is an owner role that has the authority to upgrade the contract and set maintenance mode.
Compiler Issues	🟢	Contract is compiled with a recent Solidity version (0.8.19), minimizing known compiler issues.
Delegate Call to Untrusted Contract	🟢	The contract does not appear to make delegate calls to untrusted contracts.
Dependence on Predictable Variables	🟢	There are no clear dependencies on predictable variables like block.timestamp or block.number.

Detail Analysis

Detail Analysis

🟢 19 Passed 🔴 2 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft	🟢	The contract does not contain functions that could lead to Ether or token theft.
Flash Loans	🟢	The contract does not interact with flash loan mechanisms.
Front Running	🟢	There are no functions exposed that could be vulnerable to front running.
Improper Events	🟢	All events are properly declared and emitted.
Improper Authorization Scheme	🔴	The contract uses a simple ownership model for critical functionality, which could be an improper authorization scheme if not managed correctly.
Integer Over/Underflow	🟢	The contract is using Solidity 0.8.x which has built-in overflow/underflow checks.

Detail Analysis

Detail Analysis

🟢 19 Passed 🔴 2 Fail

CATEGORY	STATUS	NOTES
Logical Issues	🟢	No logical issues detected within the contract's scope.
Oracle Issues	🟢	The contract does not use external data feeds or oracles.
Outdated Compiler Version	🟢	Compiled with a recent compiler version, avoiding issues with outdated compilers.
Race Conditions	🟢	No functions with race condition vulnerabilities identified.
Reentrancy	🟢	The contract's functions that could potentially be vulnerable to reentrancy are protected by the onlyProxyOwner modifier.
Signature Issues	🟢	The contract does not involve signature verification processes.

Detail Analysis

Detail Analysis

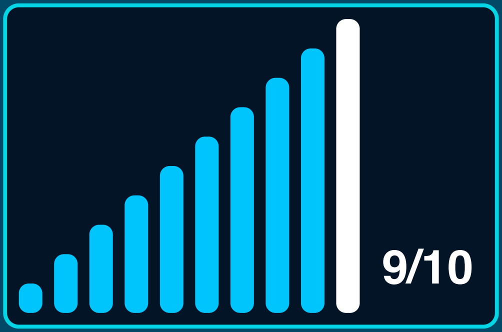
🟢 19 Passed 🔴 2 Fail

CATEGORY	STATUS	NOTES
Sybil Attack	🟢	Sybil attack vectors are not applicable to this contract's functionality.
Unbounded Loops	🟢	No unbounded loops that could lead to gas limit issues.
Unused Code	🟢	No signs of significant unused code or functions.
Overall Contract Safety	🟢	Overall, the contract follows good safety practices and patterns.

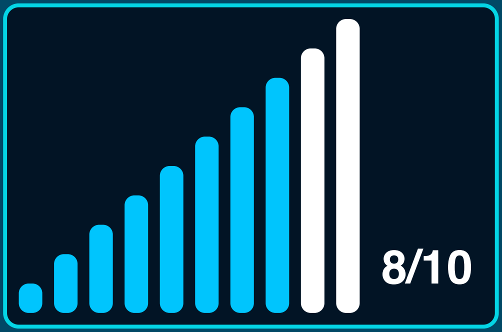
Market Analysis

Score

Total Audit Score



Security Score



Legal Disclaimer

0xscans operates as an automated system for smart contract due diligence, acknowledging the possibility of bugs or vulnerabilities impacting token values. We do not hold specific obligations regarding your trading outcomes or the utilization of audit content. Users release 0xscans from any liability associated with content obtained through the tool.

AI generated by 0xscans AI technology

Chat with us

Telegram

For more information. Visit below:

Twitter

Github