OXSCANS

Mine AI

AI Generated at 01:06 AM, UTC

March 06, 2024

OVERVIEW

This audit has been perpared for 'Mine AI' 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

Mine AI

Name **Mine AI**

Info

General Information

Tokenomics

Contract Address 0xf4aaa9428a881a5c054d0ed041f5749a336c9ab5

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	702	v0.8.19

Smart Contract Stats

Functions	Events	Constructor
26	3	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	**0** threats found
Medium	**0** threats found
Low	**0** threats found
Informational	**0** threats found

Detail Analysis

Vulnerability Check

21 Passed

0 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- Outdated Compiler Version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

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		The contract does not contain low-level calls or assembly code that could lead to arbitrary jumps or storage writes.
Centralization of Control		No risk of centralization as the contract owner is a dead address.
Compiler Issues		The contract is compiled with a recent version of the Solidity compiler (v0.8.19).
Delegate Call to Untrusted Contract		The contract does not use delegatecall.
Dependence on Predictable Variables		No critical functionality depends on predictable variables like block.timestamp or block.number.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft		The contract adheres to the ERC20 standard and does not have functions that could lead to Ether or token theft.
Flash Loans		The contract does not interact with flash loans.
Front Running		While ERC20 transfers can be front-run, the contract itself does not contain functionality that exacerbates this issue.
Improper Events		All external and state-changing functions emit appropriate events.
Improper Authorization Scheme		Authorization is properly managed; only the owner has access to critical functions, and the owner is a dead address.
Integer Over/Underflow		SafeMath library is used to prevent overflows and underflows.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Logical Issues		No logical issues or inconsistencies were found upon review.
Oracle Issues		The contract does not use external oracles.
Outdated Compiler Version		Compiler version is recent and appropriate for the contract.
Race Conditions		No functions are susceptible to race conditions.
Reentrancy		The contract functions are not vulnerable to reentrancy attacks.
Signature Issues		The contract does not use message signatures.

Detail Analysis

Detail Analysis

21 Passed

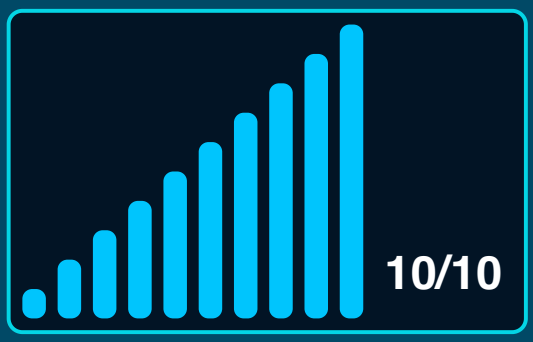
0 Fail

CATEGORY	STATUS	NOTES
Sybil Attack		The contract is not vulnerable to Sybil attacks as it does not rely on node or user reputation.
Unbounded Loops		No functions with unbounded loops that could lead to gas limit issues.
Unused Code		No significant amount of unused code present in the contract.
Overall Contract Safety		The contract adheres to best practices and is safe against known vulnerabilities as per the current analysis.

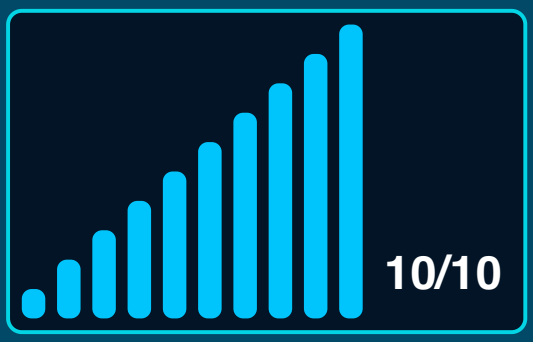
Market Analysis

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