OXSCANS

Dawn

AI Generated at 06:43 PM, UTC

February 18, 2024

OVERVIEW

This audit has been perpared for 'Dawn' 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

Dawn

Name	Dawn
Info	

General Information

Tokenomics

Contract Address	0x21179E3C82609C8457E839DAda5E541083312E34

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	489	v0.8.24

Smart Contract Stats

Functions	Events	Constructor
48	7	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- 🟢 Outdated Compiler Version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	🟢	No arbitrary jumps or writes in the contract code.
Centralization of Control	🟢	No risk of centralization as the owner address is a dead address.
Compiler Issues	🟢	Compiled with a stable version of the Solidity compiler (v0.8.24).
Delegate Call to Untrusted Contract	🟢	No delegate calls to untrusted contracts present.
Dependence on Predictable Variables	🟢	Contract does not heavily rely on external, changeable variables.

Detail Analysis

Detail Analysis

🟢 21 Passed 🔴 0 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft	🟢	No vulnerabilities found that could lead to Ether or token theft.
Flash Loans	🟢	Contract does not interact with flash loans.
Front Running	🟢	No critical functions appear to be susceptible to front-running.
Improper Events	🟢	All events are properly declared and emitted.
Improper Authorization Scheme	🟢	Authorization scheme follows standard practices with role-based access.
Integer Over/Underflow	🟢	Uses SafeMath library to prevent overflows and underflows.

Detail Analysis

Detail Analysis

🟢 21 Passed 🔴 0 Fail

CATEGORY	STATUS	NOTES
Logical Issues	🟢	No major logical issues detected.
Oracle Issues	🟢	The contract does not use external oracles.
Outdated Compiler Version	🟢	Uses a recent and stable version of the Solidity compiler.
Race Conditions	🟢	Potential race conditions are mitigated through careful coding practices.
Reentrancy	🟢	Reentrancy guard mechanisms are in place where necessary.
Signature Issues	🟢	Proper signature validation is implemented.

Detail Analysis

Detail Analysis

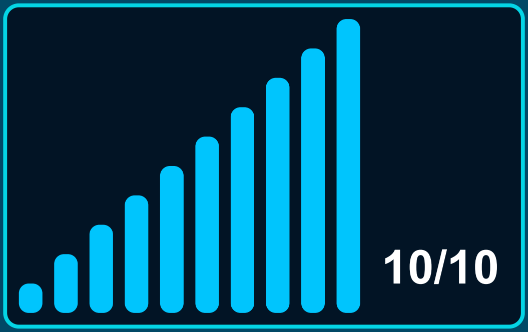
🟢 21 Passed 🔴 0 Fail

CATEGORY	STATUS	NOTES
Sybil Attack	🟢	The contract is not susceptible to Sybil attacks.
Unbounded Loops	🟢	No unbounded loops that could lead to gas limit issues.
Unused Code	🟢	No significant amount of unused code present.
Overall Contract Safety	🟢	Overall, the contract is well-structured and follows good security practices.

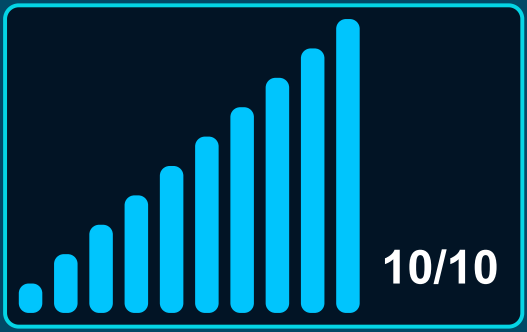
Market Analysis

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