OXSCANS

Etherscape

AI Generated at 07:33 PM, UTC

February 20, 2024

OVERVIEW

This audit has been perpared for 'Etherscape' 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

Etherscape

Name	Etherscape
Info	

General Information

Tokenomics

Contract Address	0x6c6e2c5a4eb108a1f3c985d5a7f4f233483e952f

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	330	v0.8.20

Smart Contract Stats

Functions	Events	Constructor
58	10	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	**5** threats found
● Medium	**0** threats found
● Low	**0** threats found
● Informational	**0** threats found

Detail Analysis

Vulnerability Check

🟢 16 Passed 🔴 5 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- 🟢 Outdated Compiler Version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

🟢 16 Passed 🔴 5 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write	🟢	The contract does not contain operations that would allow for 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 using a recent compiler version without known issues.
Delegate Call to Untrusted Contract	🟢	The contract does not use delegate calls, reducing the risk associated with untrusted contract interactions.
Dependence on Predictable Variables	🟢	No critical dependency on predictable variables like block.timestamp or block.number was found.

Detail Analysis

Detail Analysis

🟢 16 Passed 🔴 5 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft	🟢	The contract adheres to the ERC20 standard and does not have direct mechanisms to handle Ether, minimizing the risk of Ether/token theft.
Flash Loans	🟢	The contract does not interact with flash loan functionalities.
Front Running	🔴	Token transfer functions may be susceptible to front-running.
Improper Events	🟢	All events, including token transfer, mint, and approval, are properly implemented.
Improper Authorization Scheme	🔴	The contract includes functions that can only be executed by the owner, which could lead to an improper authorization scheme.
Integer Over/Underflow	🟢	The contract uses SafeMath to prevent integer overflows and underflows.

Detail Analysis

Detail Analysis 🟢 16 Passed 🔴 5 Fail

CATEGORY	STATUS	NOTES
Logical Issues	🔴	The contract's logic could be improved to prevent potential logical issues.
Oracle Issues	🟢	The contract does not use external oracles.
Outdated Compiler Version	🟢	The contract is compiled with a recent version of the Solidity compiler.
Race Conditions	🔴	The contract's functionalities, like token minting, may introduce race conditions.
Reentrancy	🟢	No functions were identified that could be vulnerable to reentrancy attacks.
Signature Issues	🟢	No complex signature operations that could introduce vulnerabilities were found.

Detail Analysis

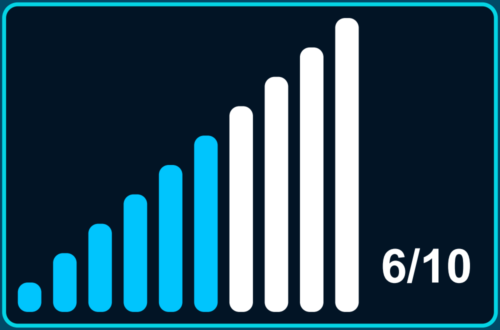
Detail Analysis 🟢 16 Passed 🔴 5 Fail

CATEGORY	STATUS	NOTES
Sybil Attack	🟢	The contract's structure does not facilitate Sybil attacks.
Unbounded Loops	🟢	No unbounded loops that could lead to excessive gas consumption were found.
Unused Code	🟢	No significant portions of unused or redundant code were found.
Overall Contract Safety	🔴	The contract has several areas of concern including front running and logical issues that could affect overall safety.

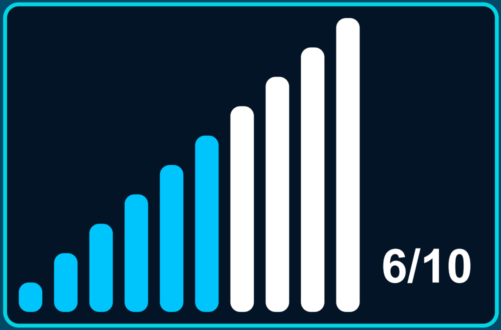
Market Analysis

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