OXSCANS

OTSea

AI Generated at 07:20 PM, UTC

February 13, 2024

OVERVIEW

This audit has been perpared for 'OTSea' 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

OTSea

OTSea is an OTC trading platform offering a simplified and streamlined trading experience for ERC20 token traders.

Name **OTSea**

Info Website Telegram Bot Docs Twitter

General Information

Tokenomics

Contract Address 0x5da151b95657e788076d04d56234bd93e409cb09

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	2784	v0.8.20

Smart Contract Stats

Functions	Events	Constructor
26	12	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	**1** threats found
Low	**0** threats found
Informational	**0** threats found

Detail Analysis

Vulnerability Check

18 Passed | 3 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- Outdated Compiler Version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

18 Passed

3 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		No arbitrary jumps or writes detected in the smart contract.
Centralization of Control		Operator role is centralized and can mint tokens arbitrarily.
Compiler Issues		Compiler version used is 0.8.20 which is known to be stable.
Delegate Call to Untrusted Contract		No delegate calls to untrusted contracts present in the smart contract.
Dependence on Predictable Variables		No dependence on predictable variables like block.timestamp or block.number found.

Detail Analysis

Detail Analysis

18 Passed

3 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft		No vulnerabilities that could lead to Ether or token theft were found.
Flash Loans		Flash loan attacks are not applicable to this contract.
Front Running		No obvious front-running vulnerabilities detected.
Improper Events		All events are properly declared and emitted.
Improper Authorization Scheme		The contract has an improper authorization scheme due to a centralized operator role.
Integer Over/Underflow		SafeMath library used consistently to prevent overflows and underflows.

Detail Analysis

Detail Analysis

18 Passed

3 Fail

CATEGORY	STATUS	NOTES
Logical Issues		No logical issues or inconsistencies found in the contract code.
Oracle Issues		The contract does not rely on external oracles.
Outdated Compiler Version		Compiler version is not outdated; it's 0.8.20.
Race Conditions		No race conditions were detected in the contract's functions.
Reentrancy		ReentrancyGuard is used to prevent reentrancy attacks.
Signature Issues		The contract does not use Ethereum signatures.

Detail Analysis

Detail Analysis

18 Passed

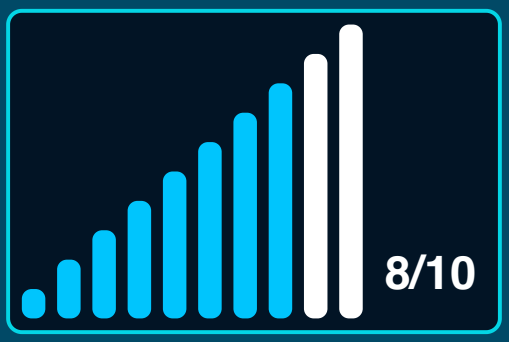
3 Fail

CATEGORY	STATUS	NOTES
Sybil Attack		Sybil attacks are not relevant to this contract's functionality.
Unbounded Loops		No unbounded loops that could lead to gas limit issues were found.
Unused Code		No significant chunks of unused code were found in the contract.
Overall Contract Safety		The contract is generally safe but centralization in control poses risks.

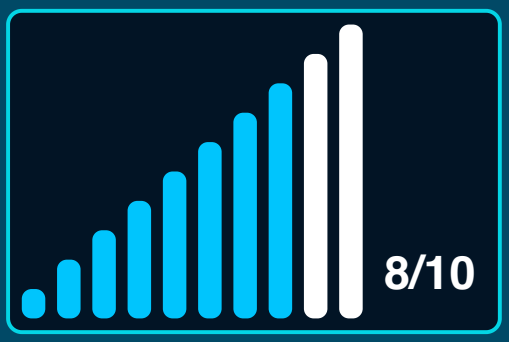
Market Analysis

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