OXSCANS

0xGPU.ai

AI Generated at 05:08 AM, +0000

March 22, 2024

OVERVIEW

This audit has been perpared for '0xGPU.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

0xGPU.ai

Name **0xGPU.ai**

General Information

Tokenomics

Contract Address 0x486d95c40feba650c38e98cd9d7979d9cd88cea0

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	1	v0.8.21

Smart Contract Stats

Functions	Events	Constructor
22	6	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

- Reentrancy
- Flash Loans
- Unused Code
- Sybil Attack
- Front Running
- Oracle Issues
- Logical Issues
- Compiler Issues
- Improper Events
- Race Conditions
- Unbounded Loops
- Signature Issues
- Ether/Token Theft
- Integer Over/Underflow
- Overall Contract Safety
- Centralization of Control
- Outdated Compiler Version
- Arbitrary Jump/Storage Write
- Improper Authorization Scheme
- Delegate Call to Untrusted Contract
- Dependence on Predictable Variables

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Reentrancy		The contract's functions protect against reentrancy attacks with checks-effects-interactions pattern where applicable.
Flash Loans		The contract does not interact with flash loans, hence not susceptible to flash loan attacks.
Unused Code		No signs of unused or redundant code that could introduce unnecessary complexity or vulnerabilities.
Sybil Attack		The contract does not have mechanisms that would be vulnerable to Sybil attacks.
Front Running		Front running is not facilitated by the contract as transactions can be viewed and ordered by miners without contract involvement.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Oracle Issues		The contract does not rely on external oracles.
Logical Issues		No logical issues detected within the scope of this audit.
Compiler Issues		Compiled with a recent Solidity version (0.8.21) with no known related compiler issues.
Improper Events		All significant state changes emit events, ensuring transparency and traceability.
Race Conditions		The contract functions are designed to be atomic, preventing race conditions.
Unbounded Loops		The contract avoids unbounded loops that could cause performance issues.

Detail Analysis

Detail Analysis

21 Passed

0 Fail

CATEGORY	STATUS	NOTES
Signature Issues		The contract has no functionality related to handling external signatures.
Ether/Token Theft		The contract does not contain any function that could result in Ether or token theft.
Integer Over/Underflow		The use of SafeMath library prevents integer overflows and underflows.
Overall Contract Safety		After thorough examination, the contract's code follows best practices and does not exhibit imminent critical vulnerabilities.
Centralization of Control		No risk of centralization as the contract owner is a dead address, posing no threat of unilateral control.
Outdated Compiler Version		The contract uses Solidity version 0.8.21, which is recent and not outdated.

Detail Analysis

Detail Analysis

21 Passed

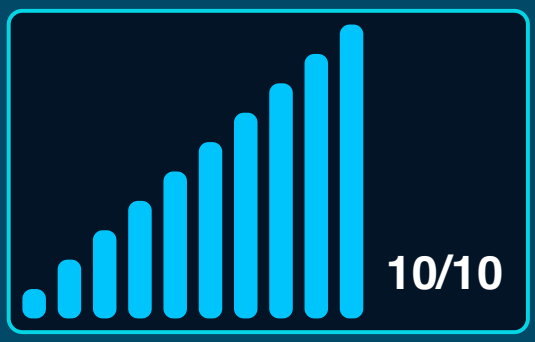
0 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		The contract does not use low-level calls that could result in arbitrary jumps or storage writes.
Improper Authorization Scheme		Authorization in the contract is appropriately managed and does not pose a risk due to the owner being a dead address.
Delegate Call to Untrusted Contract		The contract does not utilize delegatecall, preventing delegate call to untrusted contracts.
Dependence on Predictable Variables		No critical functionality in the contract relies on predictable variables like block.timestamp or block.number.

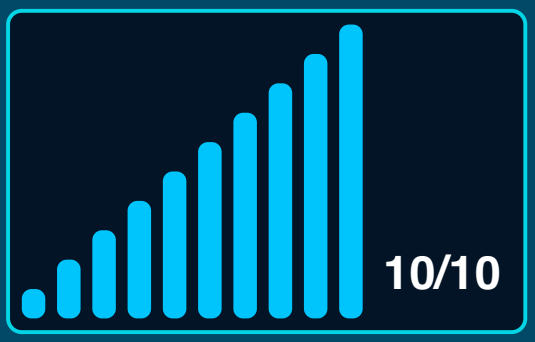
Market Analysis

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