



OXSCANS

Beam

AI Generated at 03:21 PM, UTC

February 18, 2024

OVERVIEW

This audit has been prepared for 'Beam' 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

1 General Info

2 General Analysis

3 Vulnerability check

4 Threat Analysis

5 Risks & Recommendations

6 Conclusions

7 Disclaimer

General Information

Beam

The \$BEAM token serves as the native crypto asset for the Beam network, a gaming network empowered by the Merit Circle DAO.

Name

Beam

Category

Binance Launchpool

Immutable Ecosystem

Gaming (GameFi)

DWF Labs Portfolio

BNB Chain Ecosystem

Ethereum Ecosystem

Info

[Website](#)

[Telegram Bot](#)

General Information

Tokenomics

Ticker

BEAMX

Network

Ethereum

Contract Address

0x62d0a8458ed7719fdaf978fe5929c6d342b0bfce

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)



1

Token holders



26647

Compiler



v0.8.6

Smart Contract Stats

Functions



35

Events



7

Constructor



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 secuirty 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 detected; contract uses standard OpenZeppelin libraries. |
| Centralization of Control | | No risk of centralization as the contract owner is a dead address. |
| Compiler Issues | | Compiled with a recent compiler version without known issues. |
| Delegate Call to Untrusted Contract | | No delegate calls to untrusted contracts present in the code. |
| Dependence on Predictable Variables | | No reliance on blockhash, timestamp, or block number for critical logic. |

Detail Analysis

Detail Analysis



21 Passed



0 Fail

| CATEGORY | STATUS | NOTES |
|-------------------------------|--------|--|
| Ether/Token Theft | | No functions that transfer Ether or tokens without proper authorization. |
| Flash Loans | | Flash loan attack vector not applicable to this contract. |
| Front Running | | No apparent vulnerabilities to front-running detected. |
| Improper Events | | All external and public state-changing functions emit events. |
| Improper Authorization Scheme | | Uses standard AccessControl authorization, with checks for role-based permissions. |
| Integer Over/Underflow | | SafeMath not required for Solidity 0.8.x; arithmetic operations are safe. |

Detail Analysis

Detail Analysis



21 Passed



0 Fail

| CATEGORY | STATUS | NOTES |
|---------------------------|--------|---|
| Logical Issues | | No logical errors detected; manual review recommended for complex logic. |
| Oracle Issues | | Contract does not use oracles. |
| Outdated Compiler Version | | Uses a recent and stable version of the Solidity compiler. |
| Race Conditions | | No race conditions detected in contract interactions. |
| Reentrancy | | No reentrancy vulnerabilities detected; uses known, safe patterns. |
| Signature Issues | | The contract uses EIP-712 compliant signatures which are secure and standard. |

Detail Analysis

Detail Analysis



21 Passed



0 Fail

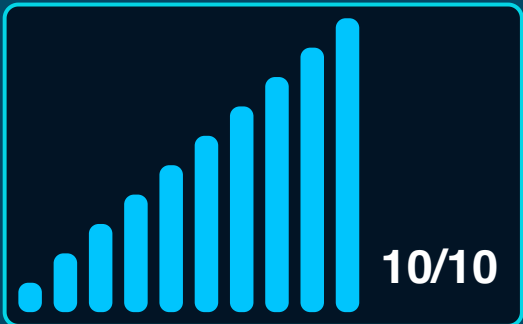
| CATEGORY | STATUS | NOTES |
|-------------------------|--------|---|
| Sybil Attack | | Sybil attack vector not applicable to this contract. |
| Unbounded Loops | | No unbounded loops that could lead to gas limit issues. |
| Unused Code | | No significant chunks of unused code found in the contract. |
| Overall Contract Safety | | Contract follows standard security patterns and practices. |

Market Analysis

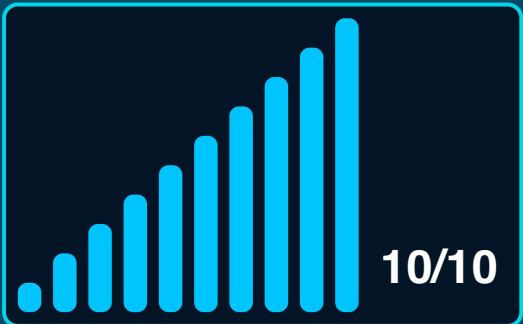


Score

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