OXSCANS

Moon Tropica

AI Generated at 02:44 PM, UTC

February 28, 2024

OVERVIEW

This audit has been perpared for 'Moon Tropica' 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

Moon Tropica

Crypto Twitter in an RPG game developed with the community.

Name	**Moon Tropica**
Category	**Gaming (GameFi)** **Ethereum Ecosystem**
Info	Website Telegram Bot

General Information

Tokenomics

Ticker	0X8E0E57DCB1CE8D9091DF38EC1BFC3B224529754A
Network	Ethereum
Contract Address	0x8e0e57dcb1ce8d9091df38ec1bfc3b224529754a

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	3147	v0.5.9

Smart Contract Stats

Functions	Events	Constructor
26	8	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	**2** threats found
Informational	**2** threats found

Detail Analysis

Vulnerability Check

19 Passed

2 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

19 Passed

2 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write		The contract does not contain 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 compiled with an outdated version of the Solidity compiler (0.5.9), which may not include recent security fixes.
Delegate Call to Untrusted Contract		The contract does not use delegatecall to untrusted contracts.
Dependence on Predictable Variables		The contract does not appear to have a dependence on predictable variables for its core logic.

Detail Analysis

Detail Analysis

19 Passed

2 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft		There are no functions that transfer Ether or tokens without proper authorization or that seem vulnerable to theft.
Flash Loans		The contract does not interact with flash loan functions.
Front Running		The contract functions do not appear to be susceptible to front-running attacks.
Improper Events		All events are properly emitted following state changes.
Improper Authorization Scheme		The contract uses a role-based authorization scheme which is appropriate.
Integer Over/Underflow		The contract uses DSMath library which has overflow/underflow protections.

Detail Analysis

Detail Analysis

19 Passed

2 Fail

CATEGORY	STATUS	NOTES
Logical Issues	●	No logical issues detected in the contract code.
Oracle Issues	●	The contract does not use oracles.
Outdated Compiler Version	●	The contract uses Solidity version 0.5.9 which is outdated.
Race Conditions	●	The contract does not seem to have functions that are susceptible to race conditions.
Reentrancy	●	The contract does not exhibit reentrancy vulnerabilities.
Signature Issues	●	The contract does not handle external signatures.

Detail Analysis

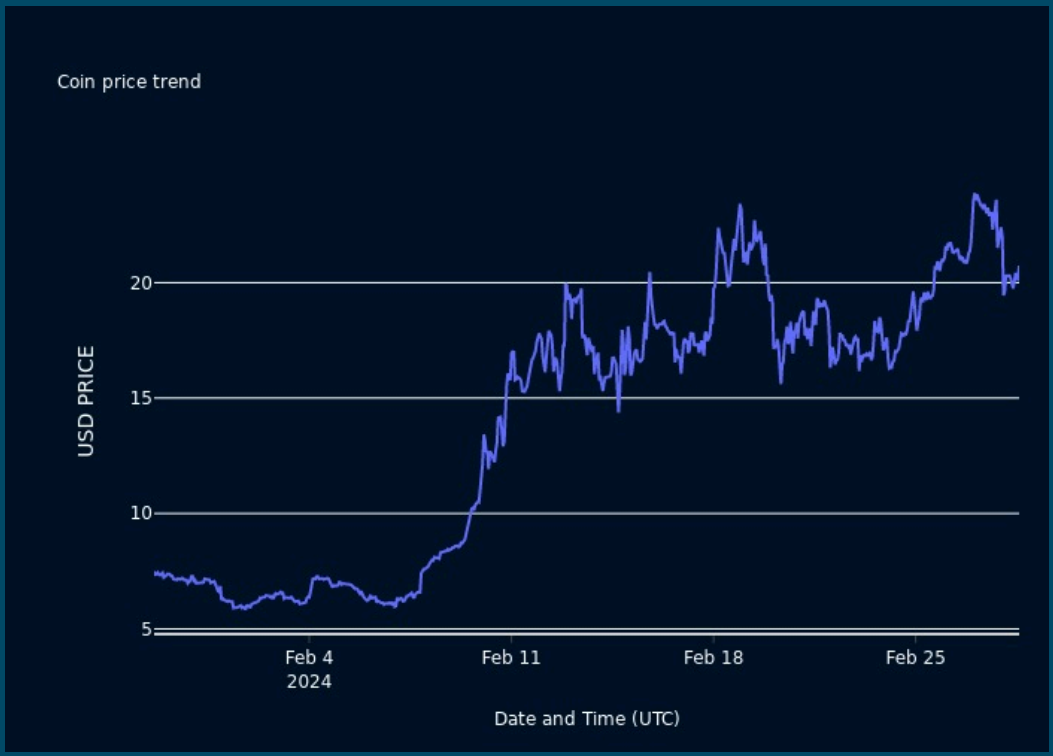
Detail Analysis

19 Passed

2 Fail

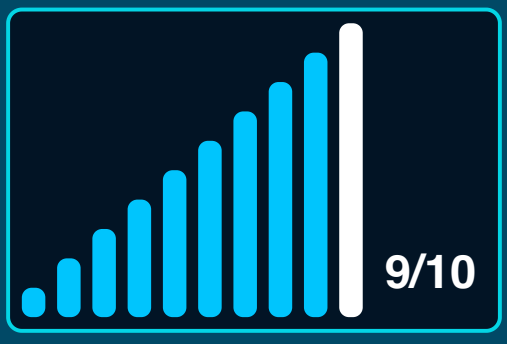
CATEGORY	STATUS	NOTES
Sybil Attack		The contract is not susceptible to Sybil attacks.
Unbounded Loops		The contract does not contain unbounded loops that could lead to denial of service.
Unused Code		No significant amount of unused code present in the contract.
Overall Contract Safety		The contract follows good practices and does not exhibit critical security vulnerabilities.

Market Analysis

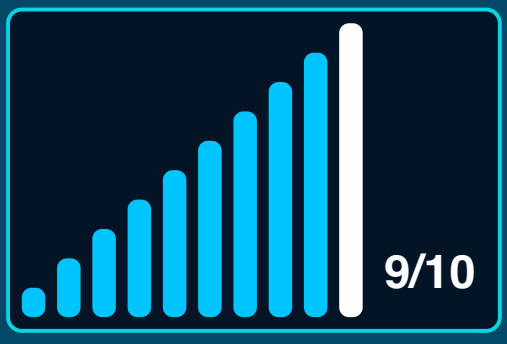


Score

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