



Moon Guard

MARCH

Smart Contract Audit Report

MARCH
November, 2021

Audit Details



Project Name

March



Contract address

0x5977003b14bfc08eed42e9a0da26c6ee166d5a84



Blockchain

Binance Smart Chain



Project website

<https://marctoken.nl/>

Line Contract Code Audit

Codes line	Bug found	Results
Reentrancy on a single Function	No Bug	Passed
Fallback Function security	No Bug	Passed
Overflow and underflow	No Bug	Passed
Insufficient gas griefing	No Bug	Passed
DoS with unexpected revert	No Bug	Passed
Economy model	No Bug	Passed
Claimable Function	No Bug	Passed
Block gas limit	No Bug	Passed
Unchecked Return Value calls	No Bug	Passed
Oracle calls	No Bug	Passed
Malicious codes log	No Bug	Passed
Data daily delivery	No Bug	Passed
Compile fallacy	No Bug	Passed
Owner access funds	No Bug	Passed
Open ZeppelinContract implementation	No Bug	Passed

Proper check up have been done and Codes are risk free at the time of audit.

Security Audit Summary

Smart contract owner can't exclude from the fee.
Smart contract owner has no marketing wallet or fee wallet.
Smart contract Ownership was renounced at the time of audit.
Smart contract code is clear and safe at the time of audit



Low Risk Issues

No medium risks issues found.



Medium Risk Issues

No medium risks issues found.



High Risk Issues

No high severity issues found.

Contract recommendations:

All codes passed our inspections, No security risks found at the time of smart contract audit. Moon Guard team has no recommendations

Disclaimer

This report involves company terms & conditions by reading this report you've agreed to our terms & conditions, if you're not satisfied with our policy we advice to instantly keep off from this report thank you.

At MoonGuard audit company we check for harmful code lines that may result to lost of huge community funds, However we don't touch or guild the smart contract codes but we can recommend ways and steps on how to avoid those harmful codes.

The smart contract our team analyst is a token contract that has no harmful code. No any other smart contract was audited from the March team.

Blockchain technology and cryptographic assets present a high level of ongoing risk. MoonGuard position is that each company and individual are responsible for their own due diligence and continuous security. MoonGuard aim is to help reduce the hackers attack and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

this audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner. No information on our report is subjected to financial advic, we do not advice to get involve in any project we audit make sure you do your own research before getting involve in any blockchain projects