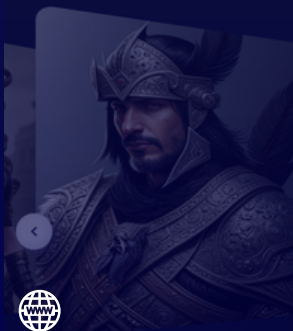
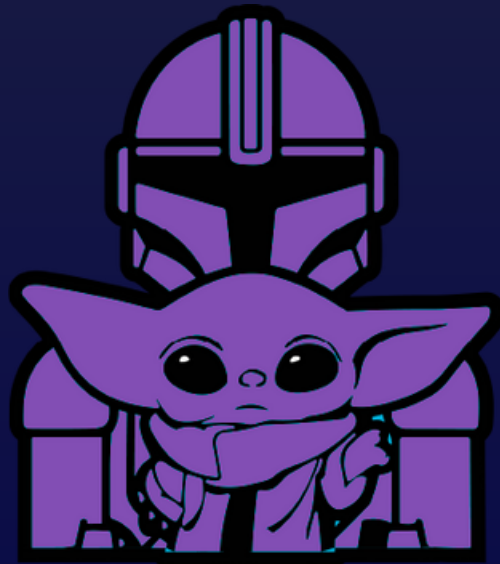


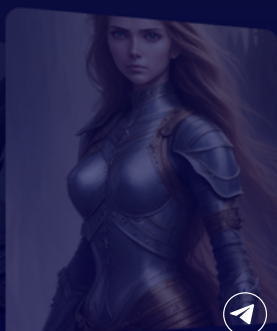


AUDIT REPORT

MANDYODA TOKEN (MAND)

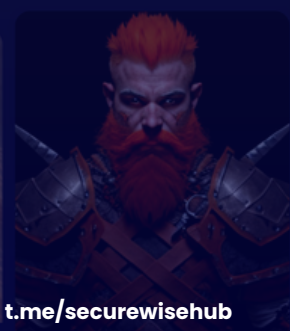


Deon
Full-Stack Developer

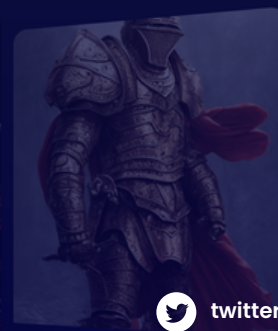


t.me/securewisehub

Paloma
Sales / Marketing Manager



Walter
CEO/Founder



twitter.com/securewiseAudit

Robbie
Senior Full-Stack Developer



Thomas
Senior Full-Stack Blockchain Dev

Quick Result

Quick Result	Status
Owner can mint new token?	Not Detected
Owner can update tax over 25% ?	Pass
Owner can pause trade ?	Not Detected
Owner can enable trading ?	Pass
Owner can add Blacklist ?	Pass
Owner can set Max Tx ?	Yes
Owner can set Max Wallet Amount ?	Not Detected
KYC ?	No

Page 6 for more details

MandYoda Token (MAND) as **PASSED** the smart contract audit with **High Risk**

Findings

Risk Classification	Description
High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.
Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fixed as soon as possible.
Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
Informational	A vulnerability that have informational character but is not effecting any of the code

Severity	Found	Pending	Resolved
High	1	0	0
Medium	0	0	0
Low	2	0	0
Informational	7	0	0
Total	10	0	0

Contents

- 01 Quick Result
- 02 Findings
- 04 Overview
- 05 Auditing Approach and Methodologies
- 06 Findings Summary
- 07 Function Privileges
- 08 Inheritance Graph
- 09 Manuel Review
- 10 Disclaimer

Overview

Token Name: MandYoda Token (**MAND**)

Language: Solidity

Contract Address: 0x2D24Fd27B3C0fd6A89380fad360c78C6B10da16b

Network: Binance Smart Chain

Total Supply: 1000000000

KYC: No

Website: <https://mandyoda.com/>

Twitter: <https://twitter.com/MandYodaToken>

Telegram: <https://t.me/mandyoda>

Report Date: September 29, 2023

Testnet Link:

<https://testnet.bscscan.com/address/0x8C1f0c4665e43Ea7efe2f18B42B1817264E9641f>

Auditing Approach and Methodologies

SecureWise has performed starting with analyzing the code, issues, code quality, and libraries. Reviewed line-by-line by our team. Finding any potential issue like race conditions, transaction-ordering dependence, timestamp dependence, and denial of service attacks.

Methodology

- Understanding the size, scope and functionality of your project's source code
- Manual review of code, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Testing and automated analysis of the Smart Contract to determine proper logic has been followed throughout the whole process
- Deploying the code on testnet using multiple live test
- Analyzing a program to determine the specific input that causes different parts of a program to execute its functions.
- Checking whether all the libraries used in the code are on the latest version.

Goals

Smart Contract System is secure, resilient and working according to the specifications and without any vulnerabilities.

Risk Classification

High: Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, of the contract and its functions. Must be fixed as soon as possible.

Medium: Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Must be fixed as soon as possible.











Low: Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

Informational: A vulnerability that have informational character but is not effecting any of the code

Findings Summary

SecureWise has applied the automated and manual analysis of Smart Contract and were reviewed for common contract vulnerabilities and centralized exploits

Findings

	Trade must be enabled by the owner. TRADE ENABLED
	There is a sniper tax, but if it is not removed by the owner, everyone pays 99% fee. SNIPER FEE REMOVED
	If the owner marks any address as CEX, that address can buy or sell without fee.
	Owner can limit buyers' maximum holding quantity.
	Everyone can trigger swap back function there is a lack of authorization.
	The owner has the authority to change the autoSwap setting and can set swapThreshold to "0" If the owner set to zero, contract would always enter into swaps
	maxBuy only used for MarketMaker and Cex. logically can be able transfer more than max buy
	The owner has the authority to change fees max buy 10% sell 10% transfer 10% and cex transfer 10%
	The owner has the authority to exclude/include addresses from fees.
	The owner has the authority to withdraw claimstuck tokens and bnb from the contract.

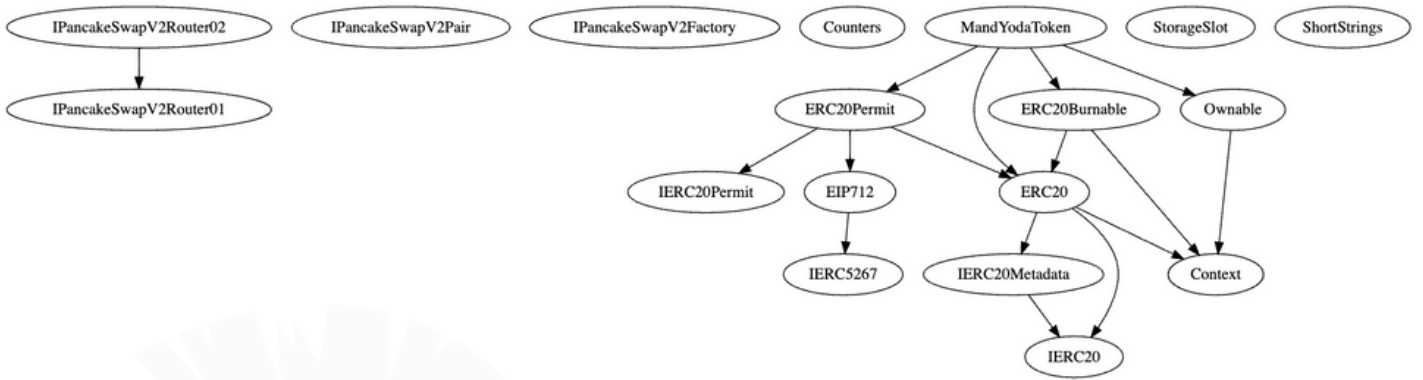
Function Privileges

```

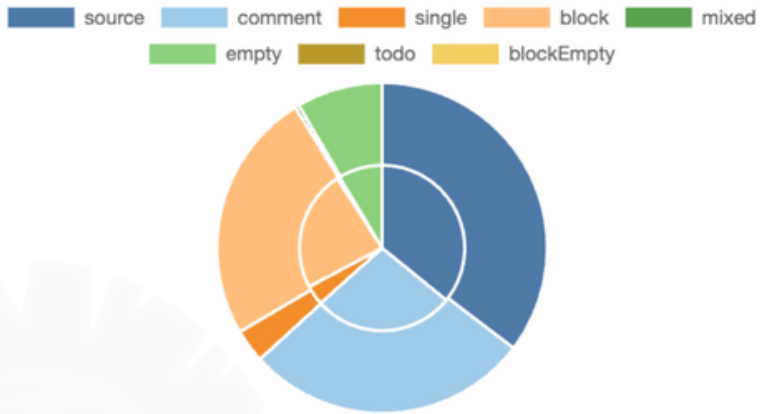
|||||
**ERC20Burnable** | Implementation | Context, ERC20 |||
| L | burn | Public ! | ● |NO ! |
| L | burnFrom | Public ! | ● |NO ! |
|||||
**MandYodaToken** | Implementation | ERC20, ERC20Burnable, Ownable, ERC20Permit |||
| L | <Constructor> | Public ! | ● | ERC20 ERC20Permit |
| L | <Receive Ether> | External ! | 🚫 |NO ! |
| L | _mint | Internal 🔒 | ● | |
| L | initializeProject | External ! | ● | onlyOwner |
| L | _transfer | Internal 🔒 | ● | |
| L | _takeTax | Internal 🔒 | ● | |
| L | _getTotalTax | Internal 🔒 | | |
| L | _shouldSwapBack | Internal 🔒 | | |
| L | _swapBack | Internal 🔒 | ● | swapping |
| L | removeSniperTax | External ! | ● | onlyOwner |
| L | enableTrading | External ! | ● | onlyOwner |
| L | triggerSwapBack | External ! | ● |NO ! |
| L | recoverBNB | External ! | ● |NO ! |
| L | recoverBEP20 | External ! | ● |NO ! |
| L | setIsWhitelisted | External ! | ● | onlyOwner |
| L | setIsCEX | External ! | ● | onlyOwner |
| L | setIsMarketMaker | External ! | ● | onlyOwner |
| L | setTaxes | External ! | ● | onlyOwner |
| L | setShares | External ! | ● | onlyOwner |
| L | setSwapBackSettings | External ! | ● | onlyOwner |
| L | setTransferGas | External ! | ● | onlyOwner |
| L | setMaxBuy | External ! | ● | onlyOwner |
| L | setMarketingWallet | External ! | ● | onlyOwner |
| L | router | Internal 🔒 | | |
| L | isEthereumMainnet | Internal 🔒 | | |
| L | isGoerli | Internal 🔒 | | |
| L | isSepolia | Internal 🔒 | | |
| L | isBSCMainnet | Internal 🔒 | | |
| L | isBSCTestnet | Internal 🔒 | | |
| L | isTestnet | Internal 🔒 | | |

```

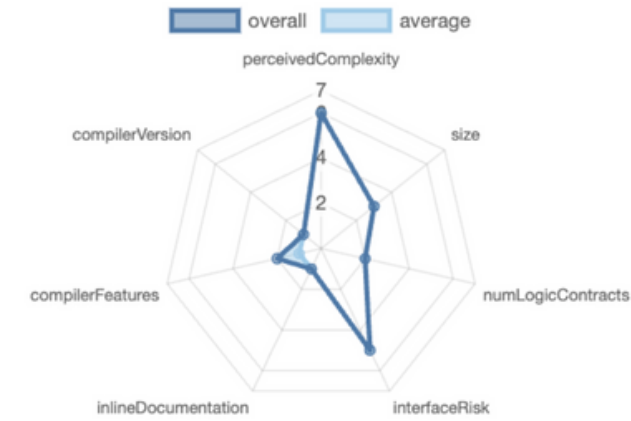

Inheritance Graph



Source Lines



Risk



Disclaimer

SecureWise provides the smart contract audit of solidity. Audit and report are for informational purposes only and not, nor should be considered, as an endorsement to engage with, invest in, participate, provide an incentive, or disapprove, criticise, discourage, or purport to provide an opinion on any particular project or team.

This audit report doesn't provide any warranty or guarantee regarding the nature of the technology analysed. These reports, in no way, provide investment advice, nor should be used as investment advice of any sort. Investors must always do their own research and manage their risk.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and SecureWise and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) SecureWise owe no duty of care towards you or any other person, nor does SecureWise make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SecureWise hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SecureWise hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SecureWise, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.



AUDIT REPORT

SecureWise



securewise.org



t.me/securewisehub



twitter.com/securewiseAudit



SecureWise Scanner



t.me/pinksalefreechecks

