

Smart Contract Audit

FOR

MYRADOGE

DATED : 08 FEBRUARY 24'



AUDIT SUMMARY

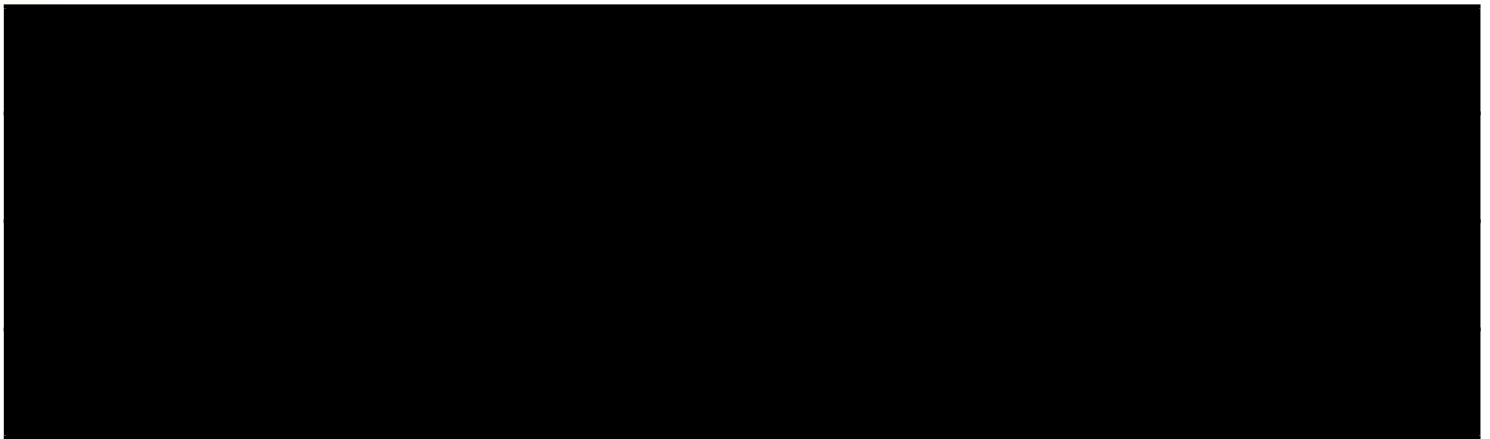
Project name - MYRADOGE

Date: 08 February, 2024

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: Passed

Issues Found





Token Information

Token Name : MYRADOGE

Token Symbol: MYRA

Decimals: 9

Token Supply : 1,000,000,000

Token Address:

0x385FDD34C1432B7AC0Ed19C51DcFf3136b5b70DC

Owner:

0x413178403bcE833B19642df6d4d10C3D9EF47abD

Deployer:

0x413178403bcE833B19642df6d4d10C3D9EF47abD



TOKEN OVERVIEW

Fees:

Buy Fees: upto 5 %

Sell Fees: upto 5 %

Transfer Fees: 5 %

Fees Privilege: none

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: yes

Blacklist: No

Other Privileges: modifying swap threshold - toggling
internal swap - excluding wallets from fee - including
wallets in fee



AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
 - Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
 - Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
 - Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
 - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-



VULNERABILITY CHECKLIST

- | | |
|--|---|
|  Return values of low-level calls |  Gasless Send |
|  Private modifier |  Using block.timestamp |
|  Multiple Sends |  Re-entrancy |
|  Using Suicide |  Tautology or contradiction |
|  Gas Limitand Loops |  Timestamp Dependence |
|  Address hardcoded |  Revert/require functions |
|  Exception Disorder |  Use of tx.origin |
|  Using inline assembly |  Integer overflow/underflow |
|  Divide before multiply |  Dangerous strict equalities |
|  Missing Zero Address Validation |  Using SHA3 |
|  Compiler version not fixed |  Using throw |
-



CLASSIFICATION OF RISK

Severity

Description

◆ Critical	This smart contract is highly rated for its security, reliability, and stable operation, providing a solid foundation for safe and efficient transactions
◆ High-Risk	A feature that enhances the flexibility of a contract, allowing users to achieve their desired outcomes in various ways.
◆ Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
◆ Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
◆ Gas Optimization / Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity

Found

◆ Critical	0
◆ High-Risk	0
◆ Medium-Risk	1
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0



POINTS TO NOTE

- Owner is able to change buy/sell/transfer taxes (5%)
 - Owner is not able to set max buy/sell/transfer/hold amount
 - Owner is not able to blacklist an arbitrary wallet
 - Owner is not able to disable trades
 - Owner has to enable trades manually for holders
 - Owner is not able to mint new tokens
 - Owner is able to set a max wallet/transfer/buy/sell amount.
-



CONTRACT ASSESMENT

Contract	Type	Bases			
└──────────┘	└──────────┘	└──────────┘	└──────────┘	└──────────┘	└──────────┘
└┬┘	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
└┬┘	**IERC20**	Interface			
└┬┘	totalSupply	External !		NO!	
└┬┘	balanceOf	External !		NO!	
└┬┘	transfer	External !	●	NO!	
└┬┘	allowance	External !		NO!	
└┬┘	approve	External !	●	NO!	
└┬┘	transferFrom	External !	●	NO!	
└┬┘	**SafeMath**	Library			
└┬┘	add	Internal H			
└┬┘	sub	Internal .H			
└┬┘	sub	Internal H.			
└┬┘	mul	Internal H.			
└┬┘	div	Internal .H			
└┬┘	div	Internal H.			
└┬┘	mod	Internal H.			
└┬┘	mod	Internal H			
└┬┘	**Context**	Implementation			
└┬┘	_msgSender	Internal H			
└┬┘	_msgData	Internal H.			
└┬┘	**Address**	Library			
└┬┘	isContract	Internal H.			
└┬┘	sendValue	Internal H.	●		
└┬┘	functionCall	Internal H.	●		
└┬┘	functionCall	Internal H.	●		
└┬┘	functionCallWithValue	Internal H.	●		
└┬┘	functionCallWithValue	Internal H.	●		
└┬┘	_functionCallWithValue	Private (u)	●		
└┬┘	**Ownable**	Implementation		Context	
└┬┘	<Constructor>	Public !	●	NO!	
└┬┘	owner	Public !		NO!	
└┬┘	renounceOwnership	Public !	●	onlyOwner	
└┬┘	transferOwnership	Public !	●	onlyOwner	
└┬┘	**IUniswapV2Factory**	Interface			



CONTRACT ASSESMENT

```
|  | feeTo | External ! | | NO! |
|  | feeToSetter | External ! | | NO! |
|  | getPair | External ! | | NO! |
|  | allPairs | External ! | | NO! |
|  | allPairsLength | External ! | | NO! |
|  | createPair | External ! | ● | NO! |
|  | setFeeTo | External ! | ● | NO! |
|  | setFeeToSetter | External ! | ● | NO! |
|  |  |  |  |  |
|  |  |  |  |  |
| **IUniswapV2Pair** | Interface | |  |
|  | name | External ! | | NO! |
|  | symbol | External ! | | NO! |
|  | decimals | External ! | | NO! |
|  | totalSupply | External ! | | NO! |
|  | balanceOf | External ! | | NO! |
|  | allowance | External ! | | NO! |
|  | approve | External ! | ● | NO! |
|  | transfer | External ! | ● | NO! |
|  | transferFrom | External ! | ● | NO! |
|  | DOMAIN_SEPARATOR | External ! | | NO! |
|  | PERMIT_TYPEHASH | External ! | | NO! |
|  | nonces | External ! | | NO! |
|  | permit | External ! | ● | NO! |
|  | MINIMUM_LIQUIDITY | External ! | | NO! |
|  | factory | External ! | | NO! |
|  | token0 | External ! | | NO! |
|  | token1 | External ! | | NO! |
|  | getReserves | External ! | | NO! |
|  | price0CumulativeLast | External ! | | NO! |
|  | price1CumulativeLast | External ! | | NO! |
|  | kLast | External ! | | NO! |
|  | mint | External ! | ● | NO! |
|  | burn | External ! | ● | NO! |
|  | swap | External ! | ● | NO! |
|  | skim | External ! | ● | NO! |
|  | sync | External ! | ● | NO! |
|  | initialize | External ! | ● | NO! |
|  |  |  |  |  |
| **IUniswapV2Router01** | Interface | |  |
|  | factory | External ! | | NO! |
|  | WETH | External ! | | NO! |
```



CONTRACT ASSESMENT

```
| L | addLiquidity | External ! | ● | NO! |
| L | addLiquidityETH | External ! | ■ | NO! |
| L | removeLiquidity | External ! | ● | NO! |
| L | removeLiquidityETH | External ! | ● | NO! |
| L | removeLiquidityWithPermit | External ! | ● | NO! |
| L | removeLiquidityETHWithPermit | External ! | ● | NO! |
| L | swapExactTokensForTokens | External ! | ● | NO! |
| L | swapTokensForExactTokens | External ! | ● | NO! |
| L | swapExactETHForTokens | External ! | ■ | NO! |
| L | swapTokensForExactETH | External ! | ● | NO! |
| L | swapExactTokensForETH | External ! | ● | NO! |
| L | swapETHForExactTokens | External ! | ■ | NO! |
| L | quote | External ! | | NO! |
| L | getAmountOut | External ! | | NO! |
| L | getAmountIn | External ! | | NO! |
| L | getAmountsOut | External ! | | NO! |
| L | getAmountsIn | External ! | | NO! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● | NO! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | ■ | NO! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO! |
|||||
| **TROLLBNB** | Implementation | Context, IERC20, Ownable |||
| L | <Constructor> | Public ! | ● | NO! |
| L | name | External ! | | NO! |
| L | symbol | External ! | | NO! |
| L | decimals | External ! | | NO! |
| L | totalSupply | External ! | | NO! |
| L | isExcludedFromMaxTx | External ! | | NO! |
| L | balanceOf | Public ! | | NO! |
| L | transfer | External ! | ● | NO! |
| L | allowance | External ! | | NO! |
| L | approve | External ! | ● | NO! |
| L | transferFrom | External ! | ● | NO! |
| L | increaseAllowance | External ! | ● | NO! |
| L | decreaseAllowance | External ! | ● | NO! |
| L | isExcludedFromReward | External ! | | NO! |
| L | totalFees | External ! | | NO! |
```



CONTRACT ASSESMENT

	└		excludeFromMaxTx		External !		●		onlyOwner	
	└		deliver		External !		●		NO!	
	└		reflectionFromToken		External !				NO!	
	└		tokenFromReflection		Public !				NO!	
	└		excludeFromReward		External !		●		onlyOwner	
	└		includeInReward		External !		●		onlyOwner	
	└		_transferBothExcluded		Private (μ)		●			
	└		excludeFromFee		External !		●		onlyOwner	
	└		includeInFee		External !		●		onlyOwner	
	└		setMarketingWallet		External !		●		onlyOwner	
	└		setDevWallet		External !		●		onlyOwner	
	└		setBurningAddress		External !		●		onlyOwner	
	└		setSwapThresholdAmount		External !		●		onlyOwner	
	└		allowtrading		External !		●		onlyOwner	
	└		setMigrationWallet		External !		●		onlyOwner	
	└		setSwapAndLiquifyEnabled		External !		●		onlyOwner	
	└		setMaxTxPercent		External !		●		onlyOwner	
	└		manualSwap		External !		●		NO!	
	└		<Receive Ether>		External !		■		NO!	
	└		_reflectFee		Private (μ)		●			
	└		_getValues		Private (μ)					
	└		_getTValues		Private (μ)					
	└		_getRValues		Private (μ)					
	└		_getRate		Private (μ)					
	└		_getCurrentSupply		Private (μ)					
	└		_takeLiquidity		Private (μ)		●			
	└		calculateTaxFee		Private (μ)					
	└		calculateLiquidityFee		Private (μ)					
	└		removeAllFee		Private (μ)		●			
	└		restoreAllFee		Private (μ)		●			
	└		isExcludedFromFee		External !				NO!	
	└		_approve		Private (μ)		●			
	└		_transfer		Private (μ)		●			
	└		swapAndLiquify		Private (μ)		●		lockTheSwap	
	└		swapTokensForEth		Private (μ)		●			
	└		addLiquidity		Private (μ)		●			
	└		_tokenTransfer		Private (μ)		●			
	└		_transferStandard		Private (μ)		●			
	└		_transferToExcluded		Private (μ)		●			
	└		_transferFromExcluded		Private (μ)		●			



CONTRACT ASSESMENT

Legend

Symbol	Meaning
:-----: -----	
●	Function can modify state
🏠	Function is payable



STATIC ANALYSIS

```
Variable TROLLBNB.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1067) is too similar to TROLLBNB._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1502)
Variable TROLLBNB._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1500) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1204)
Variable TROLLBNB._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1479) is too similar to TROLLBNB._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1461)
Variable TROLLBNB._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1459) is too similar to TROLLBNB._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1481)
Variable TROLLBNB._getValues(uint256).rTransferAmount (contracts/Token.sol#1208) is too similar to TROLLBNB._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1481)
Variable TROLLBNB._getValues(uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1242) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1204)
Variable TROLLBNB._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1459) is too similar to TROLLBNB._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1115)
Variable TROLLBNB._getValues(uint256).rTransferAmount (contracts/Token.sol#1208) is too similar to TROLLBNB._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1115)
Variable TROLLBNB._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1459) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1229)
Variable TROLLBNB.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1067) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1204)
Variable TROLLBNB._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1479) is too similar to TROLLBNB._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1481)
Variable TROLLBNB._getValues(uint256).rTransferAmount (contracts/Token.sol#1208) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1229)
Variable TROLLBNB._getValues(uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#1242) is too similar to TROLLBNB._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1461)
Variable TROLLBNB._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1113) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1204)
Variable TROLLBNB._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1479) is too similar to TROLLBNB._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1115)
Variable TROLLBNB._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1479) is too similar to TROLLBNB._getValues(uint256).tTransferAmount (contracts/Token.sol#1229)
Variable TROLLBNB.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#1067) is too similar to TROLLBNB._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1461)
Variable TROLLBNB._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1459) is too similar to TROLLBNB._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1502)
Variable TROLLBNB._getValues(uint256).rTransferAmount (contracts/Token.sol#1208) is too similar to TROLLBNB._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1502)
Variable TROLLBNB._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1113) is too similar to TROLLBNB._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1461)
Variable TROLLBNB._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1113) is too similar to TROLLBNB._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1481)
Variable TROLLBNB._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1500) is too similar to TROLLBNB._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1461)
Variable TROLLBNB._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1113) is too similar to TROLLBNB._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1502)
Variable TROLLBNB._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1500) is too similar to TROLLBNB._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1481)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

TROLLBNB.setSwapThresholdAmount(uint256) (contracts/Token.sol#1148-1156) uses literals with too many digits:
- require(bool,string)(SwapThresholdAmount > 69000000,Swap Threshold Amount cannot be less than 69 Million) (contracts/Token.sol#1151-1154)
TROLLBNB.slitherConstructorVariables() (contracts/Token.sol#853-1513) uses literals with too many digits:
- maxTxAmount = 5000000 * 10 ** 6 * 10 ** 9 (contracts/Token.sol#898)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output



DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.



ABOUT AUDITACE

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



<https://auditace.tech/>



https://t.me/Audit_Ace



https://twitter.com/auditace_
