



Smart Contract Audit

FOR

Stich Inu

DATED : 20 May 23'



AUDIT SUMMARY

Project name – Stich Inu

Date: 20 May, 2023

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

Audit Status: **Passed**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	1	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0



USED TOOLS

Tools:

1- Manual Review:

a line by line code review has been performed by audit ace team.

2- BSC Test Network:

all tests were done on BSC Test network, each test has its transaction has attached to it.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

<https://testnet.bscscan.com/address/0xc38714F350897F64bB40679321f7Ad3b4173B96e#code>



Token Information

Token Name : Stitch Inu

Token Symbol: StitchInu

Decimals: 9

Token Supply:420,000,000,000,000,000

Token Address:

0x8e79ab7C02D5b8B1cC5A6154EdEbd0f0033E821C

Checksum:

f803552931fc9b646677b37fdd16ec74396fdc29

Owner:

0xC0B3f99418E1871A9B4f2c68e3EBB2db8EE3fF2C



TOKEN OVERVIEW

Fees:

Buy Fees: 0-25%

Sell Fees: 0-25 %

Transfer Fees: 0-25%

Fees Privilege: owner

Ownership : owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: none

Blacklist: No

Other Privileges: Modifying fees- including in rewards-
excluding from rewards- changing swap threshold
- changing reward settings (min token to be eligible
and cooldown)- initial distribution of the tokens



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

These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.

◆ High-Risk

A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.

◆ 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

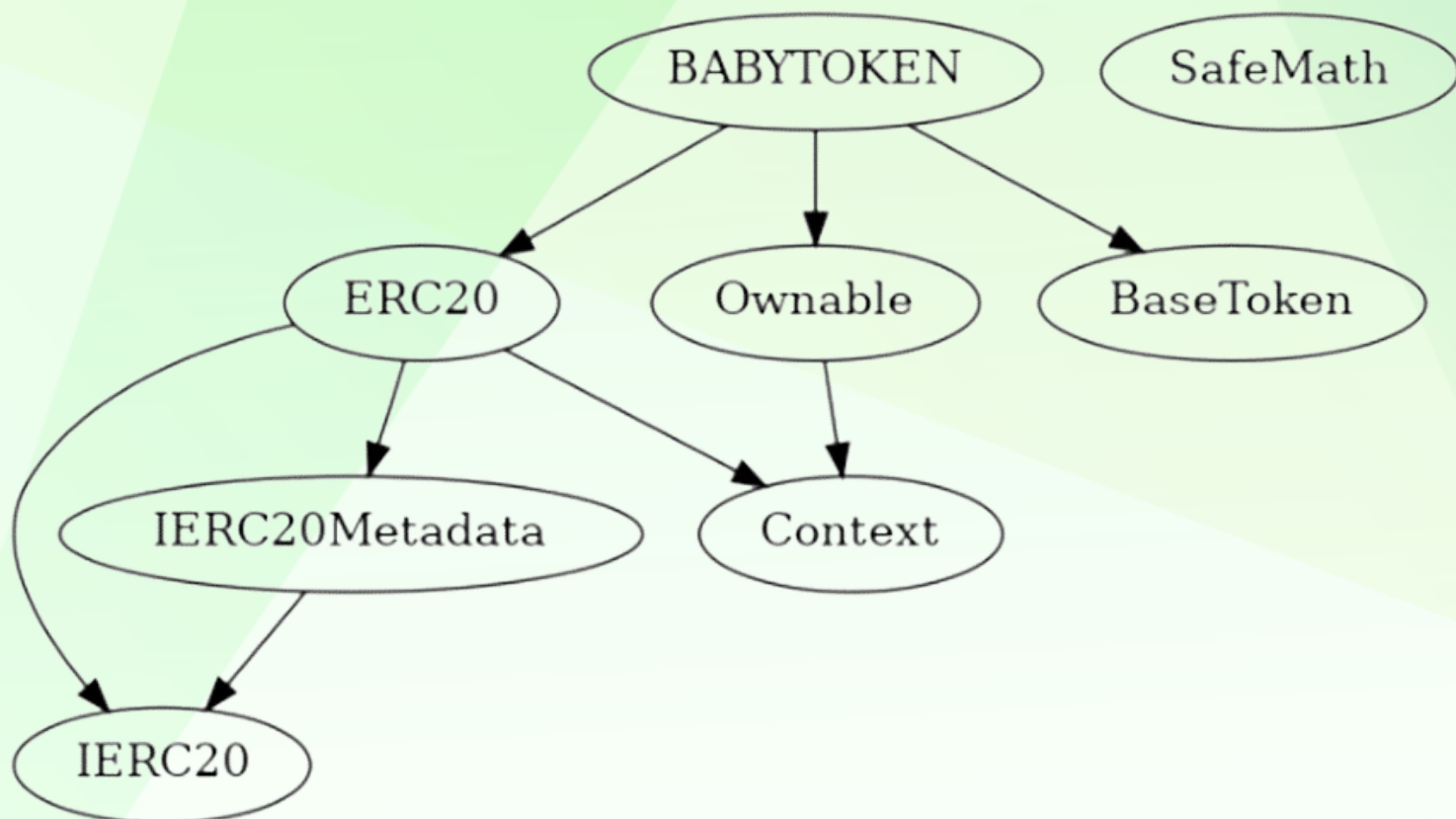
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

0

INHERITANCE TREE





POINTS TO NOTE









































- Owner is not able to change buy/sell/transfer fees within range 0-25%
 - Owner is not able to blacklist an arbitrary address.
 - Owner is not able to disable trades
 - Owner is not able to limit buy/sell/transfer/wallet amounts
 - Owner is not able to mint new tokens
 - **Token is pinksale generated (already tested) and uses busd as reward token.**
-

CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
IERC20 Interface					
L	totalSupply	External	!	NO!	
L	balanceOf	External	!	NO!	
L	transfer	External	!	NO!	
L	allowance	External	!	NO!	
L	approve	External	!	NO!	
L	transferFrom	External	!	NO!	
IERC20Metadata Interface IERC20					
L	name	External	!	NO!	
L	symbol	External	!	NO!	
L	decimals	External	!	NO!	
Context Implementation					
L	_msgSender	Internal	🔒		
L	_msgData	Internal	🔒		
ERC20 Implementation Context, IERC20, IERC20Metadata					
L	<Constructor>	Public	!	NO!	
L	name	Public	!	NO!	
L	symbol	Public	!	NO!	
L	decimals	Public	!	NO!	
L	totalSupply	Public	!	NO!	
L	balanceOf	Public	!	NO!	
L	transfer	Public	!	NO!	
L	allowance	Public	!	NO!	
L	approve	Public	!	NO!	
L	transferFrom	Public	!	NO!	
L	increaseAllowance	Public	!	NO!	
L	decreaseAllowance	Public	!	NO!	
L	_transfer	Internal	🔒		
L	_mint	Internal	🔒		
L	_burn	Internal	🔒		
L	_approve	Internal	🔒		
L	_beforeTokenTransfer	Internal	🔒		
L	_afterTokenTransfer	Internal	🔒		
Ownable Implementation Context					

CONTRACT ASSESMENT

```

| L | <Constructor> | Public ! |  | NO! |
| L | owner | Public ! | | NO! |
| L | renounceOwnership | Public ! |  | onlyOwner |
| L | transferOwnership | Public ! |  | onlyOwner |
| L | _setOwner | Private  |  | |
|||||
| **SafeMath** | Library | |||
| L | tryAdd | Internal  | | |
| L | trySub | Internal  | | |
| L | tryMul | Internal  | | |
| L | tryDiv | Internal  | | |
| L | tryMod | Internal  | | |
| L | add | Internal  | | |
| L | sub | Internal  | | |
| L | mul | Internal  | | |
| L | div | Internal  | | |
| L | mod | Internal  | | |
| L | sub | Internal  | | |
| L | div | Internal  | | |
| L | mod | Internal  | | |
|||||
| **Clones** | Library | |||
| L | clone | Internal  |  | |
| L | cloneDeterministic | Internal  |  | |
| L | predictDeterministicAddress | Internal  | | |
| L | predictDeterministicAddress | Internal  | | |
|||||
| **Address** | Library | |||
| L | isContract | Internal  | | |
| L | sendValue | Internal  |  | |
| L | functionCall | Internal  |  | |
| L | functionCall | Internal  |  | |
| L | functionCallWithValue | Internal  |  | |
| L | functionCallWithValue | Internal  |  | |
| L | functionStaticCall | Internal  | | |
| L | functionStaticCall | Internal  | | |
| L | functionDelegateCall | Internal  |  | |
| L | functionDelegateCall | Internal  |  | |
| L | verifyCallResult | Internal  | | |
|||||
| **IUniswapV2Factory** | Interface | |||
| L | feeTo | External ! | | NO! |

```

CONTRACT ASSESMENT

```
| | feeToSetter | External ! | | NO! |
| | getPair | External ! | | NO! |
| | allPairs | External ! | | NO! |
| | allPairsLength | External ! | | NO! |
| | createPair | External ! | | NO! |
| | setFeeTo | External ! | | NO! |
| | setFeeToSetter | External ! | | NO! |
| | | |
| **IUniswapV2Router01** | Interface | | |
| | factory | External ! | | NO! |
| | WETH | External ! | | NO! |
| | addLiquidity | External ! | | NO! |
| | addLiquidityETH | External ! | | NO! |
| | removeLiquidity | External ! | | NO! |
| | removeLiquidityETH | External ! | | NO! |
| | removeLiquidityWithPermit | External ! | | NO! |
| | removeLiquidityETHWithPermit | External ! | | NO! |
| | swapExactTokensForTokens | External ! | | NO! |
| | swapTokensForExactTokens | External ! | | NO! |
| | swapExactETHForTokens | External ! | | NO! |
| | swapTokensForExactETH | External ! | | NO! |
| | swapExactTokensForETH | External ! | | NO! |
| | swapETHForExactTokens | External ! | | NO! |
| | quote | External ! | | NO! |
| | getAmountOut | External ! | | NO! |
| | getAmountIn | External ! | | NO! |
| | getAmountsOut | External ! | | NO! |
| | getAmountsIn | External ! | | NO! |
| | | |
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 | | |
| | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | | NO! |
| | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | | NO! |
| | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | | NO! |
| | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | | NO! |
| | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | | NO! |
| | | |
| **IERC20Upgradeable** | Interface | | |
| | totalSupply | External ! | | NO! |
| | balanceOf | External ! | | NO! |
| | transfer | External ! | | NO! |
| | allowance | External ! | | NO! |
```



CONTRACT ASSESMENT

```
|  | approve | External ! |  | NO! |
|  | transferFrom | External ! |  | NO! |
|  |  |
|  |  |
| **IERC20MetadataUpgradeable** | Interface | IERC20Upgradeable |  |
|  | name | External ! |  | NO! |
|  | symbol | External ! |  | NO! |
|  | decimals | External ! |  | NO! |
|  |  |
|  |  |
| **Initializable** | Implementation |  |
|  |  |
| **ContextUpgradeable** | Implementation | Initializable |  |
|  | __Context_init | Internal  |  | initializer |
|  | __Context_init_unchained | Internal  |  | initializer |
|  | _msgSender | Internal  |  |
|  | _msgData | Internal  |  |
|  |  |
| **ERC20Upgradeable** | Implementation | Initializable, ContextUpgradeable, IERC20Upgradeable,
IERC20MetadataUpgradeable |  |
|  | __ERC20_init | Internal  |  | initializer |
|  | __ERC20_init_unchained | Internal  |  | initializer |
|  | name | Public ! |  | NO! |
|  | symbol | Public ! |  | NO! |
|  | decimals | Public ! |  | NO! |
|  | totalSupply | Public ! |  | NO! |
|  | balanceOf | Public ! |  | NO! |
|  | transfer | Public ! |  | NO! |
|  | allowance | Public ! |  | NO! |
|  | approve | Public ! |  | NO! |
|  | transferFrom | Public ! |  | NO! |
|  | increaseAllowance | Public ! |  | NO! |
|  | decreaseAllowance | Public ! |  | NO! |
|  | _transfer | Internal  |  |
|  | _mint | Internal  |  |
|  | _burn | Internal  |  |
|  | _approve | Internal  |  |
|  | _beforeTokenTransfer | Internal  |  |
|  | _afterTokenTransfer | Internal  |  |
|  |  |
|  |  |
| **OwnableUpgradeable** | Implementation | Initializable, ContextUpgradeable |  |
|  | __Ownable_init | Internal  |  | initializer |
|  | __Ownable_init_unchained | Internal  |  | initializer |
|  | owner | Public ! |  | NO! |
```



CONTRACT ASSESMENT

```
|  | renounceOwnership | Public ! |  | onlyOwner |
|  | transferOwnership | Public ! |  | onlyOwner |
|  | _setOwner | Private  |  |
|||||
| **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!|
|||||
| **SafeMathInt** | Library | |||
|  | mul | Internal  | |
|  | div | Internal  | |
|  | sub | Internal  | |
|  | add | Internal  | |
|  | abs | Internal  | |
|  | toUint256Safe | Internal  | |
|||||
```

CONTRACT ASSESMENT

```

| **SafeMathUint** | Library | ||| |
|  | toInt256Safe | Internal | | |
| |||||
| **IterableMapping** | Library | |||
|  | get | Internal | | |
|  | getIndexOfKey | Internal | | |
|  | getKeyAtIndex | Internal | | |
|  | size | Internal | | |
|  | set | Internal | | |
|  | remove | Internal | | |
| |||||
| **DividendPayingTokenInterface** | Interface | |||
|  | dividendOf | External | | |NO|
|  | withdrawDividend | External | | |NO|
| |||||
| **DividendPayingTokenOptionalInterface** | Interface | |||
|  | withdrawableDividendOf | External | | |NO|
|  | withdrawnDividendOf | External | | |NO|
|  | accumulativeDividendOf | External | | |NO|
| |||||
| **DividendPayingToken** | Implementation | ERC20Upgradeable, OwnableUpgradeable,
DividendPayingTokenInterface, DividendPayingTokenOptionalInterface |||
|  | __DividendPayingToken_init | Internal | | | | initializer |
|  | distributeCAKEDividends | Public | | | | onlyOwner |
|  | withdrawDividend | Public | | | |NO|
|  | _withdrawDividendOfUser | Internal | | | |
|  | dividendOf | Public | | | |NO|
|  | withdrawableDividendOf | Public | | | |NO|
|  | withdrawnDividendOf | Public | | | |NO|
|  | accumulativeDividendOf | Public | | | |NO|
|  | _transfer | Internal | | | |
|  | _mint | Internal | | | |
|  | _burn | Internal | | | |
|  | _setBalance | Internal | | | |
| |||||
| **BABYTOKENDividendTracker** | Implementation | OwnableUpgradeable, DividendPayingToken |||
|  | initialize | External | | | | initializer |
|  | _transfer | Internal | | | |
|  | withdrawDividend | Public | | | |NO|
|  | excludeFromDividends | External | | | | onlyOwner |
|  | isExcludedFromDividends | Public | | | |NO|
|  | updateClaimWait | External | | | | onlyOwner |

```


CONTRACT ASSESMENT













```

|  | updateMinimumTokenBalanceForDividends | External ! |  | onlyOwner | |
|  | getLastProcessedIndex | External ! | |NO! |
|  | getNumberOfTokenHolders | External ! | |NO! |
|  | getAccount | Public ! | |NO! |
|  | getAccountAtIndex | Public ! | |NO! |
|  | canAutoClaim | Private  | | |
|  | setBalance | External ! |  | onlyOwner |
|  | process | Public ! |  |NO! |
|  | processAccount | Public ! |  | onlyOwner |
|  |  |
|  |  |
|  | **BaseToken** | Implementation | | |
|  |  |
|  | **BABYTOKEN** | Implementation | ERC20, Ownable, BaseToken | | |
|  | <Constructor> | Public ! |  | ERC20 |
|  | <Receive Ether> | External ! |  |NO! |
|  | setSwapTokensAtAmount | External ! |  | onlyOwner |
|  | excludeFromFees | External ! |  | onlyOwner |
|  | excludeMultipleAccountsFromFees | External ! |  | onlyOwner |
|  | setMarketingWallet | External ! |  | onlyOwner |
|  | setTokenRewardsFee | External ! |  | onlyOwner |
|  | setLiquiditFee | External ! |  | onlyOwner |
|  | setMarketingFee | External ! |  | onlyOwner |
|  | _setAutomatedMarketMakerPair | Private  |  | |
|  | updateGasForProcessing | Public ! |  | onlyOwner |
|  | updateClaimWait | External ! |  | onlyOwner |
|  | getClaimWait | External ! | |NO! |
|  | updateMinimumTokenBalanceForDividends | External ! |  | onlyOwner |
|  | getMinimumTokenBalanceForDividends | External ! | |NO! |
|  | getTotalDividendsDistributed | External ! | |NO! |
|  | isExcludedFromFees | Public ! | |NO! |
|  | withdrawableDividendOf | Public ! | |NO! |
|  | dividendTokenBalanceOf | Public ! | |NO! |
|  | excludeFromDividends | External ! |  | onlyOwner |
|  | isExcludedFromDividends | Public ! | |NO! |
|  | getAccountDividendsInfo | External ! | |NO! |
|  | getAccountDividendsInfoAtIndex | External ! | |NO! |
|  | processDividendTracker | External ! |  |NO! |
|  | claim | External ! |  |NO! |
|  | getLastProcessedIndex | External ! | |NO! |
|  | getNumberOfDividendTokenHolders | External ! | |NO! |
|  | _transfer | Internal  |  | |



```



CONTRACT ASSESMENT

^L	swapAndSendToFee	Private 		
^L	swapAndLiquify	Private 		
^L	swapTokensForEth	Private 		
^L	swapTokensForCake	Private 		
^L	addLiquidity	Private 		
^L	swapAndSendDividends	Private 		

Legend

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

[illegible]

**Result => A static analysis of contract's source code has been performed using slither,
No major issues were found in the output**



FUNCTIONAL TESTING

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

All the functionalities have been tested, no issues were found

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0xce24bb9fce945d03dd024f5e314b4ba2cac31a241e5b269e534becfd6b493195>

2- Buying when excluded (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x6d68c089acbb901875077a8e51f9dfde6187fe71aadce2d349114ea5cc163a31>

3- Selling when excluded (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x0fbf92c14b8e3b8e36ff29a630c3536be9e0a4d32eb456acc3cb04b2d6f736>

4- Transferring when excluded (0% tax) (passed):

<https://testnet.bscscan.com/tx/0xe312c3c6490c48d51786bef729370276d3a27f96fab9eb90c8d987834a7a4c07>

5- Buying from a regular wallet (0-25% tax) (passed):

<https://testnet.bscscan.com/tx/0x1a3d0b3d749f8b71a7f4a72b8d38314de54e41e7949a04ea1433e2f2db23c60c>

6- Selling from a regular wallet (0-25% tax) (passed):

<https://testnet.bscscan.com/tx/0x848fde8a939209507ba21a969ec50953d1fa2ccaa3a8bc69a4cbe91fd589ef9b>



FUNCTIONAL TESTING

7- Transferring from a regular wallet (0-25% tax) (passed):

<https://testnet.bscscan.com/tx/0x69e8f3b5e3bb7fb92116beb4f1cb08996765502f387c4a0f7a01c1962434d79e>

8-Internal swap + rewards distribution + auto liquidity((passed):

<https://testnet.bscscan.com/tx/0x848fde8a939209507ba21a969ec50953d1fa2ccaa3a8bc69a4cbe91fd589ef9b>

ISSUES FOUND

Category: Centralization

Subject: Excessive fees

Severity: Medium

Overview:

Owner is able to set buy/sell/transfer each one up to 25%

Code:

```
function setTokenRewardsFee(uint256 value) external onlyOwner { ... }  
function setLiquiditFee(uint256 value) external onlyOwner { ... }  
function setMarketingFee(uint256 value) external onlyOwner { ... }
```

Suggestion:

Implement a limit for max amount of buy/sell/transfer fees.

Buy Fees ≤ 10

Sell Fees ≤ 10

Transfer Fees ≤ 10



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_



<https://github.com/Audit-Ace>
