auditace.tech

AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Smurfs Cat Dog

DATED : 19 September 23'

AUDIT SUMMARY

Project name – Smurfs Cat Dog

Date: 19 September 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	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1.Code Comparison:

We used specialized tools to perform a line-by-line comparison between the project's code and that of Uniswap V2 to identify any differences.

2.Differential Analysis:

Our audit team conducted a thorough review of the differentials to assess whether they introduce any security vulnerabilities or logical errors.

3.Additional Modules:

Any additional smart contracts, not part of the original Uniswap V2, were audited as separate entities, following our standard auditing procedures.

Token Information

Token Address :
0x8A0f8cC69Fd2e372cb39E749Af98c0EB92E1D3dC

Name: Smurfs Cat Dog

Symbol: SCATDOG

Decimals: 9

Network: Binance smart chain

Token Type: BEP20

Owner: 0x68d21F5acec12ea0e1E10F059a43c1A83c0160F5

Deployer: 0x68d21F5acec12ea0e1E10F059a43c1A83c0160F5

Token Supply: 100,000,000,000,000

Checksum:
ab673ab3b0b2ac9b227c0dc8ce447cbbed914f67

Testnet version:
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
https://testnet.bscscan.com/token/0x1C12927b65e7C87BBA00D00933Fa39B1bcC982CA

TOKEN OVERVIEW

Forked Codebase:

This project is an exact fork of Uniswap V2, a well-known and previously audited decentralized exchange. Due to the established reputation and multiple prior audits of Uniswap V2, our audit focused primarily on differences between this project and the original Uniswap V2 codebase.

Limitations

Reduced Depth of Review:

While Uniswap V2's codebase has been audited multiple times, it's important to note that our audit did not re-examine the original code in depth. Our focus was on identifying deviations and ensuring that those changes do not introduce new vulnerabilities.

Contextual Differences:

Even if the codebase is identical, the context in which the fork operates might differ, including user behavior, governance, or tokenomics, which are outside the scope of this audit.

Key Features:

1.Automated Market Making: Donswap utilizes an x * y = k formula for its AMM, where x and y are the amounts of two tokens in a liquidity pool, and k is a constant. This formula allows for efficient and low-slippage trading.

2.Decentralization: Being a DEX, Donswap is entirely decentralized, allowing users to maintain control over their assets at all times. There is no need for KYC (Know Your Customer) checks, and the code is open-source.

TOKEN OVERVIEW

3.Liquidity Provision: Users can become liquidity providers by depositing tokens in pairs, earning a share of the trading fees in return.

4.Token Swaps: Donswap supports direct ERC-20 to ERC-20 swaps

5.Routing: Donswap also offers multi-hop trades, routing through multiple pairs to optimize trading.

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

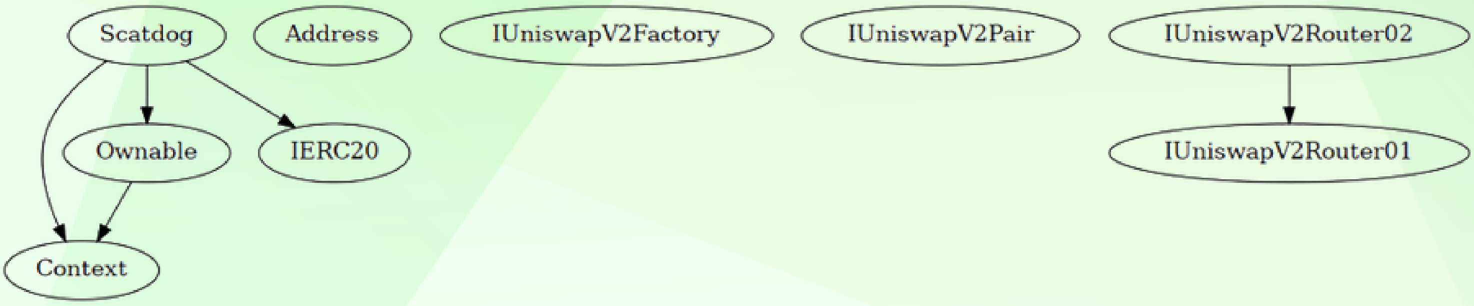
CLASSIFICATION OF RISK

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	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0

INHERITANCE TREE

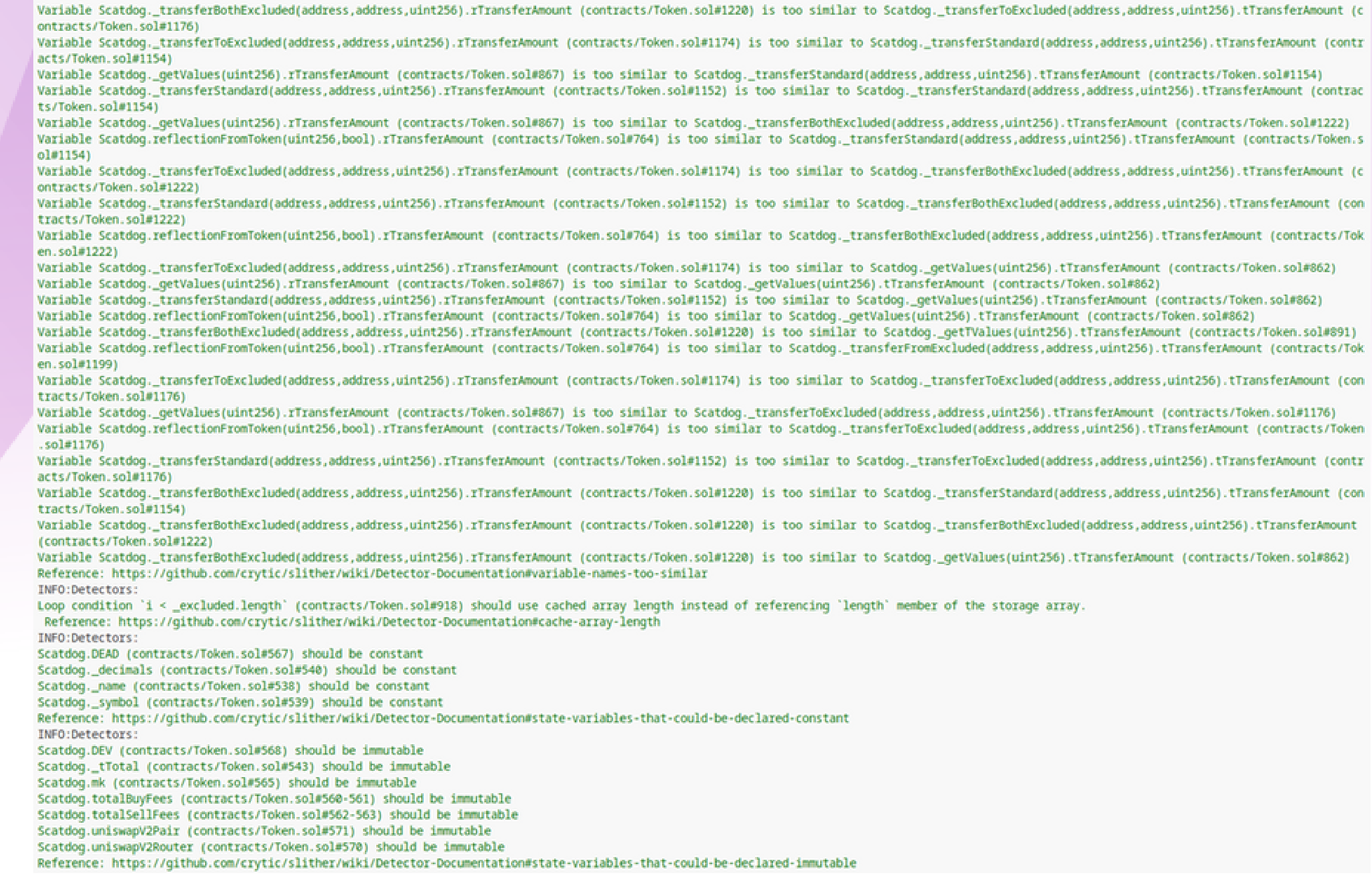


POINTS TO NOTE

- Owner is able to adjust buy/sell/transfer fees within 0-6%

- Owner is not able to blacklist an arbitrary wallet
- Owner is not able to disable trades
- Owner is not able to mint new tokens
- Owner is not able to set maximum wallet and maximum buy/sell/transfer limits

STATIC ANALYSIS



```
Variable Scatdog._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1220) is too similar to Scatdog._transferToExcluded(address,address,uint256).tTransferAmount (c
ontracts/Token.sol#1176)
Variable Scatdog._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1174) is too similar to Scatdog._transferStandard(address,address,uint256).tTransferAmount (contr
acts/Token.sol#1154)
Variable Scatdog._getValues(uint256).rTransferAmount (contracts/Token.sol#867) is too similar to Scatdog._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#1154)
Variable Scatdog._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1152) is too similar to Scatdog._transferStandard(address,address,uint256).tTransferAmount (contrac
ts/Token.sol#1154)
Variable Scatdog._getValues(uint256).rTransferAmount (contracts/Token.sol#867) is too similar to Scatdog._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1222)
Variable Scatdog.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#764) is too similar to Scatdog._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.s
ol#1154)
Variable Scatdog._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1174) is too similar to Scatdog._transferBothExcluded(address,address,uint256).tTransferAmount (c
ontracts/Token.sol#1222)
Variable Scatdog._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1152) is too similar to Scatdog._transferBothExcluded(address,address,uint256).tTransferAmount (con
tracts/Token.sol#1222)
Variable Scatdog.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#764) is too similar to Scatdog._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Tok
en.sol#1222)
Variable Scatdog._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1174) is too similar to Scatdog._getValues(uint256).tTransferAmount (contracts/Token.sol#862)
Variable Scatdog._getValues(uint256).rTransferAmount (contracts/Token.sol#867) is too similar to Scatdog._getValues(uint256).tTransferAmount (contracts/Token.sol#862)
Variable Scatdog._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1152) is too similar to Scatdog._getValues(uint256).tTransferAmount (contracts/Token.sol#862)
Variable Scatdog.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#764) is too similar to Scatdog._getValues(uint256).tTransferAmount (contracts/Token.sol#862)
Variable Scatdog._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1220) is too similar to Scatdog._getTValues(uint256).tTransferAmount (contracts/Token.sol#891)
Variable Scatdog.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#764) is too similar to Scatdog._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Tok
en.sol#1199)
Variable Scatdog._transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1174) is too similar to Scatdog._transferToExcluded(address,address,uint256).tTransferAmount (con
tracts/Token.sol#1176)
Variable Scatdog._getValues(uint256).rTransferAmount (contracts/Token.sol#867) is too similar to Scatdog._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#1176)
Variable Scatdog.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#764) is too similar to Scatdog._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token
.sol#1176)
Variable Scatdog._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#1152) is too similar to Scatdog._transferToExcluded(address,address,uint256).tTransferAmount (contr
acts/Token.sol#1176)
Variable Scatdog._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1220) is too similar to Scatdog._transferStandard(address,address,uint256).tTransferAmount (con
tracts/Token.sol#1154)
Variable Scatdog._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1220) is too similar to Scatdog._transferBothExcluded(address,address,uint256).tTransferAmount
(contracts/Token.sol#1222)
Variable Scatdog._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#1220) is too similar to Scatdog._getValues(uint256).tTransferAmount (contracts/Token.sol#862)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Loop condition `i < _excluded.length` (contracts/Token.sol#918) should use cached array length instead of referencing `length` member of the storage array.
 Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#cache-array-length
INFO:Detectors:
Scatdog.DEAD (contracts/Token.sol#567) should be constant
Scatdog._decimals (contracts/Token.sol#540) should be constant
Scatdog._name (contracts/Token.sol#538) should be constant
Scatdog._symbol (contracts/Token.sol#539) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
Scatdog.DEV (contracts/Token.sol#568) should be immutable
Scatdog._tTotal (contracts/Token.sol#543) should be immutable
Scatdog.mk (contracts/Token.sol#565) should be immutable
Scatdog.totalBuyFees (contracts/Token.sol#560-561) should be immutable
Scatdog.totalSellFees (contracts/Token.sol#562-563) should be immutable
Scatdog.uniswapV2Pair (contracts/Token.sol#571) should be immutable
Scatdog.uniswapV2Router (contracts/Token.sol#570) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

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

No major issues were found in the output

CONTRACT ASSESMENT

```
| Contract|      Type      |Bases     |                |              |
|:----------:|:-------------------:|:----------------:|:----------------:|:---------------:|
|    └| **Function Name** |**Visibility** | **Mutability** |**Modifiers** |
||||||
| **Context** | Implementation | |||
| └ | _msgSender | Internal 🔒 |  | |
| └ | _msgData | Internal 🔒 |  | |
||||||
| **Ownable** | Implementation | Context |||
| └ | <Constructor> | Public ❗ | 🛑|NO ❗ |
| └ | owner | Public ❗ |  |NO ❗ |
| └ | renounceOwnership | Public ❗ | 🛑| onlyOwner |
| └ | transferOwnership | Public ❗ | 🛑| onlyOwner |
||||||
| **IERC20** | Interface | |||
| └ | totalSupply | External ❗ |  |NO ❗ |
| └ | balanceOf | External ❗ |  |NO ❗ |
| └ | transfer | External ❗ | 🛑 |NO ❗ |
| └ | allowance | External ❗ |  |NO ❗ |
| └ | approve | External ❗ | 🛑 |NO ❗ |
| └ | transferFrom | External ❗ | 🛑|NO ❗ |
||||||
| **Address** | Library | |||
| └ | isContract | Internal 🔒 |  | |
| └ | sendValue | Internal 🔒 | 🛑| |
| └ | functionCall | Internal 🔒 | 🛑| |
| └ | functionCall | Internal 🔒 | 🛑 | |
| └ | functionCallWithValue | Internal 🔒 | 🛑 | |
| └ | functionCallWithValue | Internal 🔒 | 🛑 | |
| └ | _functionCallWithValue | Private 🔐 | 🛑 | |
```

CONTRACT ASSESMENT

```
||||||
| **IUniswapV2Factory** | Interface | |||
| └ | 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❗ |
| └ | burn | External ❗ | 🛑 |NO❗ |
| └ | swap | External ❗ | 🛑 |NO❗ |
| └ | skim | External ❗ | 🛑 |NO❗ |
| └ | sync | External ❗ | 🛑 |NO❗ |
| └ | initialize | External ❗ | 🛑|NO❗ |
```

CONTRACT ASSESMENT

```
| **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 ❗ |
||||||
| **Scatdog** | Implementation | Context, IERC20, Ownable |||
| └ | <Constructor> | Public ❗ | 🛑|NO ❗ |
| └ | name | Public ❗ | |NO ❗ |
| └ | symbol | Public ❗ | |NO ❗ |
| └ | decimals | Public ❗ | |NO ❗ |
| └ | totalSupply | Public ❗ | |NO ❗ |
```

CONTRACT ASSESMENT

```
| └ | balanceOf | Public ❗️ | |NO❗️ |
| └ | transfer | Public ❗️ | 🛑 |NO❗️ |
| └ | allowance | Public ❗️ | |NO❗️ |
| └ | approve | Public ❗️ | 🛑 |NO❗️ |
| └ | transferFrom | Public ❗️ | 🛑|NO❗️ |
| └ | increaseAllowance | Public ❗️ | 🛑|NO❗️ |
| └ | decreaseAllowance | Public ❗️ | 🛑 |NO❗️ |
| └ | isExcludedFromReward | Public ❗️ | |NO❗️ |
| └ | totalReflectionDistributed | Public ❗️ ||NO❗️ |
| └ | deliver | Public ❗️ | 🛑 |NO❗️ |
| └ | reflectionFromToken | Public ❗️ | |NO❗️ |
| └ | tokenFromReflection | Public ❗️ | |NO❗️ |
| └ | excludeFromReward | Public ❗️ | 🛑| onlyOwner |
| └ | includeInReward | External ❗️ | 🛑| onlyOwner |
| └ | <Receive Ether> | External ❗️ | 💵 |NO❗️ |
| └ | clearStuckTokens | External ❗️ | 🛑|NO❗️ |
| └ | updateFeeBuy | Public ❗️ | 🛑 | onlyOwner |
| └ | updateFeeSell | Public ❗️ | 🛑 | onlyOwner |
| └ | _reflectFee | Private 🔐 | 🛑| |
| └ | _getValues | Private 🔐 | | |
| └ | _getTValues | Private 🔐 | | |
| └ | _getRValues | Private 🔐 | | |
| └ | _getRate | Private 🔐 | | |
| └ | _getCurrentSupply | Private 🔐 || |
| └ | _takeLiquidity | Private 🔐 | 🛑| |
| └ | _takeMarketing | Private 🔐 | 🛑| |
| └ | calculateTaxFee | Private 🔐 | | |
| └ | calculateLiquidityFee | Private 🔐 || |
| └ | calculateMarketingFee | Private 🔐 || |
| └ | removeAllFee | Private 🔐 | 🛑| |
| └ | setBuyFee | Private 🔐 | 🛑| |
| └ | setSellFee | Private 🔐 | 🛑| |
| └ | isExcludedFromFee | Public ❗️ | |NO❗️ |
| └ | _approve | Private 🔐 | 🛑| |
| └ | _transfer | Private 🔐 | 🛑| |
| └ | swapAndLiquify | Private 🔐 | 🛑| |
| └ | swapAndSendMarketing | Private 🔐 | 🛑 | |
| └ | setSwapTokensAtAmount | External ❗️ | 🛑| onlyOwner |
| └ | setSwapEnabled | External ❗️ | 🛑| onlyOwner |
```

CONTRACT ASSESMENT

└	_tokenTransfer	Private 🔐	🛑	
└	_transferStandard	Private 🔐	🛑	
└	_transferToExcluded	Private 🔐	🛑	
└	_transferFromExcluded	Private 🔐	🛑	
└	_transferBothExcluded	Private 🔐	🛑	
└	excludeFromFees	External ❗	🛑	onlyOwner
└	isContract	Internal 🔒		

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

FUNCTIONAL TESTING

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x0344732a1ad02a918729130ae2c749c896342438b1e2be29d741b99d041c34ce

2- Buying when excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0x600db344591c634a84bc48da2878e392be01ede598b3095f5e58885b916d703e

3- Selling when excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0x62b3f0afd63e7e7fffceb2737f6fc12a06dd3be91164e2e7a917f3237cac0f14

4- Transferring when excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0xcf052eb691ae03576002cf855995356417ddef06edd9e4ff94a2dd9c8a4d72ec

5- Buying when not excluded from fees (0-6% tax) (passed):
https://testnet.bscscan.com/tx/0x4c4082fa9122027866cdde7b382a833518fe7e2538e764265c83e6e0a8ca83ef

6- Selling when not excluded from fees (0-6% tax) (passed):
https://testnet.bscscan.com/tx/0x95296bdb34c49c8728c4907cdd64e786cf326a4ce2acd85575af57490760f535

7- Transferring when not excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0xd790f5b565a9854b744821ceecb691d30734222506ab5d80379de75820e60eff

8- Internal swap (passed):
https://testnet.bscscan.com/tx/0x95296bdb34c49c8728c4907cdd64e786cf326a4ce2acd85575af57490760f535

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 specializes 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