



# Smart Contract Audit

FOR

**Diamond CEO**

DATED : 20 MAR 23'



# AUDIT SUMMARY

---

**Project name – DIAMOND CEO**

**Date:** 20 March, 2023

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

**Audit Status:** Passed

**Contract is developed by Pinksale safu dev**

## Issues Found

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

# USED TOOLS

---

## Tools:

### 1- Manual Review:

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

### 2- BSC Testnet network:

all tests were done on Bsc Testnet 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/token/0xab4be3eadc0c51bcbf4c45825f8d495ba97c8a14>

---



# Token Information

---

**Token Name :** Diamond CEO

**Token Symbol:** DIAMOND

**Decimals:** 9

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

**Token Address:**

0x4DE0822b0b2Eb431e7dd91c00deDBB872d61c35C

**Checksum:**

9225d27328b1d6419c72064383d062322e9e2390

**Owner:**

0x3D154fF09C916c987d54C9CBf49d4d01f11b262D

**Deployer:**

0x3D154fF09C916c987d54C9CBf49d4d01f11b262D

---



# TOKEN OVERVIEW

---

## **Fees:**

Buy Fees: 4%

Sell Fees: 4%

Transfer Fees: 0%

---

**Fees Privilege:** None

---

**Ownership :** Renounced

---

**Minting:** No mint function

---

**Max Tx Amount/ Max Wallet Amount:** No

---

**Blacklist:** No

---

**Other Privileges:** changing fee - excluding from  
rewards - including in rewards - changing swap  
threshold

---



# 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  |  <b>Gasless Send</b>           |
|  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

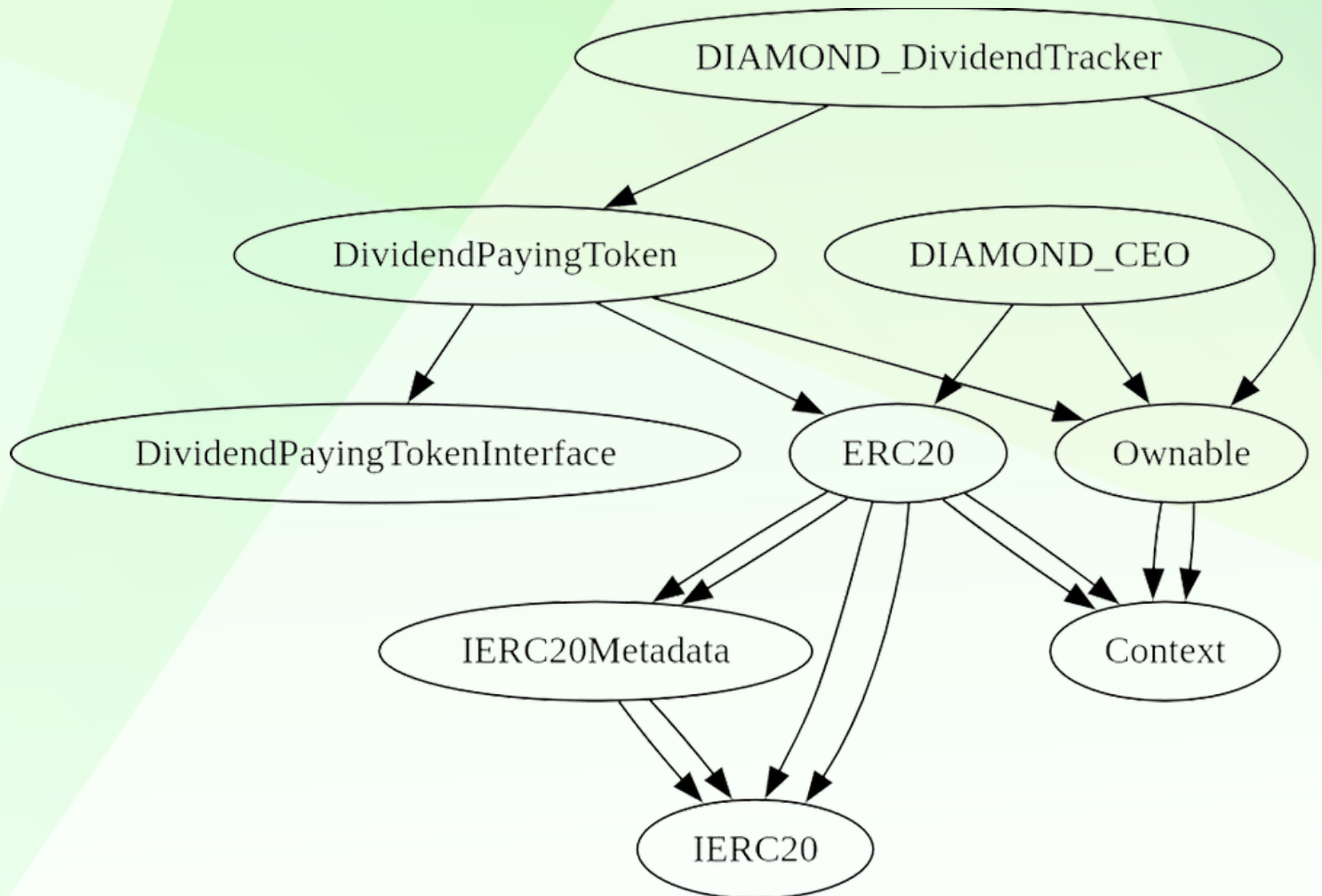
### Found

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



# INHERITANCE TREE

---



# POINTS TO NOTE

---

- Owner is not able to set buy/sell fees more than 12% (24% max fee)
  - Owner is not able to set transfer fees (0% always)
  - 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 is not able to mint new tokens
  - **Owner must enable trading for investors**
-

# CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
**Context**   Implementation					
L	_msgSender	Internal	🔒		
L	_msgData	Internal	🔒		
**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!
**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	_tokengeneration	Internal	🔒	🛑	
L	_burn	Internal	🔒	🛑	
L	_approve	Internal	🔒	🛑	
L	_beforeTokenTransfer	Internal	🔒	🛑	
**SafeMath**   Library					

# CONTRACT ASSESMENT

```

|  | add | Internal | | |
|  | sub | Internal | | |
|  | sub | Internal | | |
|  | mul | Internal | | |
|  | div | Internal | | |
|  | div | Internal | | |
|  | mod | Internal | | |
|  | mod | Internal | | |
| | | |
| **SafeMathInt** | Library | | |
|  | mul | Internal | | |
|  | div | Internal | | |
|  | sub | Internal | | |
|  | add | Internal | | |
|  | abs | Internal | | |
|  | toUint256Safe | Internal | | |
| | | |
| **SafeMathUint** | Library | | |
|  | toInt256Safe | Internal | | |
| | | |
| **Ownable** | Implementation | Context | | |
|  | <Constructor> | Public | | NO |
|  | owner | Public | | NO |
|  | renounceOwnership | Public | | onlyOwner |
|  | transferOwnership | Public | | onlyOwner |
| | | |
| **IPair** | Interface | | |
|  | sync | External | | NO |
| | | |
| **IFactory** | Interface | | |
|  | createPair | External | | NO |
|  | getPair | External | | NO |
| | | |
| **IRouter** | Interface | | |
|  | factory | External | | NO |
|  | WETH | External | | NO |
|  | addLiquidityETH | External | | NO |
|  | swapExactTokensForTokensSupportingFeeOnTransferTokens | External | | NO |
|  | swapExactETHForTokens | External | | NO |
|  | swapExactTokensForETHSupportingFeeOnTransferTokens | External | | NO |
| | | |
| **DividendPayingTokenInterface** | Interface | | |

```

# CONTRACT ASSESMENT

```

|  | dividendOf | External ! | | NO! |
|  | distributeDividends | External ! | | NO! |
|  | withdrawableDividendOf | External ! | | NO! |
|  | withdrawnDividendOf | External ! | | NO! |
|  | accumulativeDividendOf | External ! | | NO! |
|  |  |
| **DividendPayingToken** | Implementation | ERC20, DividendPayingTokenInterface, Ownable |||
|  | <Constructor> | Public ! | | ERC20 |
|  | <Receive Ether> | External ! | | NO! |
|  | distributeDividends | Public ! | | NO! |
|  | _withdrawDividendOfUser | Internal | | |
|  | setRewardToken | External ! | | onlyOwner |
|  | swapBnbForCustomToken | Internal | | |
|  | dividendOf | Public ! | | NO! |
|  | withdrawableDividendOf | Public ! | | NO! |
|  | withdrawnDividendOf | Public ! | | NO! |
|  | accumulativeDividendOf | Public ! | | NO! |
|  | _transfer | Internal | | |
|  | _tokengeneration | Internal | | |
|  | _burn | Internal | | |
|  | _setBalance | Internal | | |
|  |  |
| **IterableMapping** | Library | |||
|  | get | Internal | | |
|  | getIndexOfKey | Internal | | |
|  | getKeyAtIndex | Internal | | |
|  | size | Internal | | |
|  | set | Internal | | |
|  | remove | Internal | | |
|  |  |
| **Address** | Library | |||
|  | sendValue | Internal | | |
|  |  |
| **DIAMOND_CEO** | Implementation | ERC20, Ownable |||
|  | <Constructor> | Public ! | | ERC20 |
|  | <Receive Ether> | External ! | | NO! |
|  | updateDividendTracker | Public ! | | onlyOwner |
|  | processDividendTracker | External ! | | NO! |
|  | claim | External ! | | NO! |
|  | rescueBEP20Tokens | External ! | | onlyOwner |
|  | forceSend | External ! | | NO! |
|  | excludeFromFees | Public ! | | onlyOwner |

```

# CONTRACT ASSESMENT

```

| | excludeMultipleAccountsFromFees | Public ! | 🔴 | onlyOwner |
| | excludeFromDividends | External ! | 🔴 | onlyOwner |
| | setMarketingWallet | External ! | 🔴 | onlyOwner |
| | setSwapTokensAtAmount | External ! | 🔴 | onlyOwner |
| | setBuyTaxes | External ! | 🔴 | onlyOwner |
| | setSellTaxes | External ! | 🔴 | onlyOwner |
| | setSwapEnabled | External ! | 🔴 | onlyOwner |
| | enableTradingEnabled | External ! | 🔴 | onlyOwner |
| | setAntiBotBlocks | External ! | 🔴 | onlyOwner |
| | setMinBalanceForDividends | External ! | 🔴 | onlyOwner |
| | _setAutomatedMarketMakerPair | Private 🗑️ | 🔴 | |
| | setGasForProcessing | External ! | 🔴 | onlyOwner |
| | setClaimWait | External ! | 🔴 | onlyOwner |
| | getClaimWait | External ! | | NO! |
| | getTotalDividendsDistributed | External ! | | NO! |
| | isExcludedFromFees | Public ! | | NO! |
| | withdrawableDividendOf | Public ! | | NO! |
| | getCurrentRewardToken | External ! | | NO! |
| | dividendTokenBalanceOf | Public ! | | NO! |
| | getAccountDividendsInfo | External ! | | NO! |
| | getAccountDividendsInfoAtIndex | External ! | | NO! |
| | getLastProcessedIndex | External ! | | NO! |
| | getNumberOfDividendTokenHolders | External ! | | NO! |
| | _transfer | Internal 🗑️ | 🔴 | |
| | swapAndLiquify | Private 🗑️ | 🔴 | |
| | swapTokensForBNB | Private 🗑️ | 🔴 | |
| | addLiquidity | Private 🗑️ | 🔴 | |
| | | |
| | **DIAMOND_DividendTracker** | Implementation | Ownable, DividendPayingToken | |
| | <Constructor> | Public ! | 🔴 | DividendPayingToken |
| | _transfer | Internal 🗑️ | | |
| | setMinBalanceForDividends | External ! | 🔴 | onlyOwner |
| | excludeFromDividends | External ! | 🔴 | onlyOwner |
| | updateClaimWait | External ! | 🔴 | onlyOwner |
| | getLastProcessedIndex | External ! | | NO! |
| | getNumberOfTokenHolders | External ! | | NO! |
| | getCurrentRewardToken | External ! | | NO! |
| | getAccount | Public ! | | NO! |
| | getAccountAtIndex | Public ! | | NO! |
| | canAutoClaim | Private 🗑️ | | |
| | setBalance | Public ! | 🔴 | onlyOwner |




```





# CONTRACT ASSESMENT

```
|  | process | Public ! |  | NO ! |
|  | processAccount | Public ! |  | onlyOwner |
|  |  |
|  |  |
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |  |
|  | <Constructor> | Public ! |  | NO ! |
|  | 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  |  |  |
|  | _spendAllowance | Internal  |  |  |
|  | _beforeTokenTransfer | Internal  |  |  |
|  | _afterTokenTransfer | Internal  |  |  |
|  |  |
|  |  |
| **IERC20** | Interface |  |
|  | totalSupply | External ! |  | NO ! |
|  | balanceOf | External ! |  | NO ! |
|  | transfer | External ! |  | NO ! |
|  | allowance | External ! |  | NO ! |
|  | approve | External ! |  | NO ! |
|  | transferFrom | External ! |  | NO ! |
|  |  |
|  |  |
| **IERC20Metadata** | Interface | IERC20 |  |
|  | name | External ! |  | NO ! |
|  | symbol | External ! |  | NO ! |
|  | decimals | External ! |  | NO ! |
|  |  |
|  |  |
| **Context** | Implementation |  |
|  | _msgSender | Internal  |  |  |
|  | _msgData | Internal  |  |  |
|  |  |
|  |  |
| **Ownable** | Implementation | Context |  |
```

# CONTRACT ASSESMENT

```
| L | <Constructor> | Public ! |  | NO! |
| L | owner | Public ! | | NO! |
| L | _checkOwner | Internal  | | |
| L | renounceOwnership | Public ! |  | onlyOwner |
| L | transferOwnership | Public ! |  | onlyOwner |
| L | _transferOwnership | Internal  |  | |
| | | | |
| **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  | | |
```

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





# STATIC ANALYSIS

```
Function IRouter.WETH() (contracts/Token.sol#749) is not in mixedCase
Parameter DividendPayingToken.withdrawDividendOf(address). owner (contracts/Token.sol#965) is not in mixedCase
Parameter DividendPayingToken.withdrawDividendOf(address). owner (contracts/Token.sol#973) is not in mixedCase
Parameter DividendPayingToken.withdrawDividendOf(address). owner (contracts/Token.sol#982) is not in mixedCase
Parameter DividendPayingToken.accumulativeDividendOf(address). owner (contracts/Token.sol#993) is not in mixedCase
Constant DividendPayingToken.magnitude (contracts/Token.sol#839) is not in UPPER_CASE_WITH_UNDERSCORES
Contract DIAMOND_CEO (contracts/Token.sol#1144-1679) is not in CapWords
Parameter DIAMOND_CEO.setBuyTaxes(uint256,uint256,uint256). rewards (contracts/Token.sol#1359) is not in mixedCase
Parameter DIAMOND_CEO.setBuyTaxes(uint256,uint256,uint256). marketing (contracts/Token.sol#1360) is not in mixedCase
Parameter DIAMOND_CEO.setBuyTaxes(uint256,uint256,uint256). liquidity (contracts/Token.sol#1361) is not in mixedCase
Parameter DIAMOND_CEO.setSellTaxes(uint256,uint256,uint256). rewards (contracts/Token.sol#1371) is not in mixedCase
Parameter DIAMOND_CEO.setSellTaxes(uint256,uint256,uint256). marketing (contracts/Token.sol#1372) is not in mixedCase
Parameter DIAMOND_CEO.setSellTaxes(uint256,uint256,uint256). liquidity (contracts/Token.sol#1373) is not in mixedCase
Parameter DIAMOND_CEO.setSwapEnabled(bool). enabled (contracts/Token.sol#1384) is not in mixedCase
Constant DIAMOND_CEO.deadWallet (contracts/Token.sol#1157-1158) is not in UPPER_CASE_WITH_UNDERSCORES
Variable DIAMOND_CEO.isExcludedFromFees (contracts/Token.sol#1189) is not in mixedCase
Contract DIAMOND_DividendTracker (contracts/Token.sol#1681-1934) is not in CapWords
Parameter DIAMOND_DividendTracker.getAccount(address). account (contracts/Token.sol#1765) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#24)" inContext (contracts/Token.sol#18-27)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

Variable DividendPayingToken.withdrawDividendOfUser(address). withdrawableDividend (contracts/Token.sol#896) is too similar to DIAMOND_DividendTracker.getAccount(address).withdrawableDividends (contracts/Token.sol#1773)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

DIAMOND_CEO.setGasForProcessing(uint256) (contracts/Token.sol#1421-1432) uses literals with too many digits:
- require(bool,string)(newValue >= 200000 && newValue <= 500000,GasForProcessing must be between 200,000 and 500,000) (contracts/Token.sol#1422-1425)
DIAMOND_CEO.slitherConstructorVariables() (contracts/Token.sol#1144-1679) uses literals with too many digits:
- gasForProcessing = 300000 (contracts/Token.sol#1179)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

SafeMathInt.MAX_INT256 (contracts/Token.sol#603) is never used in SafeMathInt (contracts/Token.sol#601-658)
DIAMOND_CEO.currentRewardToken (contracts/Token.sol#1163) is never used in DIAMOND_CEO (contracts/Token.sol#1144-1679)
DIAMOND_CEO.lastSell (contracts/Token.sol#1185) is never used in DIAMOND_CEO (contracts/Token.sol#1144-1679)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable

DIAMOND_CEO.currentRewardToken (contracts/Token.sol#1163) should be constant
DIAMOND_CEO.launchtax (contracts/Token.sol#1187) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

DIAMOND_CEO.pair (contracts/Token.sol#1148) should be immutable
DIAMOND_CEO.router (contracts/Token.sol#1147) should be immutable
DividendPayingToken.router (contracts/Token.sol#841) 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 issues found**



# 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/0xc9380c3c46a798d099f911b6bf51685c1b47f338ed7da2585766041361c0a9c5>

### **2- Buying when excluded from fees (0% tax)(Passed):**

<https://testnet.bscscan.com/tx/0xe9051e37b311d522ffaa046ae5eef19a0faf20cbb300f2b2b19c7b51a9e1f6d7>

### **3- Selling when excluded from fees (0% tax)(Passed):**

<https://testnet.bscscan.com/tx/0xbea7884892b642161741cbe3d38d5c5ec63cad25300bf127e582a48572bd0237>

### **4- Transferring when excluded from fees (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0xb27bea61e044d44426d9f029623b0b40eba6b5e5fcbc5dab6dc3a650e16ff5b7>

### **5- Buying when not excluded from fees (upto 12% tax) (passed):**

<https://testnet.bscscan.com/tx/0x84ca80af7ae474f4108550acdce5f644eba765dbf0cfe43d99039db9a59d5c6b>

---



# FUNCTIONAL TESTING

---

## 6- Selling when not excluded from fees (up to 12% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xd91b2cf8764f37e1892326d0fb1d6021851d62df74a0e830cfc236d356c62787>

## 7- Transferring when not excluded from fees (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x370ff9cffccb358bc8829a53ac40a27df7adb88534962387e841ed465f6c68f1>

## 8- Internal swap (**passed**):

**As can seen in this transaction, marketing wallet received BNB**

<https://testnet.bscscan.com/address/0x7a73873727b99737456e305d8c567f39775d7d3b#internaltx>

## 9- Auto Liquidity (**passed**):

**Auto liquidity generated tokens are burnt, as can be seen in this transaction**

<https://testnet.bscscan.com/address/0x7a73873727b99737456e305d8c567f39775d7d3b#internaltx>

## 10- Distribution of rewards (**passed**):

**BUSD tokens are distributed between holders, this can be seen in this transaction**

<https://testnet.bscscan.com/address/0x7a73873727b99737456e305d8c567f39775d7d3b#internaltx>

---

# MANUAL TESTING

---

## Centralization - Owner must enable trading

**Severity:** High

**Function:** enable Trading Enabled

**Lines:** 1388-1392

**Status:** Resolved

**Overview:**

The owner must activate trading for investors to buy, sell, or transfer tokens. If trading remains disabled, token holders will be unable to trade their tokens.

```
function enableTradingEnabled() external onlyOwner {  
    require(!tradingEnabled, "Trading is already enabled");  
    tradingEnabled = true;  
    startTradingBlock = block.number;  
}
```

**Recommendation:**

Incorporate a safety mechanism that allows investors to activate trading if a specified duration has elapsed since the conclusion of the presale.

**Alleviation:**

Since the contract is owned by safu dev, enabling trades is guaranteed.



# 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://t.me/Audit_Ace)**



**[https://twitter.com/auditace\\_](https://twitter.com/auditace_)**



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

---