AuditAce
FROM INCEPTION TO SUCCESS

# Smart Contract Audit

FOR

# Skills 100

DATED : 08 Mar 23'

# AUDIT SUMMARY

**Project name** – Skills 100

**Date**: 08 March, 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 | 1 | 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/token/0x443a0Eca78bb506149AE747aA7659735aaD7E94E#readContract

# Token Information

**Token Name** : Skills 100

**Token Symbol**: S100

**Decimals:** 18

**Token Supply**: 100,000

**Token Address:**
0x09C0e2bC53A2bB2da18CDDe4b190FE585aF68b75

**Checksum:**
1f2fc18bc0c9d665cb1505a567a63130ac1fb09f

**Owner:**
0x3cb718c917749338f362b99dCC170Fe741057D3F
**(at time of writing the audit)**

# TOKEN OVERVIEW

**Fees:**

Buy Fees: 25% Currently

Sell Fees: 25% Currently

Transfer Fees: 25% Currently

**Fees Privilige:** Owner

**Ownership** : Owned

**Minting:** No mint function

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

**Blacklist:** No

**Other Priviliges**: including and excluding form fee - changing distirbution settings (min tokens to be eligible, cooldown between claims etc)

# 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

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

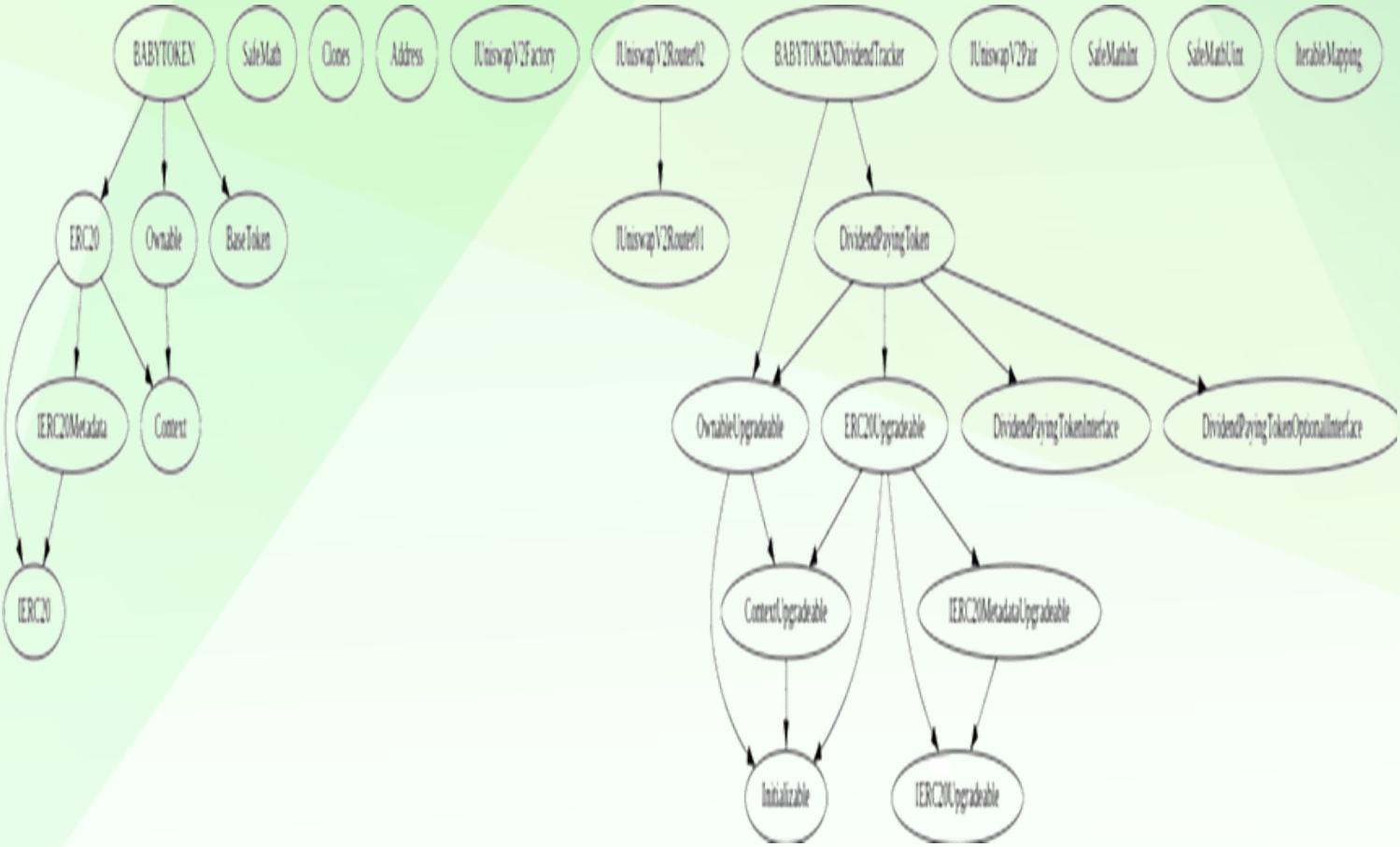
# CLASSIFICATION OF RISK

| 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 | 1 |
| Gas Optimization / Suggestions | 0 |

# INHERITANCE TREE



# OVERVIEW

This token has three different types of fees, which are used for marketing, maintaining liquidity, and providing rewards to holders. The fees collected are converted to a stablecoin called BUSD and sent to a marketing wallet. Another part of the fee is used to maintain liquidity and is sent to a dividend tracker to provide BUSD rewards to holders. Rewards are distributed to holders every time a buy, sell or transfer occurs, and can also be manually claimed from the BscScan website.

# POINTS TO NOTE

- Fees are currently 25% on buy/sell/transfers
- Owner is able to change buy/sell/transfer fees but sum of fees can not exceed 25% (however initial fee is more than this number)
- Contract is recognized as proxy in bscscan, however this is because dividend distributor is minimal proxy contract which is not upgradeable currently
- 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

# TOKEN DISTRIBUTION

It should be noted that the owner currently holds 100% of the total supply. However, information about the distribution of these tokens is not available, and it is recommended that investors exercise caution when considering this aspect.

# 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❗ |
| | | | | |
| **IERC20Metadata** | Interface | IERC20 | | |
| └ | name | External ❗ | | NO❗ |
| └ | symbol | External ❗ | | NO❗ |
| └ | decimals | External ❗ | | NO❗ |
| | | | | |
| **Context** | Implementation | | | |
| └ | _msgSender | Internal 🔒 | | |
| └ | _msgData | Internal 🔒 | | |
| | | | | |
| **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 🔒 | 🛑 | |
| └ | _beforeTokenTransfer | Internal 🔒 | 🛑 | |
| └ | _afterTokenTransfer | Internal 🔒 | 🛑 | |
| | | | | |
| **Ownable** | Implementation | Context | | |

# CONTRACT ASSESMENT

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

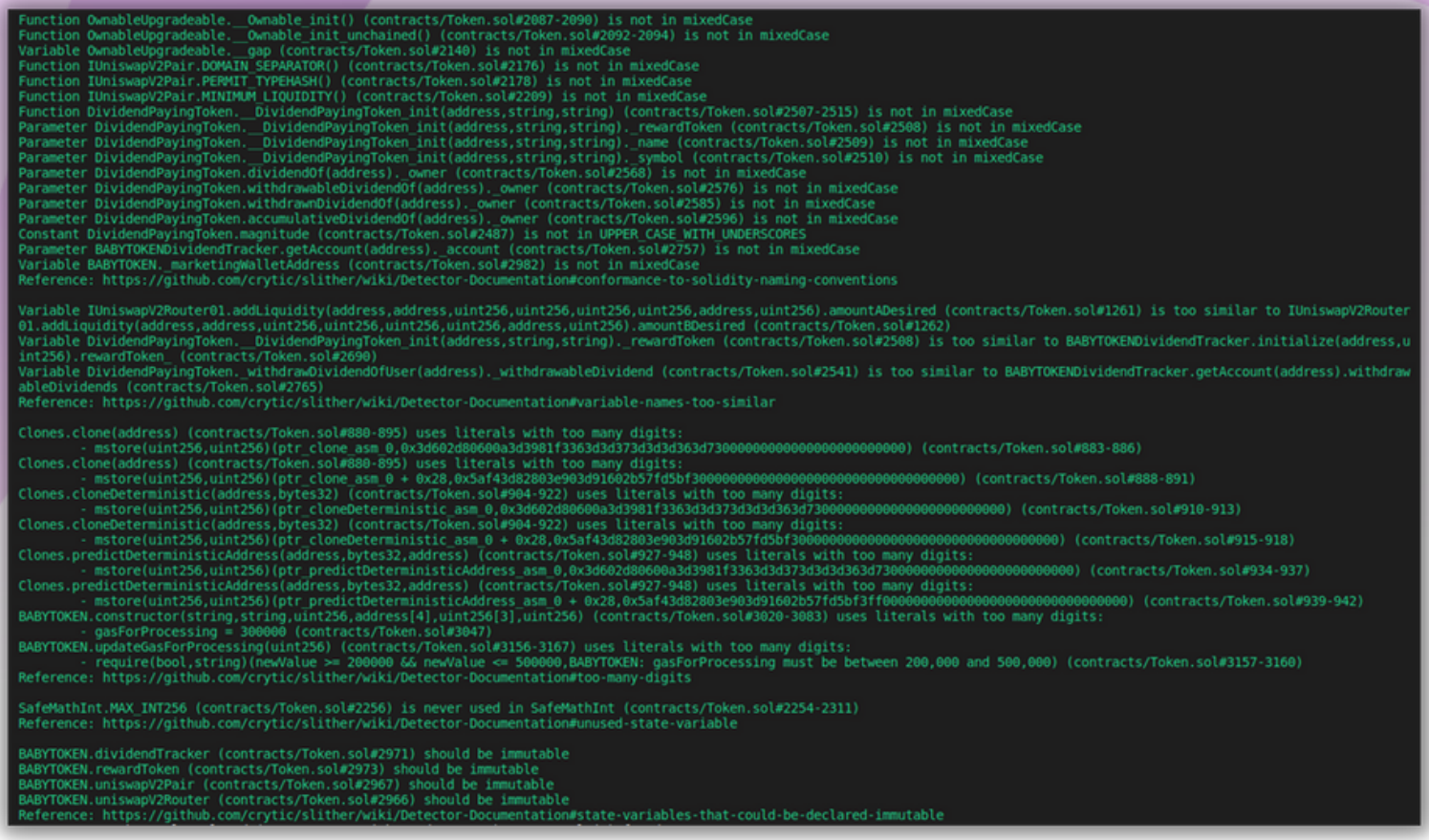
| └ | updateMinimumTokenBalanceForDividends | External ❗ | 🛑 | onlyOwner |
| └ | getLastProcessedIndex | External ❗ | | NO❗ |
| └ | getNumberOfTokenHolders | External ❗ | | NO❗ |
| └ | getAccount | Public ❗ | | NO❗ |
| └ | getAccountAtIndex | Public ❗ | | NO❗ |
| └ | canAutoClaim | Private 🔐 | | |
| └ | 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

| └ | swapAndSendToFee | Private 🔐 | 🛑 | |
| └ | swapAndLiquify | Private 🔐 | 🛑 | |
| └ | swapTokensForEth | Private 🔐 | 🛑 | |
| └ | swapTokensForCake | Private 🔐 | 🛑 | |
| └ | addLiquidity | Private 🔐 | 🛑 | |
| └ | swapAndSendDividends | Private 🔐 | 🛑 | |

| Symbol | Meaning |
|:--------:|----------|
| 🛑 | Function can modify state |
| 💵 | Function is payable |

# STATIC ANALYSIS



```
Function OwnableUpgradeable.__Ownable_init() (contracts/Token.sol#2087-2090) is not in mixedCase
Function OwnableUpgradeable.__Ownable_init_unchained() (contracts/Token.sol#2092-2094) is not in mixedCase
Variable OwnableUpgradeable.__gap (contracts/Token.sol#2140) is not in mixedCase
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (contracts/Token.sol#2176) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (contracts/Token.sol#2178) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (contracts/Token.sol#2209) is not in mixedCase
Function DividendPayingToken.__DividendPayingToken_init(address,string,string) (contracts/Token.sol#2507-2515) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._rewardToken (contracts/Token.sol#2508) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._name (contracts/Token.sol#2509) is not in mixedCase
Parameter DividendPayingToken.__DividendPayingToken_init(address,string,string)._symbol (contracts/Token.sol#2510) is not in mixedCase
Parameter DividendPayingToken.dividendOf(address)._owner (contracts/Token.sol#2568) is not in mixedCase
Parameter DividendPayingToken.withdrawableDividendOf(address)._owner (contracts/Token.sol#2576) is not in mixedCase
Parameter DividendPayingToken.withdrawnDividendOf(address)._owner (contracts/Token.sol#2585) is not in mixedCase
Parameter DividendPayingToken.accumulativeDividendOf(address)._owner (contracts/Token.sol#2596) is not in mixedCase
Constant DividendPayingToken.magnitude (contracts/Token.sol#2487) is not in UPPER_CASE_WITH_UNDERSCORES
Parameter BABYTOKENDividendTracker.getAccount(address)._account (contracts/Token.sol#2757) is not in mixedCase
Variable BABYTOKEN._marketingWalletAddress (contracts/Token.sol#2982) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#1261) is too similar to IUniswapV2Router
01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#1262)
Variable DividendPayingToken.__DividendPayingToken_init(address,string,string)._rewardToken (contracts/Token.sol#2508) is too similar to BABYTOKENDividendTracker.initialize(address,u
int256).rewardToken_ (contracts/Token.sol#2690)
Variable DividendPayingToken._withdrawDividendOfUser(address)._withdrawableDividend (contracts/Token.sol#2541) is too similar to BABYTOKENDividendTracker.getAccount(address).withdraw
ableDividends (contracts/Token.sol#2765)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

Clones.clone(address) (contracts/Token.sol#880-895) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_clone_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d7300000000000000000000000) (contracts/Token.sol#883-886)
Clones.clone(address) (contracts/Token.sol#880-895) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_clone_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3000000000000000000000000000000000) (contracts/Token.sol#888-891)
Clones.cloneDeterministic(address,bytes32) (contracts/Token.sol#904-922) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_cloneDeterministic_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d7300000000000000000000000) (contracts/Token.sol#910-913)
Clones.cloneDeterministic(address,bytes32) (contracts/Token.sol#904-922) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_cloneDeterministic_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3000000000000000000000000000000000) (contracts/Token.sol#915-918)
Clones.predictDeterministicAddress(address,bytes32,address) (contracts/Token.sol#927-948) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_predictDeterministicAddress_asm_0,0x3d602d80600a3d3981f3363d3d373d3d3d363d7300000000000000000000000) (contracts/Token.sol#934-937)
Clones.predictDeterministicAddress(address,bytes32,address) (contracts/Token.sol#927-948) uses literals with too many digits:
        - mstore(uint256,uint256)(ptr_predictDeterministicAddress_asm_0 + 0x28,0x5af43d82803e903d91602b57fd5bf3ff0000000000000000000000000000000000) (contracts/Token.sol#939-942)
BABYTOKEN.constructor(string,string,uint256,address[4],uint256[3],uint256) (contracts/Token.sol#3020-3083) uses literals with too many digits:
        - gasForProcessing = 300000 (contracts/Token.sol#3047)
BABYTOKEN.updateGasForProcessing(uint256) (contracts/Token.sol#3156-3167) uses literals with too many digits:
        - require(bool,string)(newValue >= 200000 && newValue <= 500000,BABYTOKEN: gasForProcessing must be between 200,000 and 500,000) (contracts/Token.sol#3157-3160)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

SafeMathInt.MAX_INT256 (contracts/Token.sol#2256) is never used in SafeMathInt (contracts/Token.sol#2254-2311)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable

BABYTOKEN.dividendTracker (contracts/Token.sol#2971) should be immutable
BABYTOKEN.rewardToken (contracts/Token.sol#2973) should be immutable
BABYTOKEN.uniswapV2Pair (contracts/Token.sol#2967) should be immutable
BABYTOKEN.uniswapV2Router (contracts/Token.sol#2966) 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**

# 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/0x38a1917661da7d7e321ad422799e23e3910cfc330b6b8e1c2aee941bf63b9615

**2- Buying when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0x7a11a88f56898ede5c755a818cb78025651bf441add628edf45f17e75d9f6598

**3- Selling when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0x2e3e2d75be52402cd9199fbccf452bf0d511a4e69f2a8fb66df6348efde6778b

**4- Transferring when excluded (0% tax) (passed):**
https://testnet.bscscan.com/tx/0xb26c4f1d9cd73ea4907080ec860c5ad7b36d9835d79bd5eb3125cd6bdfda8c83

# FUNCTIONAL TESTING

**5- Buying when not excluded from fees (25% tax) (passed):**
https://testnet.bscscan.com/tx/0xd1680de78c32da5d156474eff6fab11c6152132e194c1c333acca1222e9c4581

**6- Selling when not excluded from fees (25% tax) (passed):**
https://testnet.bscscan.com/tx/0x9245bf64d382d5f17e740338247eba549805847253c22b2259d99eea7c289194

**7- Transferring when not excluded from fees (25% tax) (passed):**
https://testnet.bscscan.com/tx/0x54070a16b9c7b56f447c511c5079827d448e326cc37052b33f42a08c761fccef

**8-Internal swap (passed):**
**marketing wallet received ETH**
https://testnet.bscscan.com/tx/0x9245bf64d382d5f17e740338247eba549805847253c22b2259d99eea7c289194

**9- Reflections (passed):**
as can seen in this transaction:
https://testnet.bscscan.com/tx/0x9245bf64d382d5f17e740338247eba549805847253c22b2259d99eea7c289194
distributor is sending BUSD to holders (auto distribution)

**10- Auto Liquidity (passed):**
https://testnet.bscscan.com/token/0x34e07586acbcd1046bb54102361c4187316711 56?a=0x000000000000000000000000000000000000dead

# MANUAL TESTING

## Low Risk Issue

IIssue: some ERC20 tokens may not return a boolean after transfer success

Type : **Logical**

Function: _withdrawDividendOfUser

Line: 2370 - 2380

Severity: Low

**Overview: Some ERC20 contracts may not support returning a boolean (true) if the transfer was successful**

```
function _withdrawDividendOfUser(
    address payable user
) internal returns (uint256) {
    uint256 _withdrawableDividend = withdrawableDividendOf(user);
    if ( withdrawableDividend > 0) {
        withdrawnDividends[user] = withdrawnDividends[user].add(
            _withdrawableDividend
        );
        emit DividendWithdrawn(user, _withdrawableDividend);
        bool success = IERC20(rewardToken).transfer( //@audit use safeTransfer to transfer tokens
            user,
            _withdrawableDividend
        );

        if (!success) {
            withdrawnDividends[user] = withdrawnDividends[user].sub(
                _withdrawableDividend
            );
            return 0;
        }
```

### Recommendations

use SafeERC20 to handle token transfers

# Social Media Overview

**Here are the Social Media Accounts of**

Skills 100

**https://t.me/s100_token**

**https://twitter.com/S100_token**


**https://skills100.net/**

# 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**