



# Smart Contract Audit

FOR

Luffy op

DATED : 25 MAR 23'



# AUDIT SUMMARY

---

**Project name** – Luffy op

**Date:** 25 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	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 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/0x7eb2bf681cc3f6055fe960053cf4dfde957988f4>

---



# Token Information

---

**Token Name :** Luffy op

**Token Symbol:** Luffy op

**Decimals:** 9

**Token Supply:** 10,000,000,000,000,000,000,000,000,000

**Token Address:**

0xb4ef1dB8cd4969189146a17BE5874fAf7968F162

**Checksum:**

19ce8b1d6cbea46ac0f5ba96100710d6561d8bc9

**Owner:**

0x00

**(renounced)**

---



# TOKEN OVERVIEW

---

## **Fees:**

Buy Fees: 9%

Sell Fees: 9%

Transfer Fees: 9%

---

**Fees Privilege:** None

---

**Ownership :** Renounced

---

**Minting:** No mint function

---

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

---

**Blacklist:** No

---

**Other Privileges:** None (ownership renounced)

---



# 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

0

### ◆ Low-Risk

0

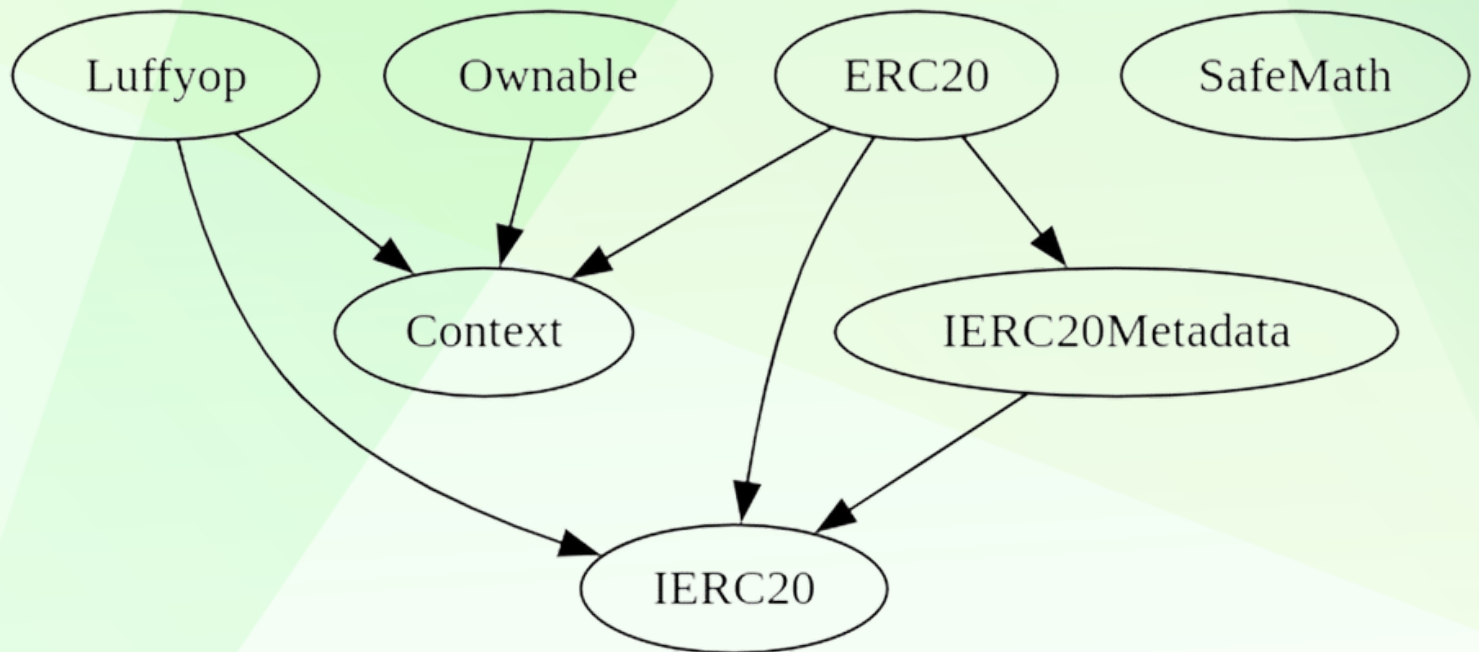
### ◆ Gas Optimization / Suggestions

0



# INHERITANCE TREE

---



# POINTS TO NOTE

---

- **Ownership is renounced, meaning owner has not control over the contract functions**
  - **Owner is not able to modify buy/sell/transfer fees (9% for each)**
  - **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**
-



# CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	<b>**Modifiers**</b>	
	<b>**IERC20**</b>	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!
	<b>**SafeMath**</b>	Library			
L	add	Internal	🔒		
L	sub	Internal	🔒		
L	mul	Internal	🔒		
L	div	Internal	🔒		
L	sub	Internal	🔒		
L	div	Internal	🔒		
	<b>**Context**</b>	Implementation			
L	_msgSender	Internal	🔒		
L	_msgData	Internal	🔒		
	<b>**Address**</b>	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	Private	🔒		
	<b>**IUniswapV2Factory**</b>	Interface			
L	feeTo	External	!	NO!	
L	feeToSetter	External	!	NO!	
L	getPair	External	!	NO!	
L	allPairs	External	!	NO!	



# CONTRACT ASSESMENT

```
| | 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! |
| | | |
| **IUniswapV2Router01** | Interface | | |
| | factory | External ! | | NO! |
| | WETH | External ! | | NO! |
| | addLiquidity | External ! | | NO! |
| | addLiquidityETH | External ! | | NO! |
| | removeLiquidity | External ! | | NO! |
| | removeLiquidityETH | External ! | | NO! |
| | removeLiquidityWithPermit | External ! | | NO! |
```

# CONTRACT ASSESMENT

```
| 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! |
| | | | |
| **Luffyop** | Implementation | Context, IERC20 | | |
| L | owner | Public ! | | NO! |
| L | renounceOwnership | Public ! |  | NO! |
| 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 | <Receive Ether> | External ! |  | NO! |
| L | _getCurrentSupply | Private  | | |
| L | _approve | Private  |  | |
| L | _transfer | Private  |  | |
| L | sendToWallet | Private  |  | |
| L | swapAndLiquify | Private  |  | lockTheSwap |
```

# CONTRACT ASSESMENT

```

|  | swapTokensForBNB | Private |  |  | |
|  | addLiquidity | Private |  |  | |
|  | remove_Random_Tokens | Public |  |  | NO! |
|  | _tokenTransfer | Private |  |  | |
|  |  |  |  |  |  |
| **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 |  | | |

```

# CONTRACT ASSESMENT

```
||||| |
| **Ownable** | Implementation | Context |||
|  | <Constructor> | Public ! |  | NO! |
|  | owner | Public ! |  | NO! |
|  | _checkOwner | Internal  |  |
|  | renounceOwnership | Public ! |  | onlyOwner |
|  | transferOwnership | Public ! |  | onlyOwner |
|  | _transferOwnership | Internal  |  |
|||||
| **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  |  |
| Symbol | Meaning |
|:-----:|-----|
|  | Function can modify state |
|  | Function is payable |
```



```

Reentrancy in Luffypop: transferFrom(address,address,uint256) (contracts/Token.sol#672-687):
  External calls:
    - _transfer(sender,recipient,amount) (contracts/Token.sol#677)
      - wallet.transfer(amount) (contracts/Token.sol#783)
  External calls sending eth:
    - _transfer(sender,recipient,amount) (contracts/Token.sol#677)
      - wallet.transfer(amount) (contracts/Token.sol#783)
      - uniswapV2Router.addLiquidityETH(value: BNBAmount)(address(this),tokenAmount,0,0,Wallet_Burn,block.timestamp) (contracts/Token.sol#831-838)
  State variables written after the call(s):
    - _approve(sender, msgSender(), allowances[sender][ msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (contracts/Token.sol#678-685)
      - allowances[theOwner][theSpender] = amount (contracts/Token.sol#731)
  Event emitted after the call(s):
    - Approval(theOwner,theSpender,amount) (contracts/Token.sol#732)
      - _approve(sender, msgSender(), allowances[sender][ msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (contracts/Token.sol#678-685)
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-4

Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#358) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#359)
Variable Luffypop.swapAndLiquify(uint256).tokens_to_D (contracts/Token.sol#792) is too similar to Luffypop.swapAndLiquify(uint256).tokens_to_M (contracts/Token.sol#791)
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#variable-names-too-similar

Luffypop.slitherConstructorVariables() (contracts/Token.sol#546-886) uses literals with too many digits:
  - _tTotal = 100000000000000 * 10 ** 6 * 10 ** 6 * 10 ** 6 * 10 ** 6 decimals (contracts/Token.sol#580-581)
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#too-many-digits

Luffypop.MAX (contracts/Token.sol#578) is never used in Luffypop (contracts/Token.sol#546-886)
Luffypop.previousMaxWalletToken (contracts/Token.sol#593) is never used in Luffypop (contracts/Token.sol#546-886)
Luffypop.previousMaxTxAmount (contracts/Token.sol#595) is never used in Luffypop (contracts/Token.sol#546-886)
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#unused-state-variable

Luffypop.Percent_AutoLP (contracts/Token.sol#591) should be constant
Luffypop.Percent_Burn (contracts/Token.sol#590) should be constant
Luffypop.Percent_Dev (contracts/Token.sol#589) should be constant
Luffypop.Percent_Marketing (contracts/Token.sol#588) should be constant
Luffypop.Wallet_Dev (contracts/Token.sol#574-575) should be constant
Luffypop.Wallet_Marketing (contracts/Token.sol#572-573) should be constant
Luffypop.Tax_On_Buy (contracts/Token.sol#586) should be constant
Luffypop.Tax_On_Sell (contracts/Token.sol#587) should be constant
Luffypop.swapAndLiquifyEnabled (contracts/Token.sol#599) should be constant
Luffypop.swapTrigger (contracts/Token.sol#585) should be constant
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

Luffypop.maxTxAmount (contracts/Token.sol#594) should be immutable
Luffypop.maxWalletToken (contracts/Token.sol#592) should be immutable
Luffypop.previousMaxTxAmount (contracts/Token.sol#595) should be immutable
Luffypop.previousMaxWalletToken (contracts/Token.sol#593) should be immutable
Luffypop.uniswapV2Pair (contracts/Token.sol#597) should be immutable
Luffypop.uniswapV2Router (contracts/Token.sol#596) should be immutable
Reference: https://github.com/cryptic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable

```

## No issues found





# FUNCTIONAL TESTING

---

## Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

### 1- Adding Liquidity (**Passed**):

liquidity added on Pancakeswap V2:

<https://testnet.bscscan.com/tx/0x500149db927f0f8aa609667f4a96a1d06f8652df2bdd41c1946c1bf49aaf77ef>

### 2- Buying when trading not enabled (owner% )(**Passed**):

<https://testnet.bscscan.com/tx/0x9263fbb988402e34832a1a54b7e6dc1362b86e690b693c254972ba90ee8ddb9f>

### 3- Selling when trading not enabled (0% )(**Passed**):

<https://testnet.bscscan.com/tx/0x4cf7fd2a3bb6f24f536c8e905021f0f2eb75262b1fa668dfe078ecbfd254b295>

### 4- Transferring when trading not enabled (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xe4d828bf612389f2012b4260f71a4189679b014311ac64d51e558c347d7df754>

### 5- Buying when trading enabled (9% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xda4c3d6a821092ae1ee0a488e3670107645c55e5844a1bcdde0bc3238266f7d5>

---



# FUNCTIONAL TESTING

---

## 6- Selling when trading enabled (9% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x6d84d23abc9a7bea39472cbc2a9f9d9d72df257a751da68ede8cd9219b806069>

## 7- Transferring when trading enabled (9% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xe0a4bd14ef2bc75f71f42763b3dd47a5af13e6bde15bf5930cd779268ba45c15>

---



# MANUAL TESTING

---

## No Issues Found





# 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>**

---