



Smart Contract Audit

FOR

Oggy CEO

DATED : 17 April 23'



AUDIT SUMMARY

Project name – Oggy CEO

Date: 17 April, 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	2
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 :

The code has undergone static analysis using Slither.

Testnet Link:

<https://testnet.bscscan.com/token/0x5A2D3100e84E1930f4c14852Fe88cda0fDE429A6>



Token Information

Token Name : Oggy CEO

Token Symbol: OGGYCEO

Decimals: 9

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

Token Address:

0xCa84d3644582a300A57822Ff6680751eA500c7F1

Checksum:

e428d8bf84fdb64e4e18f03c32ef1ebfd5fe6353

Owner:

0x24ceBc6B4f2e9772394515aa273742D0593ACB3B
(at time of audit)



TOKEN OVERVIEW

Fees:

Buy Fees: 10%

Sell Fees: 10%

Transfer Fees: 10%

Fees Privilege: None

Ownership: Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: including and excluding form fee



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

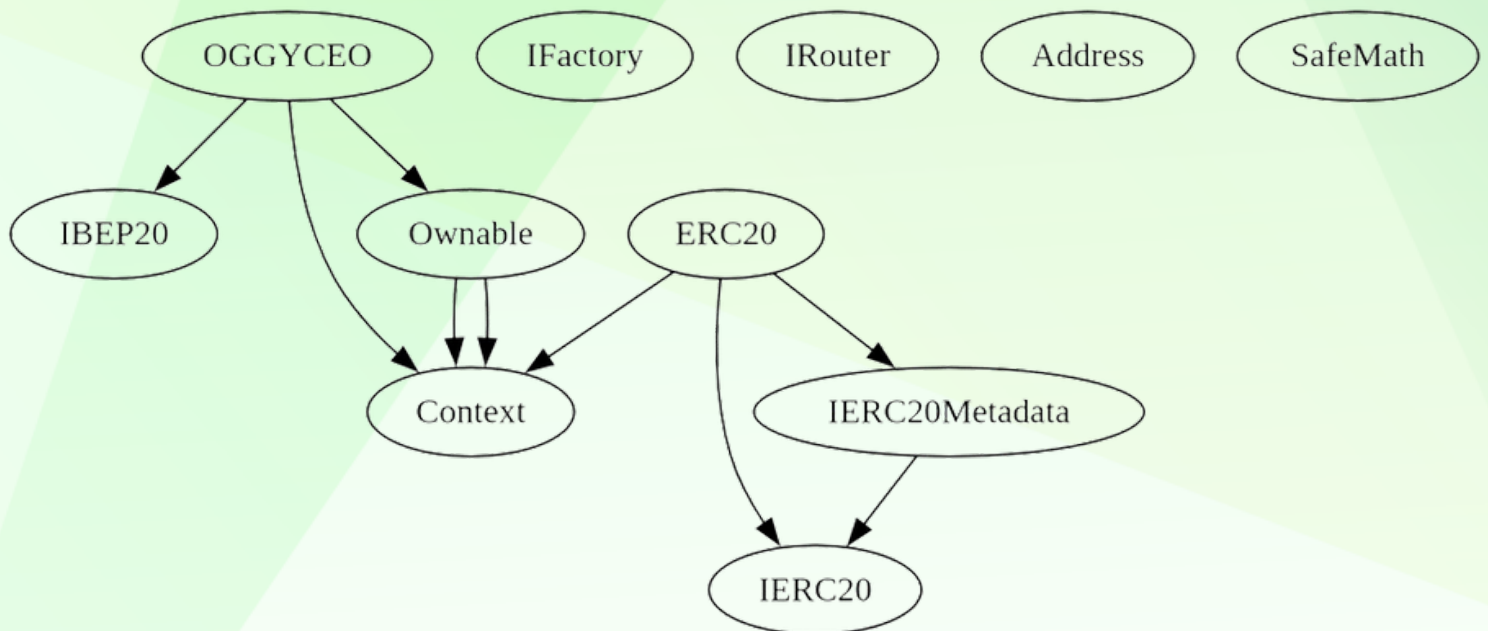
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

2

INHERITANCE TREE





POINTS TO NOTE

- **Owner is not able to modify fees (10% buy/sell/transfers)**
 - **Owner must enable trading for investors to be able to trade**
 - **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			
:-----: :-----: :-----: :-----: :-----:					
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
IBEP20 Interface					
└	totalSupply	External	!		NO !
└	balanceOf	External	!		NO !
└	transfer	External	!		NO !
└	allowance	External	!		NO !
└	approve	External	!		NO !
└	transferFrom	External	!		NO !
Context Implementation					
└	_msgSender	Internal	🔒		
└	_msgData	Internal	🔒		
Ownable Implementation Context					
└	<Constructor>	Public	!		NO !
└	owner	Public	!		NO !
└	renounceOwnership	Public	!		onlyOwner
└	_setOwner	Private	🔒		
IFactory Interface					
└	createPair	External	!		NO !
IRouter Interface					
└	factory	External	!		NO !
└	WETH	External	!		NO !
└	addLiquidityETH	External	!		\$📦 NO !
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External	!		NO !
Address Library					
└	sendValue	Internal	🔒		
OGGYCEO Implementation Context, IBEP20, Ownable					
└	<Constructor>	Public	!		NO !
└	name	Public	!		NO !
└	symbol	Public	!		NO !
└	decimals	Public	!		NO !
└	totalSupply	Public	!		NO !
└	balanceOf	Public	!		NO !
└	allowance	Public	!		NO !
└	approve	Public	!		NO !
└	transferFrom	Public	!		NO !

CONTRACT ASSESMENT

```

└─ increaseAllowance | Public ! | ● |NO ! |
└─ decreaseAllowance | Public ! | ● |NO ! |
└─ transfer | Public ! | ● |NO ! |
└─ isExcludedFromReward | Public ! | |NO ! |
└─ reflectionFromToken | Public ! | |NO ! |
└─ tokenFromReflection | Public ! | |NO ! |
└─ excludeFromReward | Public ! | ● |onlyOwner |
└─ includeInReward | External ! | ● |onlyOwner |
└─ excludeFromFee | Public ! | ● |onlyOwner |
└─ includeInFee | Public ! | ● |onlyOwner |
└─ isExcludedFromFee | Public ! | |NO ! |
└─ _reflectRfi | Private 🔒 | ● |
└─ _takeMarketing | Private 🔒 | ● |
└─ _getValues | Private 🔒 | |
└─ _getTValues | Private 🔒 | |
└─ _getRValues | Private 🔒 | |
└─ _getRate | Private 🔒 | |
└─ _getCurrentSupply | Private 🔒 | |
└─ _approve | Private 🔒 | ● |
└─ _transfer | Private 🔒 | ● |
└─ _tokenTransfer | Private 🔒 | ● |
└─ swapAndLiquify | Private 🔒 | ● |lockTheSwap |
└─ swapTokensForBNB | Private 🔒 | ● |
└─ bulkExcludeFee | External ! | ● |onlyOwner |
└─ <Receive Ether> | External ! | 💰 |NO ! |
|||||
**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 🔒 | ● |

```

CONTRACT ASSESMENT

```

└| _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 |||
└| <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 | 🔒 | | |

```



CONTRACT ASSESMENT

	L		mod		Internal	🔒			
	Symbol		Meaning						
	:	-----	:	-----					
	●		Function can modify state						
	💰		Function is payable						



STATIC ANALYSIS

```
Reentrancy in OGGYCEO.transferFrom(address,address,uint256) (contracts/Token.sol#223-235):
  External calls:
    - _transfer(sender,recipient,amount) (contracts/Token.sol#228)
      - (success) = recipient.call{value: amount}{} (contracts/Token.sol#108)
      - router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (contracts/Token.sol#504-510)
      - address(marketingWallet).sendValue(deltaBalance) (contracts/Token.sol#490)
  External calls sending eth:
    - _transfer(sender,recipient,amount) (contracts/Token.sol#228)
      - (success) = recipient.call{value: amount}{} (contracts/Token.sol#108)
  Event emitted after the call(s):
    - Approval(owner,spender,amount) (contracts/Token.sol#424)
      - _approve(sender,msgSender(),currentAllowance - amount) (contracts/Token.sol#232)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

OGGYCEO.includeInReward(address) (contracts/Token.sol#294-305) has costly operations inside a loop:
  - _excluded.pop() (contracts/Token.sol#301)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop

Context._msgData() (contracts/Token.sol#35-38) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

OGGYCEO._rTotal (contracts/Token.sol#133) is set pre-construction with a non-constant function or state variable:
  - (MAX - (MAX % _rTotal))
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state

Pragma version^0.8.17 (contracts/Token.sol#6) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#105-110):
  - (success) = recipient.call{value: amount}{} (contracts/Token.sol#108)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IRouter.WETH() (contracts/Token.sol#77) is not in mixedCase
Struct OGGYCEO.valuesFromGetValues (contracts/Token.sol#157-165) is not in CapWords
Constant OGGYCEO._decimals (contracts/Token.sol#129) is not in UPPER_CASE_WITH_UNDERSCORES
Constant OGGYCEO._name (contracts/Token.sol#140) is not in UPPER_CASE_WITH_UNDERSCORES
Constant OGGYCEO._symbol (contracts/Token.sol#141) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#36)" inContext (contracts/Token.sol#30-39)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

OGGYCEO._tTotal (contracts/Token.sol#132) should be constant
OGGYCEO.deadWallet (contracts/Token.sol#137) should be constant
OGGYCEO.marketingWallet (contracts/Token.sol#138) should be constant
OGGYCEO.swapTokensAtAmount (contracts/Token.sol#135) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

OGGYCEO.pair (contracts/Token.sol#127) should be immutable
OGGYCEO.router (contracts/Token.sol#126) 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, and no issues were found

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0xedc709076d64c727549c47baa2a688081b9ee3a8646bd623f87d42c674a2c856>

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

<https://testnet.bscscan.com/tx/0x94bd19952dc2cf63b62311514cce7eaae6bdb93a8990849085d79f0f6928b4dd>

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

<https://testnet.bscscan.com/tx/0xc5b2fc26719411d78ea751bcb004ed235bf5a98ab5496d0a48e045e5226a4b1c>

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

<https://testnet.bscscan.com/tx/0xe9d4a01dd91594a226eaa750f5da9fb69d1e5c3a75890552da9c89ec36d8ae18>

5- Buying when not excluded from fees (10% tax) (passed):

<https://testnet.bscscan.com/tx/0x49d66fa5e73d57b4bff8317a4ed574e70e4b15a51680edb295157ccf17b39434>



FUNCTIONAL TESTING

6- Selling when not excluded from fees (10% tax) (passed):

[https://testnet.bscscan.com/tx/0x1deac479b2b66a7f99204fa4cca
b72342f45bda6cd81ce882f1c0b7c5174416d](https://testnet.bscscan.com/tx/0x1deac479b2b66a7f99204fa4cca
b72342f45bda6cd81ce882f1c0b7c5174416d)

7- Transferring when not excluded from fees (10% tax) (passed):

[https://testnet.bscscan.com/tx/0x38a40bb063e706b03209f1b1d7
7a6234a00b79ef0107602c68dbfd8a75d0d4bd](https://testnet.bscscan.com/tx/0x38a40bb063e706b03209f1b1d7
7a6234a00b79ef0107602c68dbfd8a75d0d4bd)

8- Internal swap (passed):

marketing wallet received Rewards

[https://testnet.bscscan.com/address/0x24cebc6b4f2e9772394515
aa273742d0593acb3b#internaltx](https://testnet.bscscan.com/address/0x24cebc6b4f2e9772394515
aa273742d0593acb3b#internaltx)



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.

MANUAL TESTING

Informational – No functions to change swap threshold

Overview:

Current implementation of the contract doesn't have a function to change swap threshold. Based on different market conditions and liquidity pool size, owner might need to change the swap threshold.

Recommendation:

Add a function that allows owner to change internal swap threshold





MANUAL TESTING

Informational – Lack of token/bnb withdraw function

Overview:

Current implementation of the contract doesn't have a function to withdraw stuck tokens or BNB. If some amount of tokens or BNB were sent to the contract by mistake, there are no ways to recover them.

Recommendation:

Add a function that allows owner to remove tokens of any address from the contract





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>
