auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

POPEYE

DATED : 12 MAY 23'

AUDIT SUMMARY

Project name – POPEYE

Date: 12 May, 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	1	0	1	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1.Manual Review: The code has undergone a line-by-line review by the **Ace** team.

2.BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3.Slither: The code has undergone static analysis using Slither.

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/address/0x8D839024595a12a0ae2C74C916cE26AA0d553aeC#code

Token Information

Name : Popeye Inu

Symbol : POPEYE

Decimals: 9

Network: BSC

Token Type: BEP20

Token Address :
0x8E3e73648D628d45eBa551C36BCa4D21B7294765

Owner:
0x27315c169C1A254C652877Dcf60A27BAEB515F85
(at time of writing the audit)

Deployer:0x27315c169C1A254C652877Dcf60A27BAEB515F85

Token Information

Fees:

Buy Fees: 10%

Sell Fees: 10%

Transfer Fees: 10%

Fees Privilige: None

Ownership : Owned

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Priviliges:Changing swap threshold - enabling trades

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

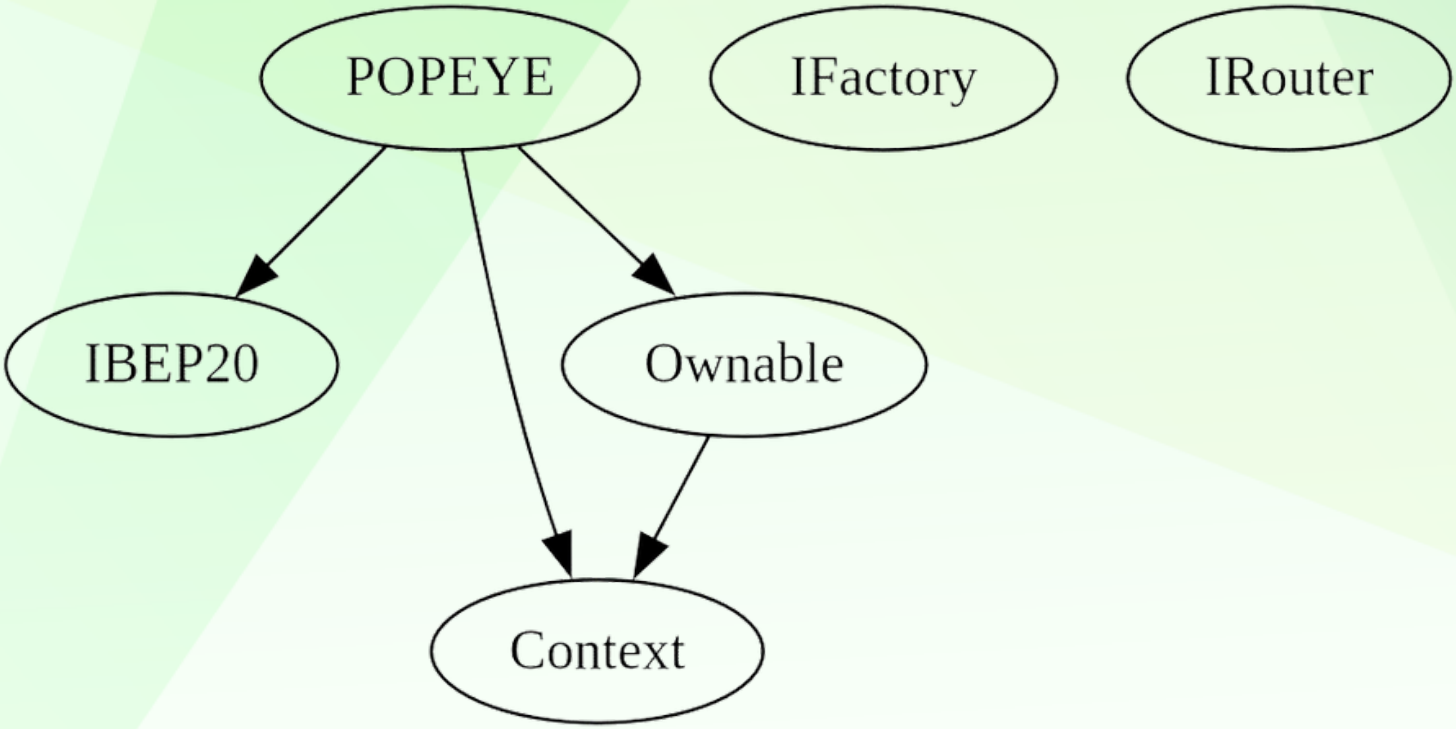
CLASSIFICATION OF RISK

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	1
High-Risk	0
Medium-Risk	1
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



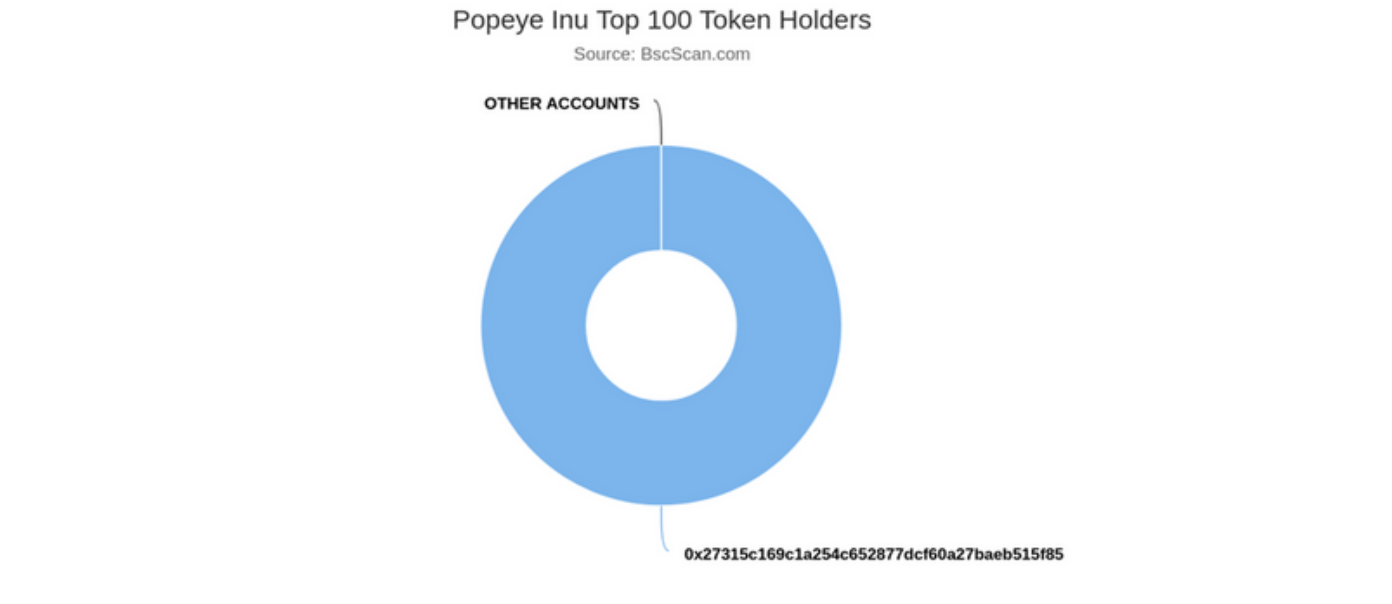
POINTS TO NOTE

- Owner is not able to change fees (10% for each type of tax)
- Owner is not able to blacklist an arbitrary address.
- Owner is not able to disable trades
- Owner is able to set max buy/sell/transfer/hold amount to 0
- Owner is not able to mint new tokens
- **Owner must enable trades manually**

TOKENOMICS AT TIME OF AUDIT

The top 100 holders collectively own 100.00% (420,000,000,000,000,000.00 Tokens) of Popeye Inu

Token Total Supply: 420,000,000,000,000,000.00 Token | Total Token Holders: 1



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
└	transferOwnership	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 🔒	🛑		
POPEYE	Implementation	Context, IBEP20, Ownable			
└	<Constructor>	Public ❗	🛑	NO ❗

CONTRACT ASSESMENT

└	name	Public ❗		|NO ❗
└	symbol	Public ❗		|NO ❗
└	decimals	Public ❗		|NO ❗
└	totalSupply	Public ❗		|NO ❗
└	balanceOf	Public ❗		|NO ❗
└	allowance	Public ❗		|NO ❗
└	approve	Public ❗	🛑	|NO ❗
└	transferFrom	Public ❗	🛑	|NO ❗
└	increaseAllowance	Public ❗	🛑	|NO ❗
└	decreaseAllowance	Public ❗	🛑	|NO ❗
└	transfer	Public ❗	🛑	|NO ❗
└	isExcludedFromReward	Public ❗		|NO ❗
└	reflectionFromToken	Public ❗		|NO ❗
└	EnableTrading	External ❗	🛑	onlyOwner
└	updatedeadline	External ❗	🛑	onlyOwner
└	tokenFromReflection	Public ❗		|NO ❗
└	excludeFromReward	Public ❗	🛑	onlyOwner
└	includeInReward	External ❗	🛑	onlyOwner
└	excludeFromFee	Public ❗	🛑	onlyOwner
└	includeInFee	Public ❗	🛑	onlyOwner
└	isExcludedFromFee	Public ❗		|NO ❗
└	_reflectRfi	Private 🔐	🛑	
└	_takeLiquidity	Private 🔐	🛑	
└	_takeMarketing	Private 🔐	🛑	
└	_takeOps	Private 🔐	🛑	
└	_takeDev	Private 🔐	🛑	
└	_getValues	Private 🔐		
└	_getTValues	Private 🔐		
└	_getRValues1	Private 🔐		
└	_getRValues2	Private 🔐		
└	_getRate	Private 🔐		
└	_getCurrentSupply	Private 🔐		
└	_approve	Private 🔐	🛑	
└	_transfer	Private 🔐	🛑	
└	_tokenTransfer	Private 🔐	🛑	

CONTRACT ASSESMENT

└	swapAndLiquify	Private 🔐	🛑	lockTheSwap
└	addLiquidity	Private 🔐	🛑	
└	swapTokensForBNB	Private 🔐	🛑	
└	bulkExcludeFee	External ❗	🛑	onlyOwner
└	updateMarketingWallet	External ❗	🛑	onlyOwner
└	updateDevWallet	External ❗	🛑	onlyOwner
└	updateOpsWallet	External ❗	🛑	onlyOwner
└	updateSwapTokensAtAmount	External ❗	🛑	onlyOwner
└	updateSwapEnabled	External ❗	🛑	onlyOwner
└	rescueBNB	External ❗	🛑	onlyOwner
└	rescueAnyBEP20Tokens	Public ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

POPEYE.includeInReward(address) (contracts/Token.sol#404-415) has costly operations inside a loop:
        - _excluded.pop() (contracts/Token.sol#411)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#costly-operations-inside-a-loop

Context._msgData() (contracts/Token.sol#46-49) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

POPEYE._rTotal (contracts/Token.sol#165) is set pre-construction with a non-constant function or state variable:
        - (MAX - (MAX % _tTotal))
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state

Pragma version^0.8.19 (contracts/Token.sol#7) 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#126-137):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#132)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Function IRouter.WETH() (contracts/Token.sol#102) is not in mixedCase
Struct POPEYE.valuesFromGetValues (contracts/Token.sol#202-216) is not in CapWords
Function POPEYE.EnableTrading() (contracts/Token.sol#370-375) is not in mixedCase
Parameter POPEYE.updatedeadline(uint256)._deadline (contracts/Token.sol#377) is not in mixedCase
Parameter POPEYE.updateSwapEnabled(bool)._enabled (contracts/Token.sol#793) is not in mixedCase
Parameter POPEYE.rescueAnyBEP20Tokens(address,address,uint256)._tokenAddr (contracts/Token.sol#805) is not in mixedCase
Parameter POPEYE.rescueAnyBEP20Tokens(address,address,uint256)._to (contracts/Token.sol#806) is not in mixedCase
Parameter POPEYE.rescueAnyBEP20Tokens(address,address,uint256)._amount (contracts/Token.sol#807) is not in mixedCase
Constant POPEYE._decimals (contracts/Token.sol#161) is not in UPPER_CASE_WITH_UNDERSCORES
Variable POPEYE.genesis_block (contracts/Token.sol#169) is not in mixedCase
Constant POPEYE._name (contracts/Token.sol#177) is not in UPPER_CASE_WITH_UNDERSCORES
Constant POPEYE._symbol (contracts/Token.sol#178) 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#47)" inContext (contracts/Token.sol#41-50)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

POPEYE._lastSell (contracts/Token.sol#156) is never used in POPEYE (contracts/Token.sol#140-817)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable

POPEYE._tTotal (contracts/Token.sol#164) should be constant
POPEYE.deadWallet (contracts/Token.sol#172) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

POPEYE.pair (contracts/Token.sol#159) should be immutable
POPEYE.router (contracts/Token.sol#158) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

Static Analysis

an static analysis of the code were performed using slither. No issues were found

FUNCTIONAL TESTING

Router (PCS V2):
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x9c4d0c5a0cd202e42aad97fc2c94920742ed72524b234d6e9c4214c788f9e08c

2- Buying when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xbff898d64a58c0f756917f5573035ed9b6c44a49927c247821549bf44f677c2c

3- Selling when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x9af288f44f4196f7828684038efd950d1c7312f3ac6d7649c91dfcf2e3db9751

4- Transferring when excluded from fees (0% tax) (passed):
https://testnet.bscscan.com/tx/0xf216bf4b3078553104ac13022dbc9852362073564affca99a497815a572caf19

5- Buying when not excluded from fees (10% tax) (passed):
https://testnet.bscscan.com/tx/0x18224a429f64d7e93ef87c6775459bb71cac42dca10e0054a4b7d90486cfa63f

6- Selling when not excluded from fees (10% tax) (passed):
https://testnet.bscscan.com/tx/0xd287b70719cc5cb17bef6100266e64d0c83861fcb274f388b345f833f81c1676

7- Transferring when not excluded from fees (10% tax) (passed):
https://testnet.bscscan.com/tx/0x4fce40632ff3b54e456c7df8a548a0fcbff733ed0bbdb28fbf1f56c7ec89e988

FUNCTIONAL TESTING

8- Internal swap (marketing wallet received BNB) (passed):
https://testnet.bscscan.com/address/0x44f0e0c1b54c85430f74577362154ea9dcd727fd#internaltx

FUNCTIONAL TESTING

Logical – 0 swap threshold can disable trades

Severity: Critical
Function: updateSwapTokensAtAmount
Status: Not Resolved
Overview:
if swapTokensAtAmount is set to 0, internal swap would be failed due to a division by zero error. (swapAndLiquify function)

```
function updateSwapTokensAtAmount(uint256 amount) external
onlyOwner {
require(
amount <= 42e14,
"Cannot set swap threshold amount higher than 1% of tokens"
);
swapTokensAtAmount = amount * 10 ** _decimals;
  }
```

Suggestion
To mitigate this Logical issue, make sure that swapTokensAtAmount is always greater than 0

```
function updateSwapTokensAtAmount(uint256 amount) external
onlyOwner {
require(
amount <= 42e14,
"Cannot set swap threshold amount higher than 1% of tokens"
);
require(
amount >= 42e12,
```

FUNCTIONAL TESTING

```
"Cannot set swap threshold amount higher than 0.01% of tokens"
);
swapTokensAtAmount = amount * 10 ** _decimals;
   }
```

FUNCTIONAL TESTING

Centralization – Trades must be enabled

Severity: Medium
function: EnableTrading
Status: Not Resolved
Overview:
The smart contract owner must enable trades for holders. If trading remain disabled, no one would be able to buy/sell/transfer tokens.

```
function EnableTrading() external onlyOwner {
require(!tradingEnabled, "Cannot re-enable trading");
tradingEnabled = true;
swapEnabled = true;
genesis_block = block.number;
  }
```

Suggestion
To mitigate this centralization issue, we propose the following options:

1. Renounce Ownership: Consider relinquishing control of the smart contract by renouncing ownership. This would remove the ability for a single entity to manipulate the router, reducing centralization risks.
2. Multi-signature Wallet: Transfer ownership to a multi-signature wallet. This would require multiple approvals for any changes to the mainRouter, adding an additional layer of security and reducing the centralization risk.
3. Transfer ownership to a trusted and valid 3rd party in order to guarantee enabling of the trades

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