



Smart Contract Audit

FOR

PEPEWOJAK CEO

DATED : 02 May 23'



AUDIT SUMMARY

Project name – PEPEWOJAK CEO

Date: 02 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	0	2	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 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/0xa3bf26981739b56c3e476b38b97baa6c2be0bb8a>



Token Information

Token Name : PEPEWOJAK CEO

Token Symbol: PEPEWOJAK

Decimals: 9

Token Supply:420,690,000,000,000

Token Address:

0xfC12Ae55e3429a6fAA48A17f161711fA0FFdA759

Checksum:

7b0d6058387825c26af841b8913f24278a52984c

Owner:

0xe43b2eeb67A9Ed947262C62972acBB43F55Bb451

Deployer:

0xe43b2eeb67A9Ed947262C62972acBB43F55Bb451



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: updating liquidity threshold -
excluding from fees - including in fees - including in
rewards - excluding from rewards

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.

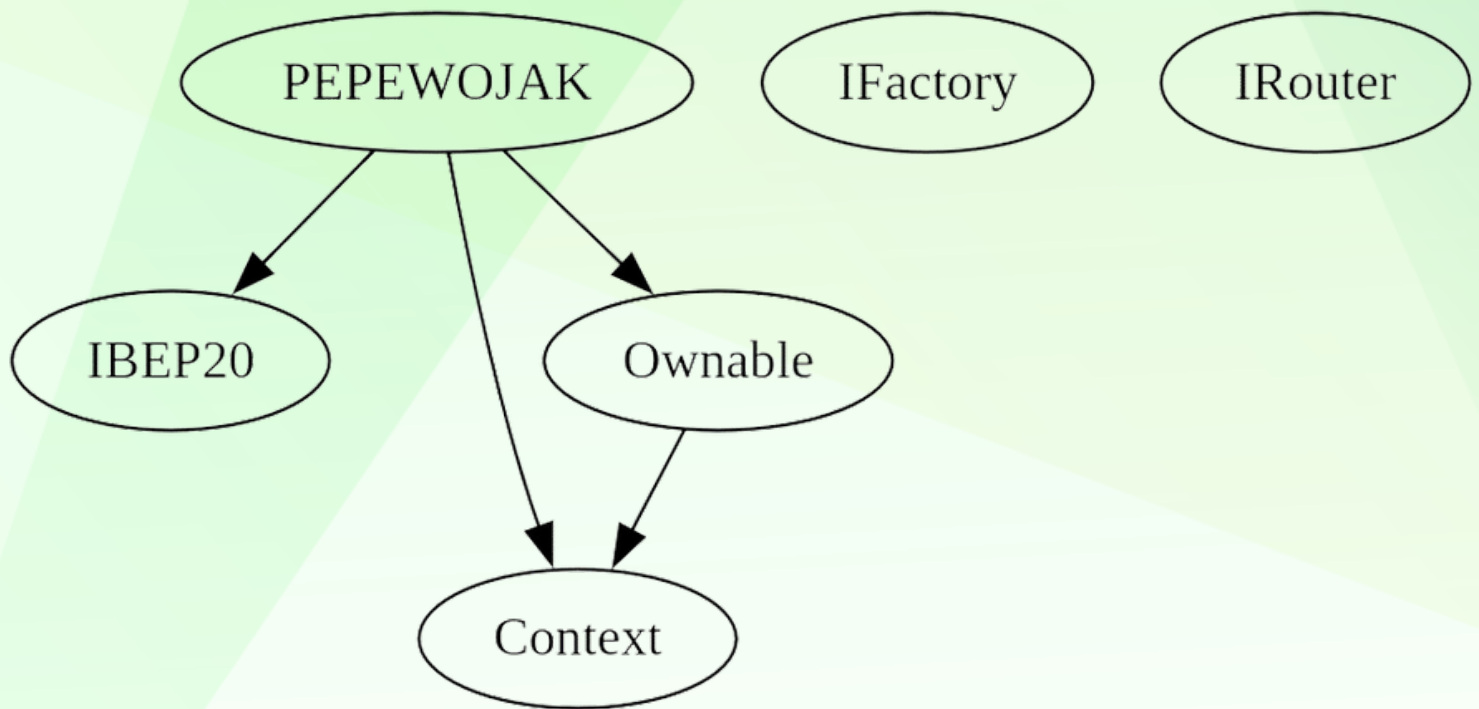
Findings

Severity

Found

◆ Critical	0
◆ High-Risk	2
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0

INHERITANCE TREE


















































POINTS TO NOTE

- Owner is not able to modify buy/sell/transfer fees (10% each)
 - **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
 - Owner is able to set a max wallet amount but not less than 1% of supply
-

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	🔒			
PEPEWOJAK	Implementation	Context, IBEP20, Ownable			
└─ <Constructor>	Public	!	NO!		
└─ name	Public	!	NO!		
└─ symbol	Public	!	NO!		
└─ decimals	Public	!	NO!		
└─ totalSupply	Public	!	NO!		
└─ balanceOf	Public	!	NO!		

CONTRACT ASSESMENT



\angle	allowance	Public !		NO !
\angle	approve	Public !		NO !
\angle	transferFrom	Public !		NO !
\angle	increaseAllowance	Public !		NO !
\angle	decreaseAllowance	Public !		NO !
\angle	transfer	Public !		NO !
\angle	isExcludedFromReward	Public !		NO !
\angle	reflectionFromToken	Public !		NO !
\angle	EnableTrading	External !		onlyOwner
\angle	updatedDeadline	External !		onlyOwner
\angle	tokenFromReflection	Public !		NO !
\angle	excludeFromReward	Public !		onlyOwner
\angle	includeInReward	External !		onlyOwner
\angle	excludeFromFee	Public !		onlyOwner
\angle	includeInFee	Public !		onlyOwner
\angle	isExcludedFromFee	Public !		NO !
\angle	_reflectRfi	Private 		
\angle	_takeLiquidity	Private 		
\angle	_takeMarketing	Private 		
\angle	_takeOps	Private 		
\angle	_takeDev	Private 		
\angle	_getValues	Private 		
\angle	_getTValues	Private 		
\angle	_getRValues1	Private 		
\angle	_getRValues2	Private 		
\angle	_getRate	Private 		
\angle	_getCurrentSupply	Private 		
\angle	_approve	Private 		
\angle	_transfer	Private 		
\angle	_tokenTransfer	Private 		
\angle	swapAndLiquify	Private 		lockTheSwap
\angle	addLiquidity	Private 		
\angle	swapTokensForBNB	Private 		
\angle	bulkExcludeFee	External !		onlyOwner
\angle	updateMarketingWallet	External !		onlyOwner
\angle	updateDevWallet	External !		onlyOwner
\angle	updateOpsWallet	External !		onlyOwner
\angle	updateSwapTokensAtAmount	External !		onlyOwner
\angle	updateMaxTxLimit	External !		onlyOwner
\angle	updateSwapEnabled	External !		onlyOwner
\angle	rescueBNB	External !		onlyOwner



CONTRACT ASSESMENT

| ^L | rescueAnyBEP20Tokens | Public  |  | onlyOwner |
| ^L | <Receive Ether> | External  |  | NO  |

Legend

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



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.



STATIC ANALYSIS

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code>

PEPEWOJAK._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^0.8.17 (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 PEPEWOJAK.valuesFromGetValues (contracts/Token.sol#203-217) is not in CapWords
Function PEPEWOJAK.EnableTrading() (contracts/Token.sol#371-376) is not in mixedCase
Parameter PEPEWOJAK.updatedDeadline(uint256)._deadline (contracts/Token.sol#378) is not in mixedCase
Parameter PEPEWOJAK.updateSwapEnabled(bool)._enabled (contracts/Token.sol#823) is not in mixedCase
Parameter PEPEWOJAK.rescueAnyBEP20Tokens(address,address,uint256)._tokenAddr (contracts/Token.sol#835) is not in mixedCase
Parameter PEPEWOJAK.rescueAnyBEP20Tokens(address,address,uint256)._to (contracts/Token.sol#836) is not in mixedCase
Parameter PEPEWOJAK.rescueAnyBEP20Tokens(address,address,uint256)._amount (contracts/Token.sol#837) is not in mixedCase
Constant PEPEWOJAK._decimals (contracts/Token.sol#161) is not in UPPER_CASE_WITH_UNDERSCORES
Variable PEPEWOJAK.genesis_block (contracts/Token.sol#170) is not in mixedCase
Constant PEPEWOJAK._name (contracts/Token.sol#178) is not in UPPER_CASE_WITH_UNDERSCORES
Constant PEPEWOJAK._symbol (contracts/Token.sol#179) 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>

PEPEWOJAK.updateSwapTokensAtAmount(uint256) (contracts/Token.sol#807-813) uses literals with too many digits:
- require(bool,string)(amount <= 4206900000000, Cannot set swap threshold amount higher than 1% of tokens) (contracts/Token.sol#808-811)
PEPEWOJAK.updateMaxTxLimit(uint256) (contracts/Token.sol#815-821) uses literals with too many digits:
- require(bool,string)(maxWallet >= 4206900000000, Cannot set max wallet amount lower than 1% of tokens) (contracts/Token.sol#816-819)
PEPEWOJAK.slitherConstructorVariables() (contracts/Token.sol#140-847) uses literals with too many digits:
- _tTotal = 420690000000000 * 10 ** _decimals (contracts/Token.sol#164)
PEPEWOJAK.slitherConstructorVariables() (contracts/Token.sol#140-847) uses literals with too many digits:
- swapTokensAtAmount = 4206900000000 * 10 ** 9 (contracts/Token.sol#167)
PEPEWOJAK.slitherConstructorVariables() (contracts/Token.sol#140-847) uses literals with too many digits:
- maxWalletLimit = 4206900000000 * 10 ** 9 (contracts/Token.sol#168)
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits>

PEPEWOJAK._lastSell (contracts/Token.sol#156) is never used in PEPEWOJAK (contracts/Token.sol#140-847)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variable>

PEPEWOJAK._tTotal (contracts/Token.sol#164) should be constant
PEPEWOJAK._deadWallet (contracts/Token.sol#173) should be constant
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant>

PEPEWOJAK._pair (contracts/Token.sol#159) should be immutable
PEPEWOJAK._router (contracts/Token.sol#158) 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/0xfca0f34dd29629e50e223c1d8655e206dd754fa52ff7ab6c833ab6ed3d628fd5>

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

<https://testnet.bscscan.com/tx/0xf68cef535a7f92434fa223a91076342f67da7f0cd1152a12cc6a23091838ebd3>

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

<https://testnet.bscscan.com/tx/0xc13c7d26369461a1b6b0c4f3d96265a0025ca652b08fcb252a7b08f8f2b74582>

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

<https://testnet.bscscan.com/tx/0x49ef00bc50e10523b5c7943cb6bcf8225c60ee06684e2ab8a7dcb2d6f832b412>

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

<https://testnet.bscscan.com/tx/0x534e241c562c81652fc4713d07c120c33c4b302434aa6c35c174344023230f76>

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

<https://testnet.bscscan.com/tx/0xe8e15600504999e4e53031cbf77c877a17f6fcf534d97ab4db37ff4efa99f1b9>



FUNCTIONAL TESTING

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

<https://testnet.bscscan.com/tx/0x4566484e0b8ad14040b78cb4c689247f4def04769e171da78de0f5ee5102e114>

8- Internal swap (passed):

All fee wallets received BNB

<https://testnet.bscscan.com/tx/0xe8e15600504999e4e53031cbf77c877a17f6fcf534d97ab4db37ff4efa99f1b9>

MANUAL TESTING

Centralization - Owner must enable trading

Severity: High

Function: EnableTrading

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

Recommendation:

to address this issue there are multiple options

- transfer ownership of contract to a trusted 3rd wallet (pinksale safu developer) to guarantee enabling of trades
- Incorporate a safety mechanism that allows investors to activate trading if a specified duration has elapsed since the conclusion of the presale or consider alternative ways such as allowing trades after investors claimed their presale tokens.

MANUAL TESTING

Logical – Setting swap threshold to 0

Severity: High

Function: updateSwapTokensAtAmount

Status: not resolved

Overview:

setting swap threshold to 0 can disable sells if contract balance is more than threshold.

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(
        amount <= 42069000000000,
        "Cannot set swap threshold amount higher than 1% of tokens"
    );
    swapTokensAtAmount = amount * 10 ** _decimals;
}
```

Recommendation:

ensure that swap threshold can not be zero.

Example:

```
function updateSwapTokensAtAmount(uint256 amount) external onlyOwner {
    require(
        amount <= 42069000000000,
        "Cannot set swap threshold amount higher than 1% of tokens"
    );
    swapTokensAtAmount = amount * 10 ** _decimals;
    require(swapTokensAtAmount > 0);
}
```



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>
