auditace.tech

AuditAce

FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

zkPepe

DATED : 8 May 23'

AUDIT SUMMARY

Project name – zkPepe

Date: 8 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	0	0	0	1
Acknowledged	0	0	0	0	0
Resolved	0	1	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 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/token/0xf0cddc483f04b18f6e0ad1a7fabb342c8cad6a43

Token Information

Token Name : zkPepe

Token Symbol: zkPepe

Decimals: 18

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

Token Address:
0x21C6fcDf49f30DCa6a5D2571A76B31121E871634

Checksum:
80b4b14b6f2ec91de8765d5ba8fe52cf73411863

Owner:
0x7075028c83801F6abbEf3DeFB9C5f10d8a35fD52
(at time of writing the audit)

Deployer:
0x7075028c83801F6abbEf3DeFB9C5f10d8a35fD52

TOKEN OVERVIEW

Fees:

Buy Fees: up to 8%

Sell Fees: up to 8%

Transfer Fees: up to 8%

Fees Privilege: Owner

Ownership: Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: changing swap threshold - changing fees - 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

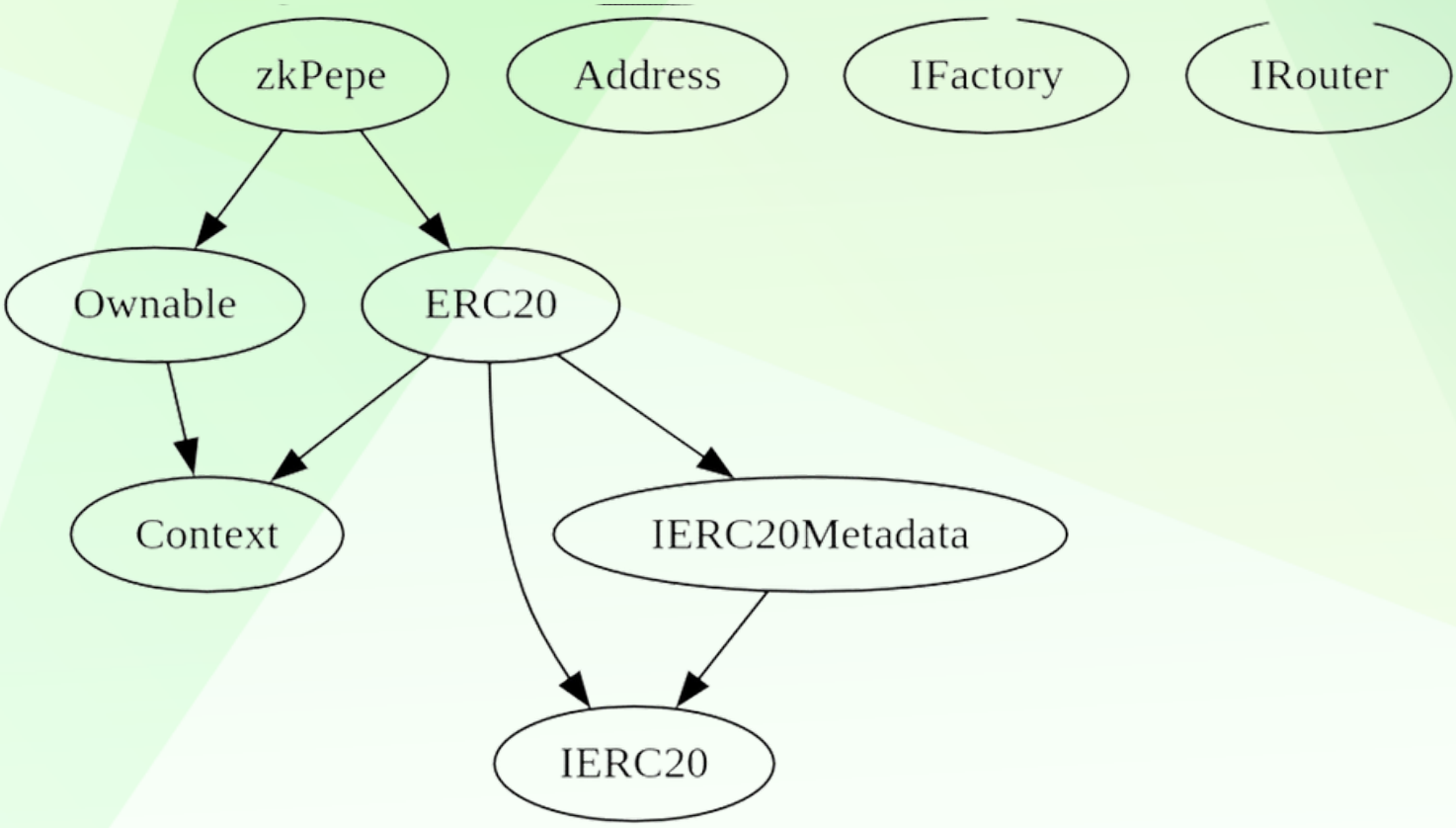
CLASSIFICATION OF RISK

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

INHERITANCE TREE



POINTS TO NOTE

- Owner is not able to set set buy/sell/transfer tax more than 8% each
- Owner is not able to set a max buy/transfer/wallet/sell 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 must enable trades for holders to be able to trade

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Mutability	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	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 ❗
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 🔒	🛑	
└	_tokengeneration	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
Address	Library			
└	sendValue	Internal 🔒	🛑	
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗

CONTRACT ASSESMENT

└	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 ❗
zkPepe	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	approve	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	increaseAllowance	Public ❗	🛑	NO ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	Liquify	Private 🔐	🛑	lockTheSwap
└	swapTokensForETH	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	updateLiquidityProvide	External ❗	🛑	onlyOwner
└	updateLiquidityTreshhold	External ❗	🛑	onlyOwner
└	EnableTrading	External ❗	🛑	onlyOwner
└	UpdateZeroBuyTax	External ❗	🛑	onlyOwner
└	UpdateZeroSellTax	External ❗	🛑	onlyOwner
└	SetBuyTax	External ❗	🛑	onlyOwner
└	SetSellTax	External ❗	🛑	onlyOwner
└	UpdateTxTax	External ❗	🛑	onlyOwner
└	updatedeadline	External ❗	🛑	onlyOwner
└	updateMarketingWallet	External ❗	🛑	onlyOwner
└	updateDevWallet	External ❗	🛑	onlyOwner
└	updateExemptFee	External ❗	🛑	onlyOwner
└	bulkExemptFee	External ❗	🛑	onlyOwner
└	rescueBNB	External ❗	🛑	onlyOwner
└	rescueBEP20	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

CONTRACT ASSESMENT

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

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

Context._msgData() (contracts/Token.sol#22-25) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#15) 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#346-357):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#352)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Variable ERC20._balances (contracts/Token.sol#78) is not in mixedCase
Variable ERC20._allowances (contracts/Token.sol#80) is not in mixedCase
Function IRouter.WETH() (contracts/Token.sol#410) is not in mixedCase
Contract zkPepe (contracts/Token.sol#433-775) is not in CapWords
Function zkPepe.Liquify(uint256,zkPepe.Taxes) (contracts/Token.sol#609-653) is not in mixedCase
Parameter zkPepe.updateLiquidityTreshhold(uint256).new_amount (contracts/Token.sol#692) is not in mixedCase
Function zkPepe.EnableTrading() (contracts/Token.sol#704-709) is not in mixedCase
Function zkPepe.UpdateZeroBuyTax() (contracts/Token.sol#711-713) is not in mixedCase
Function zkPepe.UpdateZeroSellTax() (contracts/Token.sol#715-717) is not in mixedCase
Function zkPepe.SetBuyTax() (contracts/Token.sol#719-721) is not in mixedCase
Function zkPepe.SetSellTax() (contracts/Token.sol#723-725) is not in mixedCase
Function zkPepe.UpdateTxTax() (contracts/Token.sol#727-730) is not in mixedCase
Parameter zkPepe.updatedeadline(uint256)._deadline (contracts/Token.sol#732) is not in mixedCase
Parameter zkPepe.updateExemptFee(address,bool)._address (contracts/Token.sol#748) is not in mixedCase
Variable zkPepe.genesis_block (contracts/Token.sol#445) is not in mixedCase
Constant zkPepe.deadWallet (contracts/Token.sol#451-452) 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#23)" inContext (contracts/Token.sol#17-26)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

zkPepe.constructor() (contracts/Token.sol#473-492) uses literals with too many digits:
        - _tokengeneration(msg.sender,420690000000000 * 10 ** decimals()) (contracts/Token.sol#474)
zkPepe.updateLiquidityTreshhold(uint256) (contracts/Token.sol#692-702) uses literals with too many digits:
        - require(bool,string)(new_amount >= 42069000000,Swap threshold amount should be lower or equal to 0.01% of tokens) (contracts/Token.sol#693-696)
zkPepe.updateLiquidityTreshhold(uint256) (contracts/Token.sol#692-702) uses literals with too many digits:
        - require(bool,string)(new_amount <= 4206900000000,Swap threshold amount should be lower or equal to 1% of tokens) (contracts/Token.sol#697-700)
zkPepe.slitherConstructorVariables() (contracts/Token.sol#433-775) uses literals with too many digits:
        - tokenLiquidityThreshold = 420690000000 * 10 ** 18 (contracts/Token.sol#443)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

zkPepe.launchtax (contracts/Token.sol#447) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

zkPepe.pair (contracts/Token.sol#437) should be immutable
zkPepe.router (contracts/Token.sol#436) 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/0xfd380e0944a236341b86ab506ccbc918c4080d185819633e4cf37188e4fefd72

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

https://testnet.bscscan.com/tx/0x219248b3bce0128df8d4ba95a1006b7be6098d8d925106c993fc9ba4610e6e8e

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

https://testnet.bscscan.com/tx/0x2abeeddc5da5463fc969e026a427002aacbbe1b5e7c56f399301c298202cb131

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

https://testnet.bscscan.com/tx/0xdf35585bca54e40641979a40898f03fc3fcb145f0783d65101852dbc1c192765

5- Buying when not excluded from fees (upto 8% tax) (passed):

https://testnet.bscscan.com/tx/0x24bcd482e84c1619eb175e5acccf1c483051c0ae6b440e19da814cd2f04826d1

6- Selling when not excluded from fees (upto 8% tax) (passed):

https://testnet.bscscan.com/tx/0x4f0eb5b3ecfd7d43ec9648b1ce2efd9b313cb1289df7ca642121f96c77fc9c7c

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (upto 8% tax)(passed):

https://testnet.bscscan.com/tx/0x81e26ed066166788902b4cf71aad9eaf598dd93f630f3827eefef82135b80d1a

7- Internal swap (fee wallets received BNB)(passed):

https://testnet.bscscan.com/address/0xe590f86e972b4b27ad832d699b7dd641d9481dbf#internaltx

MANUAL TESTING

Centralization – Trades must be enabled

Severity: High

function: EnableTrading

Status: Resolved (Contract is owned by Pinksale safu developer)

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;
    providingLiquidity = 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 **(applied)**

MANUAL TESTING

Informational – Redundant code

Status: Not Resolved

Overview:

Auto-liquidty feature of the contract is never used (0% liqudity tax) hence its suggested to remove auto-liquidity code.

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