auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Ezra Coin

DATED : 17 March, 2024

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

Function: EnablingTrades

Status: Open

Overview:

The OpenTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function ownerEnableTrading() public onlyOwner {
        require(!_tradingEnabled, "Cannot disable trading!");
        _tradingEnabled = !_tradingEnabled;
    }
```

Suggestion:

To reduce centralization and potential manipulation, consider one of the following approaches:

1.Automatically enable trading after a specified condition, such as the completion of a presale, is met.

2.If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can provide investors with more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad-faith actions by the original owner.

AUDIT SUMMARY

Project name – Ezra Coin

Date: 17 March, 2024

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed With High Risk**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	1	1	2	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 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/0xa80a4ee86680e1ca2371ee5e73a42c9a501b2b86#code

Token Information

Token Name : Ezra Coin

Token Symbol: Ezra

Decimals: 18

Token Supply: 500000000

Network: BscScan

Token Type: BEP-20

Token Address:
0x064e496E3017A07c25754aB3C13e0d8371aDeD93

Checksum:
Ac6659e84744e0102ab19c1d1e78a213

Owner:
0xa202bAaf58fccbDE080939591C526545A6922Cb6
(at time of writing the audit)

Deployer:
0xfD8a79064a92737230e33b839cA522F10F15996A

TOKEN OVERVIEW

Fees:

Buy Fee: 5-20%

Sell Fee: 5-20%

Transfer Fee: 2-10%

Fees Privilege: Owner

Ownership: Owned

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

AUDIT METHODOLOGY

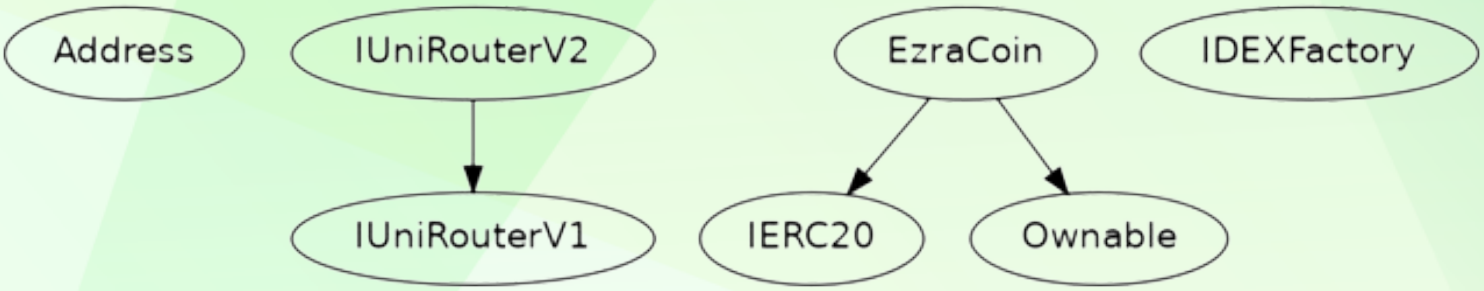
The auditing process will follow a routine as special considerations by Auditace:

- 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

- [x] Return values of low-level calls
- [x] Private modifier
- [x] Multiple Sends
- [x] Using Suicide
- [x] Gas Limitand Loops
- [x] Address hardcoded
- [x] Exception Disorder
- [x] Using inline assembly
- [x] Divide before multiply
- [x] Missing Zero Address Validation
- [x] Compiler version not fixed
- [x] **Gasless Send**
- [x] Using block.timestamp
- [x] Re-entrancy
- [x] Tautology or contradiction
- [x] Timestamp Dependence
- [x] Revert/require functions
- [x] Use of tx.origin
- [x] Integer overflow/underflow
- [x] Dangerous strict equalities
- [x] Using SHA3
- [x] Using throw

INHERITANCE TREE



STATIC ANALYSIS

A static analysis of the code was performed using Slither.

No issues were found.

```
INFO:Detectors:
EzraCoin.ownerWithdrawStrandedToken(address) (EzraCoin.sol#440-446) ignores return value by token.transfer(msg.sender,token.balanceOf(address(this))) (EzraCoin.sol#445)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unchecked-transfer
INFO:Detectors:
EzraCoin._approve(address,address,uint256).owner (EzraCoin.sol#490) shadows:
        - Ownable.owner() (EzraCoin.sol#252-254) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
EzraCoin.ownerUpdateMaxTx(uint256,uint256) (EzraCoin.sol#384-392) should emit an event for:
        - _maxTxBuy = maxBuyTx (EzraCoin.sol#390)
        - _maxTxSell = maxSellTx (EzraCoin.sol#391)
EzraCoin.ownerUpdateTax(uint8,uint8,uint8) (EzraCoin.sol#403-413) should emit an event for:
        - _buyTax = buyTax (EzraCoin.sol#410)
        - _sellTax = sellTax (EzraCoin.sol#411)
        - _transferTax = transferTax (EzraCoin.sol#412)
EzraCoin.ownerSetSwapThreshold(uint256) (EzraCoin.sol#427-433) should emit an event for:
        - _swapTokenThreshold = swapTokenThreshold * 10 ** _decimals (EzraCoin.sol#432)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-events-arithmetic
INFO:Detectors:
Reentrancy in EzraCoin._transfer(address,address,uint256) (EzraCoin.sol#316-336):
        External calls:
        - _swapContractTokens() (EzraCoin.sol#331)
                - _router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (EzraCoin.sol#368-374)
                - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
        External calls sending eth:
        - _swapContractTokens() (EzraCoin.sol#331)
                - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
        Event emitted after the call(s):
        - Transfer(from,to,amount - taxAmount) (EzraCoin.sol#347)
                - _transferTokens(from,to,amount,_sellTax) (EzraCoin.sol#333)
Reentrancy in EzraCoin.transferFrom(address,address,uint256) (EzraCoin.sol#477-488):
        External calls:
        - _transfer(sender,recipient,amount) (EzraCoin.sol#483)
                - _router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (EzraCoin.sol#368-374)
                - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (EzraCoin.sol#483)
                - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
        Event emitted after the call(s):
        - Approval(owner,spender,amount) (EzraCoin.sol#496)
                - _approve(sender,msg.sender,allowance_ - amount) (EzraCoin.sol#485)
        - Transfer(sender,recipient,amount) (EzraCoin.sol#486)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Address.isContract(address) (EzraCoin.sol#12-18) uses assembly
        - INLINE ASM (EzraCoin.sol#14-16)
Address._verifyCallResult(bool,bytes,string) (EzraCoin.sol#76-93) uses assembly
        - INLINE ASM (EzraCoin.sol#85-88)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

STATIC ANALYSIS

```
INFO:Detectors:
Address.isContract(address) (EzraCoin.sol#12-18) uses assembly
        - INLINE ASM (EzraCoin.sol#14-16)
Address._verifyCallResult(bool,bytes,string) (EzraCoin.sol#76-93) uses assembly
        - INLINE ASM (EzraCoin.sol#85-88)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Address._verifyCallResult(bool,bytes,string) (EzraCoin.sol#76-93) is never used and should be removed
Address.functionCall(address,bytes) (EzraCoin.sol#24-26) is never used and should be removed
Address.functionCall(address,bytes,string) (EzraCoin.sol#27-33) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (EzraCoin.sol#34-40) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (EzraCoin.sol#41-51) is never used and should be removed
Address.functionDelegateCall(address,bytes) (EzraCoin.sol#60-66) is never used and should be removed
Address.functionDelegateCall(address,bytes,string) (EzraCoin.sol#67-75) is never used and should be removed
Address.functionStaticCall(address,bytes) (EzraCoin.sol#52-54) is never used and should be removed
Address.functionStaticCall(address,bytes,string) (EzraCoin.sol#55-63) is never used and should be removed
Address.isContract(address) (EzraCoin.sol#12-18) is never used and should be removed
Address.sendValue(address,uint256) (EzraCoin.sol#19-23) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version0.8.17 (EzraCoin.sol#9) allows old versions
solc-0.8.17 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (EzraCoin.sol#19-23):
        - (success) = recipient.call{value: amount}() (EzraCoin.sol#21)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (EzraCoin.sol#41-51):
        - (success,returndata) = target.call{value: value}(data) (EzraCoin.sol#49)
Low level call in Address.functionStaticCall(address,bytes,string) (EzraCoin.sol#55-63):
        - (success,returndata) = target.staticcall(data) (EzraCoin.sol#61)
Low level call in Address.functionDelegateCall(address,bytes,string) (EzraCoin.sol#67-75):
        - (success,returndata) = target.delegatecall(data) (EzraCoin.sol#73)
Low level call in EzraCoin._swapContractTokens() (EzraCoin.sol#349-359):
        - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
Low level call in EzraCoin.ownerWithdrawETH() (EzraCoin.sol#435-438):
        - (success) = msg.sender.call{value: (address(this).balance)}() (EzraCoin.sol#436)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniRouterV1.WETH() (EzraCoin.sol#98) is not in mixedCase
Constant EzraCoin._decimals (EzraCoin.sol#274) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._totalSupply (EzraCoin.sol#276) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._tokenName (EzraCoin.sol#281) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._tokenSymbol (EzraCoin.sol#282) is not in UPPER_CASE_WITH_UNDERSCORES
Modifier EzraCoin.LockTheSwap() (EzraCoin.sol#299-303) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniRouterV1.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (EzraCoin.sol#103) is too similar to IUniRouterV1.addLiquidity(address,address,uint256,uint256
,uint256,uint256,address,uint256).amountBDesired (EzraCoin.sol#104)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
```

```
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (EzraCoin.sol#19-23):
        - (success) = recipient.call{value: amount}() (EzraCoin.sol#21)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (EzraCoin.sol#41-51):
        - (success,returndata) = target.call{value: value}(data) (EzraCoin.sol#49)
Low level call in Address.functionStaticCall(address,bytes,string) (EzraCoin.sol#55-63):
        - (success,returndata) = target.staticcall(data) (EzraCoin.sol#61)
Low level call in Address.functionDelegateCall(address,bytes,string) (EzraCoin.sol#67-75):
        - (success,returndata) = target.delegatecall(data) (EzraCoin.sol#73)
Low level call in EzraCoin._swapContractTokens() (EzraCoin.sol#349-359):
        - (transferMarketing) = address(marketingWallet).call{gas: 30000,value: address(this).balance}() (EzraCoin.sol#356)
Low level call in EzraCoin.ownerWithdrawETH() (EzraCoin.sol#435-438):
        - (success) = msg.sender.call{value: (address(this).balance)}() (EzraCoin.sol#436)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniRouterV1.WETH() (EzraCoin.sol#98) is not in mixedCase
Constant EzraCoin._decimals (EzraCoin.sol#274) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._totalSupply (EzraCoin.sol#276) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._tokenName (EzraCoin.sol#281) is not in UPPER_CASE_WITH_UNDERSCORES
Constant EzraCoin._tokenSymbol (EzraCoin.sol#282) is not in UPPER_CASE_WITH_UNDERSCORES
Modifier EzraCoin.LockTheSwap() (EzraCoin.sol#299-303) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniRouterV1.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (EzraCoin.sol#103) is too similar to IUniRouterV1.addLiquidity(address,address,uint256,uint256
,uint256,uint256,address,uint256).amountBDesired (EzraCoin.sol#104)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
EzraCoin.ownerUpdateMaxTx(uint256,uint256) (EzraCoin.sol#384-392) uses literals with too many digits:
        - require(bool)(maxBuyTx >= 5000000 * 10 ** 18) (EzraCoin.sol#388)
EzraCoin.ownerUpdateMaxTx(uint256,uint256) (EzraCoin.sol#384-392) uses literals with too many digits:
        - require(bool)(maxSellTx >= 5000000 * 10 * 18) (EzraCoin.sol#389)
EzraCoin.ownerSetSwapThreshold(uint256) (EzraCoin.sol#427-433) uses literals with too many digits:
        - require(bool,string)(swapTokenThreshold <= 2500000,Cannot exceed 50 billion.) (EzraCoin.sol#431)
EzraCoin.slitherConstructorVariables() (EzraCoin.sol#269-533) uses literals with too many digits:
        - _maxTxBuy = 10000000 * 10 ** _decimals (EzraCoin.sol#277)
EzraCoin.slitherConstructorVariables() (EzraCoin.sol#269-533) uses literals with too many digits:
        - _maxTxSell = 5000000 * 10 ** _decimals (EzraCoin.sol#278)
EzraCoin.slitherConstructorVariables() (EzraCoin.sol#269-533) uses literals with too many digits:
        - _swapTokenThreshold = 2500000 * 10 ** _decimals (EzraCoin.sol#279)
EzraCoin.slitherConstructorConstantVariables() (EzraCoin.sol#269-533) uses literals with too many digits:
        - _totalSupply = 500000000 * 10 ** _decimals (EzraCoin.sol#276)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
EzraCoin._pairAddress (EzraCoin.sol#289) should be immutable
EzraCoin._router (EzraCoin.sol#288) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
INFO:Slither:EzraCoin.sol analyzed (7 contracts with 93 detectors), 46 result(s) found
```

FUNCTIONAL TESTING

1- Approve (passed):
https://testnet.bscscan.com/tx/0x22eb4b0420b173aed00a536782e32c2c06bf187520e2a3771ca015d3d3c721db

2- Enable Trading (passed):
https://testnet.bscscan.com/tx/0xeeda589ded145fc4ba09299caf684a9475b50cf5f224b2c35686ccff522b4b6e

3- Update Tax (passed):
https://testnet.bscscan.com/tx/0xed244a701ac93ae2e3df0a2b6c0879e4f860c7bf96487ea7874f65140f207469

4- Update Marketing Wallet (passed):
https://testnet.bscscan.com/tx/0x096726d88dfd086d8578e32f651866457d15ae7e108198484bf39692302945e8

5- Exclude From Fee (passed):
https://testnet.bscscan.com/tx/0x3206924ed62a8505aa150e0a3f9a4253027c29688257a124ee51fb4f964d5314

POINTS TO NOTE

- The owner can transfer ownership.
- The owner can renounce ownership.
- The owner can Enable trading.
- The owner can set the fees to not more than 20%.
- The owner can update the marketing address.
- The owner can withdraw ETH.
- The owner can set swap threshold value.
- The owner can exclude address from fees.
- The owner can update max tx.

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	1
Low-Risk	2
Gas Optimization / Suggestions	0

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

Function: EnablingTrades

Status: Open

Overview:

The OpenTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function ownerEnableTrading() public onlyOwner {
        require(!_tradingEnabled, "Cannot disable trading!");
        _tradingEnabled = !_tradingEnabled;
    }
```

Suggestion:

To reduce centralization and potential manipulation, consider one of the following approaches:

1.Automatically enable trading after a specified condition, such as the completion of a presale, is met.

2.If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can provide investors with more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad-faith actions by the original owner.

MANUAL TESTING

Centralization – Missing Require Check

Severity: Medium

Function: Update Marketing Wallet

Status: Open

Overview:

The owner can set any arbitrary address excluding zero address as this is not recommended because if the owner sets the address to the contract address, then the ETH will not be sent to that address and the transaction will fail and this will lead to a potential honeypot in the contract.

```
function ownerUpdateMarketingWallet(
        address newWallet
    ) public onlyOwner {
        require(newWallet != address(0), "Cannot be zero address!");
        marketingWallet = newWallet;
    }
```

Suggestion:

It is recommended that the address should not be able to be set as a contract address.

MANUAL TESTING

Centralization – Missing Events

Severity: Low

Function: Missing Events

Status: Open

Overview:
They serve as a mechanism for emitting and recording data onto the blockchain, making it transparent and easily accessible.

```
function ownerUpdateMaxTx(
        uint256 maxBuyTx,
        uint256 maxSellTx
    ) public onlyOwner {
        require(maxBuyTx >= 5000000 * 10 ** 18);
        require(maxSellTx >= 5000000 * 10 * 18);
        _maxTxBuy = maxBuyTx;
        _maxTxSell = maxSellTx;
    }
function ownerUpdateTax(
        uint8 buyTax,
        uint8 sellTax,
        uint8 transferTax
    ) public onlyOwner {
        require(buyTax + sellTax <= 20, "Buy tax + sell tax cannot exceed 10% !");
        require(transferTax <= 10);
        _buyTax = buyTax;
        _sellTax = sellTax;
        _transferTax = transferTax;
    }
```

Suggestion:
Emit an event for critical changes.

MANUAL TESTING

Centralization – Local Variable Shadowing

Severity: Low

Function: Shadowing Local

Status: Open

Overview:

```
function _approve(
        address owner,
        address spender,
        uint256 amount
    ) private {
        require((owner != address(0) && spender != address(0)), "Owner/Spender address cannot be 0.");
        _allowances[owner][spender] = amount;
        emit Approval(owner, spender, amount);
    }
```

Suggestion:

Rename the local variable that shadows another component.

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