auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

# Smart Contract Audit

FOR

## Pepe 4 Trump

DATED : 18 June 24'

# AUDIT SUMMARY

**Project name** – Pepe 4 Trump

**Date**: 18 June, 2024

**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 | 1 | 0 | 1 |
| 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/0xc9ef70d1738e89397f9c85c061773b8ab419cf19#code

# Token Information

**Token Address:**
0x3d34562b53580B2c1dc9eAbA780825f361F82fea

**Name:** Pepe 4 Trump

**Symbol:** PEPE4TRUMP

**Decimals:** 18

**Network:** BscScan

**Token Type:** BEP-20

**Owner:** 0x46992aacF7E759BAa86b5dD1FadCfF6519E5F0E9

**Deployer:**
0x46992aacF7E759BAa86b5dD1FadCfF6519E5F0E9

**Token Supply:** 1000000000

**Checksum:** A17acbefe2a12642d388659dffd20321

**Testnet:**
https://testnet.bscscan.com/address/0xc9ef70d1738e89397f9c85c061773b8ab419cf19#code

# TOKEN OVERVIEW

**Buy Fee:** 0-25%

**Sell Fee:** 0-25%

**Transfer Fee:** 0-25%

**Fee Privilege:** Owner

**Ownership:** Owned

**Minting:** None

**Max Tx:** No

**Blacklist:** No

# AUDIT METHODOLOGY

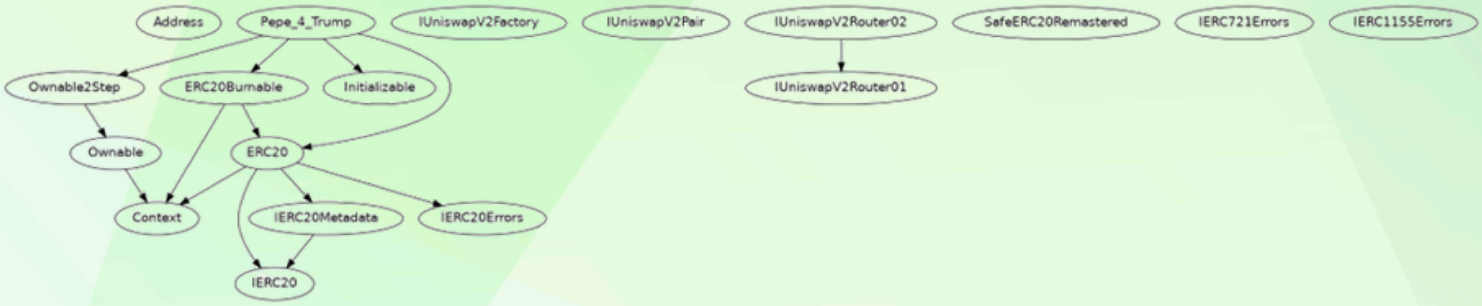
The auditing process will follow a routine as special considerations by Auditace:

- 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



# POINTS TO NOTE

- The owner can transfer ownership.
- The owner can renounce ownership.
- The owner can recover the token.
- The owner can update the swap threshold.
- The owner can update the marketing address.
- The owner can set marketing fees setup.
- The owner can set AMM Pair.

# STATIC ANALYSIS

```
INFO:Detectors:
Pepe_4_Trump._update(address,address,uint256) (Pepe_4_Trump.sol#1418-1484) uses a Boolean constant improperly:
        -false || _marketingPending > 0 (Pepe_4_Trump.sol#1457)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#misuse-of-a-boolean-constant
INFO:Detectors:
Pepe_4_Trump._update(address,address,uint256) (Pepe_4_Trump.sol#1418-1484) performs a multiplication on the result of a division:
        - fees = amount * totalFees[txType] / 10000 (Pepe_4_Trump.sol#1439)
        - _marketingPending += fees * marketingFees[txType] / totalFees[txType] (Pepe_4_Trump.sol#1442)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
Ownable2Step.transferOwnership(address).newOwner (Pepe_4_Trump.sol#883) lacks a zero-check on :
                - _pendingOwner = newOwner (Pepe_4_Trump.sol#884)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in Pepe_4_Trump._updateRouterV2(address) (Pepe_4_Trump.sol#1393-1400):
        External calls:
        - pairV2 = IUniswapV2Factory(routerV2.factory()).createPair(address(this),routerV2.WETH()) (Pepe_4_Trump.sol#1395)
        State variables written after the call(s):
        - _setAMMPair(pairV2,true) (Pepe_4_Trump.sol#1397)
                - AMMPairs[pair] = isPair (Pepe_4_Trump.sol#1409)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
INFO:Detectors:
Reentrancy in Pepe_4_Trump._update(address,address,uint256) (Pepe_4_Trump.sol#1418-1484):
        External calls:
        - _swapTokensForCoin(token2Swap) (Pepe_4_Trump.sol#1461)
                - routerV2.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path,address(this),block.timestamp) (Pepe_4_Trump.sol#1348)
        - (success,None) = address(marketingAddress).call{value: marketingPortion}() (Pepe_4_Trump.sol#1466)
        External calls sending eth:
        - (success,None) = address(marketingAddress).call{value: marketingPortion}() (Pepe_4_Trump.sol#1466)
        Event emitted after the call(s):
        - Transfer(from,to,value) (Pepe_4_Trump.sol#1113)
                - super._update(from,to,amount) (Pepe_4_Trump.sol#1480)
        - WalletTaxSent(1,marketingAddress,marketingPortion) (Pepe_4_Trump.sol#1468)
Reentrancy in Pepe_4_Trump._updateRouterV2(address) (Pepe_4_Trump.sol#1393-1400):
        External calls:
        - pairV2 = IUniswapV2Factory(routerV2.factory()).createPair(address(this),routerV2.WETH()) (Pepe_4_Trump.sol#1395)
        Event emitted after the call(s):
        - AMMPairsUpdated(pair,isPair) (Pepe_4_Trump.sol#1414)
                - _setAMMPair(pairV2,true) (Pepe_4_Trump.sol#1397)
        - RouterV2Updated(router) (Pepe_4_Trump.sol#1399)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Address._revert(bytes) (Pepe_4_Trump.sol#516-528) uses assembly
        - INLINE ASM (Pepe_4_Trump.sol#521-524)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
INFO:Detectors:
Pepe_4_Trump._update(address,address,uint256) (Pepe_4_Trump.sol#1418-1484) has a high cyclomatic complexity (14).
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#cyclomatic-complexity
```

```
INFO:Detectors:
Pragma version^0.8.20 (Pepe_4_Trump.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
solc-0.8.20 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) (Pepe_4_Trump.sol#411-420):
        - (success) = recipient.call{value: amount}() (Pepe_4_Trump.sol#416)
Low level call in Address.functionCallWithValue(address,bytes,uint256) (Pepe_4_Trump.sol#453-459):
        - (success,returndata) = target.call{value: value}(data) (Pepe_4_Trump.sol#457)
Low level call in Address.functionStaticCall(address,bytes) (Pepe_4_Trump.sol#465-468):
        - (success,returndata) = target.staticcall(data) (Pepe_4_Trump.sol#466)
Low level call in Address.functionDelegateCall(address,bytes) (Pepe_4_Trump.sol#474-477):
        - (success,returndata) = target.delegatecall(data) (Pepe_4_Trump.sol#475)
Low level call in SafeERC20Remastered._callOptionalReturnBool(IERC20,bytes) (Pepe_4_Trump.sol#846-853):
        - (success,returndata) = address(token).call(data) (Pepe_4_Trump.sol#851)
Low level call in Pepe_4_Trump._update(address,address,uint256) (Pepe_4_Trump.sol#1418-1484):
        - (success,None) = address(marketingAddress).call{value: marketingPortion}() (Pepe_4_Trump.sol#1466)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Function IUniswapV2Router01.WETH() (Pepe_4_Trump.sol#533) is not in mixedCase
Function IUniswapV2Pair.DOMAIN_SEPARATOR() (Pepe_4_Trump.sol#682) is not in mixedCase
Function IUniswapV2Pair.PERMIT_TYPEHASH() (Pepe_4_Trump.sol#683) is not in mixedCase
Function IUniswapV2Pair.MINIMUM_LIQUIDITY() (Pepe_4_Trump.sol#700) is not in mixedCase
Function SafeERC20Remastered.safeTransfer_noRevert(IERC20,address,uint256) (Pepe_4_Trump.sol#786-788) is not in mixedCase
Contract Pepe_4_Trump (Pepe_4_Trump.sol#1249-1497) is not in CapWords
Parameter Pepe_4_Trump.afterConstructor(address)._router (Pepe_4_Trump.sol#1315) is not in mixedCase
Parameter Pepe_4_Trump.updateSwapThreshold(uint16)._swapThresholdRatio (Pepe_4_Trump.sol#1351) is not in mixedCase
Parameter Pepe_4_Trump.marketingAddressSetup(address)._newAddress (Pepe_4_Trump.sol#1367) is not in mixedCase
Parameter Pepe_4_Trump.marketingFeesSetup(uint16,uint16,uint16)._buyFee (Pepe_4_Trump.sol#1376) is not in mixedCase
Parameter Pepe_4_Trump.marketingFeesSetup(uint16,uint16,uint16)._sellFee (Pepe_4_Trump.sol#1376) is not in mixedCase
Parameter Pepe_4_Trump.marketingFeesSetup(uint16,uint16,uint16)._transferFee (Pepe_4_Trump.sol#1376) is not in mixedCase
Variable Pepe_4_Trump.AMMPairs (Pepe_4_Trump.sol#1267) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Pepe_4_Trump.sol#538) is too similar to IUniswapV2Router01.addLiquidity(address,address
,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (Pepe_4_Trump.sol#539)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar
INFO:Detectors:
Pepe_4_Trump.constructor() (Pepe_4_Trump.sol#1294-1310) uses literals with too many digits:
        - _mint(supplyRecipient,10000000000 * (10 ** decimals()) / 10) (Pepe_4_Trump.sol#1308)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Slither:Pepe_4_Trump.sol analyzed (18 contracts with 93 detectors), 43 result(s) found
```

**Result => A static analysis of contract's source code has been performed using slither,**

**No major issues were found in the output**

# FUNCTIONAL TESTING

**1- Approve (passed):**

https://testnet.bscscan.com/tx/0xffbe0ee4162439242f9f19888a91c946470f223fca309c642fc2ff227cbc0e88

**2- Marketing Address Setup (passed):**

https://testnet.bscscan.com/tx/0x419cd5045f9a8e7871d04a17d369a76afb5a5c383d06fe1c56d2f0f964dea0f7

**3- Marketing Fees Setup (passed):**

https://testnet.bscscan.com/tx/0xa94f012c2e215774c5bf5f82032a13bf7dc471e7d89c62a4161e8416ab6301c9

**4- Transfer (passed):**

https://testnet.bscscan.com/tx/0x1c7efd4a4095718e3e16976ac4325102ff6a7ae158bcda154e3dce5393f02cd7

# 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 | 1 |
| Low-Risk | 0 |
| Gas Optimization / Suggestions | 1 |

# MANUAL TESTING

## Centralization – Missing Require Check.

**Severity: Medium**

**Function: setTreasuryAddress**

**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 marketingAddressSetup(address _newAddress) public
onlyOwner {
    if (_newAddress == address(0)) revert
InvalidTaxRecipientAddress(address(0));

    marketingAddress = _newAddress;
    excludeFromFees(_newAddress, true);

    emit WalletTaxAddressUpdated(1, _newAddress);
  }
```

**Suggestion:**

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

# MANUAL TESTING

## Optimization

**Severity: Informational**

**Subject: Floating Pragma Solidity version**

**Status: Open**

**Overview:**

It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

pragma solidity ^0.8.20;

**Suggestion:**

Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

# 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**