auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

LuckyMeme

DATED : 14 June 24'

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

Function: openTrading

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 openTrading() public virtual onlyOwner {
    _trading = true;
  }
```

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 give investors 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: High

Function: changePrizeWallet

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. The transaction will fail, leading to a potential honeypot in the contract.

```
function changePrizeWallet(uint256 i, address prizeWallet) public virtual onlyOwner {
    if (i == 0) {
      _annualprizeWallet = payable(prizeWallet);
    }
    else if (i == 1) {
      _monthlyprizeWallet = payable(prizeWallet);
    }
    else if (i == 2) {
      _weeklyprizeWallet = payable(prizeWallet);
    }
  }
```

Suggestion:

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

AUDIT SUMMARY

Project name – LuckyMeme

Date: 14 June, 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	2	0	2	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/0xcd16417aa313701b573b737783b4521ca08d5de0#code

Token Information

Token Address:
0x4A8826988296843B2132CD4efb21294B01553987

Name: LuckyMeme

Symbol: LME

Decimals: 18

Network: EtherScan

Token Type: ERC-20

Owner: 0x162a40Cc7893355123C19A426D66323f895fc22f

Deployer: 0x162a40Cc7893355123C19A426D66323f895fc22f

Token Supply: 1000000000

Checksum: A17acbefe2a12642d388659dffd20311

Testnet:
https://testnet.bscscan.com/address/0xcd16417aa313701b573b737783b4521ca08d5de0#code

TOKEN OVERVIEW

Buy Fee: 0%

Sell Fee: 0%

Transfer Fee: 0%

Fee Privilege: Owner

Ownership: Owned

Minting: None

Max Tx: No

Blacklist: No

AUDIT METHODOLOGY

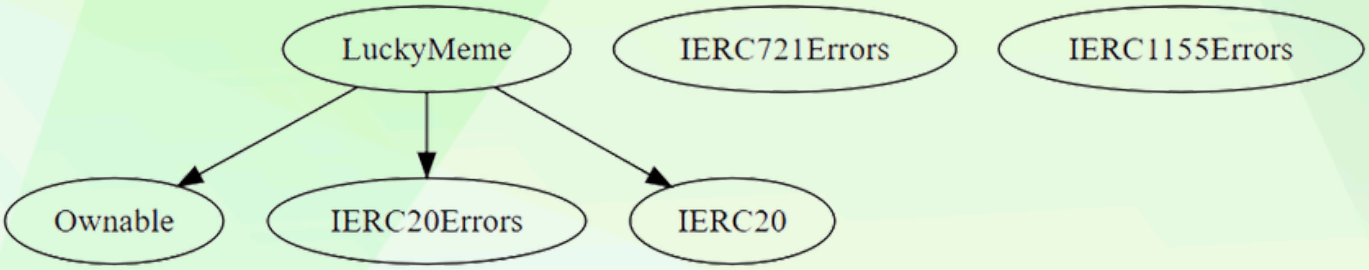
The auditing process will follow a routine as special considerations by Auditace:

- 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 Enable trading.
- The owner can change the Prize Wallet addresses.
- The owner can withdraw the token.

STATIC ANALYSIS

```
INFO:Detectors:
LuckyMeme._swapETHforToken(address,uint256) (LuckyMeme.sol#858-883) performs a multiplication on the result of a division:
        - tokenAmount = (ethAmount / presalePrice) * 10 ** _decimals (LuckyMeme.sol#866)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
INFO:Detectors:
LuckyMeme.changePrizeWallet(uint256,address).prizeWallet (LuckyMeme.sol#774) lacks a zero-check on :
                - _annualprizeWallet = address(prizeWallet) (LuckyMeme.sol#776)
                - _monthlyprizeWallet = address(prizeWallet) (LuckyMeme.sol#779)
                - _weeklyprizeWallet = address(prizeWallet) (LuckyMeme.sol#782)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Variable LuckyMeme._maxTransaction (LuckyMeme.sol#365) is not in mixedCase
Variable LuckyMeme._distributeThreshold (LuckyMeme.sol#366) is not in mixedCase
Constant LuckyMeme._taxDenominator (LuckyMeme.sol#368) is not in UPPER_CASE_WITH_UNDERSCORES
Variable LuckyMeme._distributeCounter (LuckyMeme.sol#369) is not in mixedCase
Variable LuckyMeme._trading (LuckyMeme.sol#372) is not in mixedCase
Variable LuckyMeme._presale (LuckyMeme.sol#373) is not in mixedCase
Variable LuckyMeme._hardTax (LuckyMeme.sol#374) is not in mixedCase
Variable LuckyMeme._zeroTax (LuckyMeme.sol#375) is not in mixedCase
Constant LuckyMeme._name (LuckyMeme.sol#377) is not in UPPER_CASE_WITH_UNDERSCORES
Constant LuckyMeme._symbol (LuckyMeme.sol#378) is not in UPPER_CASE_WITH_UNDERSCORES
Variable LuckyMeme._annualprizeWallet (LuckyMeme.sol#381) is not in mixedCase
Variable LuckyMeme._monthlyprizeWallet (LuckyMeme.sol#382) is not in mixedCase
Variable LuckyMeme._weeklyprizeWallet (LuckyMeme.sol#383) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Reentrancy in LuckyMeme._swapETHforToken(address,uint256) (LuckyMeme.sol#858-883):
        External calls:
        - address(owner()).transfer(ethAmount) (LuckyMeme.sol#870)
        State variables written after the call(s):
        - require(bool,string)(_presaleApprove(user,tokenAmount),Allowance not approved) (LuckyMeme.sol#874)
                - _allowances[user][spender] = value (LuckyMeme.sol#746)
        - status = transferFrom(lmeAddress,user,tokenAmount) (LuckyMeme.sol#875)
                - _allowances[user][spender] = value (LuckyMeme.sol#746)
        - _presaleApprove(user,0) (LuckyMeme.sol#882)
                - _allowances[user][spender] = value (LuckyMeme.sol#746)
        - status = transferFrom(lmeAddress,user,tokenAmount) (LuckyMeme.sol#875)
                - _balances[from] = fromBalance - value (LuckyMeme.sol#641)
                - _balances[to] += value (LuckyMeme.sol#656)
```

```
INFO:Detectors:
LuckyMeme.constructor() (LuckyMeme.sol#391-399) uses literals with too many digits:
        - _maxTransaction = 10000000 * 10 ** _decimals (LuckyMeme.sol#393)
LuckyMeme.constructor() (LuckyMeme.sol#391-399) uses literals with too many digits:
        - _distributeThreshold = 100000 * 10 ** _decimals (LuckyMeme.sol#394)
LuckyMeme.constructor() (LuckyMeme.sol#391-399) uses literals with too many digits:
        - _initialSupply = 1000000000 * 10 ** _decimals (LuckyMeme.sol#397)
LuckyMeme._swapETHforToken(address,uint256) (LuckyMeme.sol#858-883) uses literals with too many digits:
        - require(bool,string)(ethAmount >= 5000000000000000,ETH amount must be greater than 0.005 ETH) (LuckyMeme.sol#862)
LuckyMeme._swapETHforToken(address,uint256) (LuckyMeme.sol#858-883) uses literals with too many digits:
        - require(bool,string)(ethAmount <= 100000000000000000,ETH amount must be less than 1 ETH) (LuckyMeme.sol#863)
LuckyMeme.slitherConstructorVariables() (LuckyMeme.sol#360-898) uses literals with too many digits:
        - presalePrice = 2000000000000 (LuckyMeme.sol#836)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
LuckyMeme.presalePrice (LuckyMeme.sol#836) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:LuckyMeme.sol analyzed (6 contracts with 93 detectors), 23 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/0x21d3317b351988f766d13cd031a3ab1d5eb68bfcd6a96f3bcaab4ac8983c91e2

2- Open Trading (passed):

https://testnet.bscscan.com/tx/0xc8dcba7c88e9d9b8755331d0b557688977eb4f9571d153de84d6c0494d0b8349

3- Transfer (passed):

https://testnet.bscscan.com/tx/0x295828107d706ff4ef1657035cade6eb748185d5acc52c1db076a878d7a54610

4- Change Prize Wallet (passed):

https://testnet.bscscan.com/tx/0xed895ccfadabd74f95b0bf12da111594c1d8f0e47a90ad4849c42af6220fdc75

5- Zero Tax (passed):

https://testnet.bscscan.com/tx/0x3d958d8dc68b49b8a12009b2d32b1ad2392bc1e7e9c5b36203eb1884ba350f2c

6- Presale Over (passed):

https://testnet.bscscan.com/tx/0xf1c8da8fa39603b81fce8fdaf7510b27778427ea143e4202f230040b737141ff

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	2
Gas Optimization / Suggestions	1

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

Function: openTrading

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 openTrading() public virtual onlyOwner {
    _trading = true;
  }
```

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 give investors 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: High

Function: changePrizeWallet

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. The transaction will fail, leading to a potential honeypot in the contract.

```
function changePrizeWallet(uint256 i, address prizeWallet) public virtual onlyOwner {
    if (i == 0) {
      _annualprizeWallet = payable(prizeWallet);
    }
    else if (i == 1) {
      _monthlyprizeWallet = payable(prizeWallet);
    }
    else if (i == 2) {
      _weeklyprizeWallet = payable(prizeWallet);
    }
  }
```

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

Subject: 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 changePrizeWallet(uint256 i, address prizeWallet) public
virtual onlyOwner {
    if (i == 0) {
      _annualprizeWallet = payable(prizeWallet);
    }
    else if (i == 1) {
      _monthlyprizeWallet = payable(prizeWallet);
    }
    else if (i == 2) {
      _weeklyprizeWallet = payable(prizeWallet);
    }
function openTrading() public virtual onlyOwner {
    _trading = true;
  }
 }
```

Suggestion:

Emit an event for critical changes.

MANUAL TESTING

Centralization – Missing Zero Address

Severity: Low

Subject: Zero Check

Status: Open

Overview:

Functions can take a zero address as a parameter (0x00000...). If a function parameter of address type is not properly validated by checking for zero addresses, there could be serious consequences for the contract's functionality.

```
function changePrizeWallet(uint256 i, address prizeWallet) public virtual
onlyOwner {
    if (i == 0) {
      _annualprizeWallet = payable(prizeWallet);
    }
    else if (i == 1) {
      _monthlyprizeWallet = payable(prizeWallet);
    }
    else if (i == 2) {
      _weeklyprizeWallet = payable(prizeWallet);
    }
function openTrading() public virtual onlyOwner {
    _trading = true;
  }
 }
```

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 ^0.8.18;

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