



# Advanced Manual Smart Contract Audit

October 11, 2022

 CoinsultAudits

 [info@coinsult.net](mailto:info@coinsult.net)

 [coinsult.net](https://coinsult.net)

Audit requested by



**LMS Tracker**

No contract address

# Table of Contents

## 1. Audit Summary

- 1.1 Audit scope
- 1.2 Tokenomics
- 1.3 Source Code

## 2. Disclaimer

## 3. Global Overview

- 3.1 Informational issues
- 3.2 Low-risk issues
- 3.3 Medium-risk issues
- 3.4 High-risk issues

## 4. Vulnerabilities Findings

## 5. Contract Privileges

- 5.1 Maximum Fee Limit Check
- 5.2 Contract Pausability Check
- 5.3 Max Transaction Amount Check
- 5.4 Exclude From Fees Check
- 5.5 Ability to Mint Check
- 5.6 Ability to Blacklist Check
- 5.7 Owner Privileges Check

## 6. Notes

- 6.1 Notes by Coinsult
- 6.2 Notes by LMS Tracker

## 7. Contract Snapshot

## 8. Website Review

## 9. Certificate of Proof

# Audit Summary

Project Name	LMS Tracker
Website	
Blockchain	Binance Smart Chain Testnet
Smart Contract Language	Solidity
Contract Address	
Audit Method	Static Analysis, Manual Review
Date of Audit	11 October 2022

This audit report has been prepared by Coinsult's experts at the request of the client. In this audit, the results of the static analysis and the manual code review will be presented. The purpose of the audit is to see if the functions work as intended, and to identify potential security issues within the smart contract.

The information in this report should be used to understand the risks associated with the smart contract. This report can be used as a guide for the development team on how the contract could possibly be improved by remediating the issues that were identified.

# Audit Scope

Coinsult was commissioned by LMS Tracker to perform an audit based on the following code:

Not available

Note that we only audited the code available to us on this URL at the time of the audit. If the URL is not from any block explorer (main net), it may be subject to change. Always check the contract address on this audit report and compare it to the token you are doing research for.

## Audit Method

Coinsult's manual smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. This process is conducted to discover errors, issues and security vulnerabilities in the code in order to suggest improvements and ways to fix them.

### Automated Vulnerability Check

Coinsult uses software that checks for common vulnerability issues within smart contracts. We use automated tools that scan the contract for security vulnerabilities such as integer-overflow, integer-underflow, out-of-gas-situations, unchecked transfers, etc.

### Manual Code Review

Coinsult's manual code review involves a human looking at source code, line by line, to find vulnerabilities. Manual code review helps to clarify the context of coding decisions. Automated tools are faster but they cannot take the developer's intentions and general business logic into consideration.

### Used tools

- Slither: Solidity static analysis framework
- Remix: IDE Developer Tool
- CWE: Common Weakness Enumeration
- SWC: Smart Contract Weakness Classification and Test Cases
- DEX: Testnet Blockchains

# Risk Classification

Coinsult uses certain vulnerability levels, these indicate how bad a certain issue is. The higher the risk, the more strictly it is recommended to correct the error before using the contract.

Vulnerability Level	Description
● Informational	Does not compromise the functionality of the contract in any way
● Low-Risk	Won't cause any problems, but can be adjusted for improvement
● Medium-Risk	Will likely cause problems and it is recommended to adjust
● High-Risk	Will definitely cause problems, this needs to be adjusted

Coinsult has four statuses that are used for each risk level. Below we explain them briefly.

Risk Status	Description
Total	Total amount of issues within this category
Pending	Risks that have yet to be addressed by the team
Acknowledged	The team is aware of the risks but does not resolve them
Resolved	The team has resolved and remedied the risk

# SWC Attack Analysis

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Description	Status
SWC-100	Function Default Visibility	Passed
SWC-101	Integer Overflow and Underflow	Passed
SWC-102	Outdated Compiler Version	Passed
SWC-103	Floating Pragma	Passed
SWC-104	Unchecked Call Return Value	Passed
SWC-105	Unprotected Ether Withdrawal	Passed
SWC-106	Unprotected SELFDESTRUCT Instruction	Passed
SWC-107	Reentrancy	Passed
SWC-108	State Variable Default Visibility	Passed
SWC-109	Uninitialized Storage Pointer	Passed
SWC-110	Assert Violation	Passed
SWC-111	Use of Deprecated Solidity Functions	Passed
SWC-112	Delegatecall to Untrusted Callee	Passed
SWC-113	DoS with Failed Call	Passed
SWC-114	Transaction Order Dependence	Passed
SWC-115	Authorization through tx.origin	Passed

SWC-116	Block values as a proxy for time	Passed
SWC-117	Signature Malleability	Passed
SWC-118	Incorrect Constructor Name	Passed
SWC-119	Shadowing State Variables	Passed
SWC-120	Weak Sources of Randomness from Chain Attributes	Passed
SWC-121	Missing Protection against Signature Replay Attacks	Passed
SWC-122	Lack of Proper Signature Verification	Passed
SWC-123	Requirement Violation	Passed
SWC-124	Write to Arbitrary Storage Location	Passed
SWC-125	Incorrect Inheritance Order	Passed
SWC-126	Insufficient Gas Griefing	Passed
SWC-127	Arbitrary Jump with Function Type Variable	Passed
SWC-128	DoS With Block Gas Limit	Passed
SWC-129	Typographical Error	Passed
SWC-130	Right-To-Left-Override control character (U+202E)	Passed
SWC-131	Presence of unused variables	Passed
SWC-132	Unexpected Ether balance	Passed
SWC-133	Hash Collisions With Multiple Variable Length Arguments	Passed
SWC-134	Message call with hardcoded gas amount	Passed
SWC-135	Code With No Effects	Passed
SWC-136	Unencrypted Private Data On-Chain	Passed

# Global Overview

## Manual Code Review

In this audit report we will highlight the following issues:

Vulnerability Level	Total	Pending	Acknowledged	Resolved
Informational	0	0	0	0
Low-Risk	6	6	0	0
Medium-Risk	2	2	0	0
High-Risk	1	1	0	0



Error Code	Description
CS-01	Centralization Risk for Minimum Token Balance For Rewards

● **Low-Risk:** Could be fixed, will not bring problems.

### Centralization Risk for Minimum Token Balance For Rewards

```
function updateMinimumBalanceForRewards(uint256 _minimumBalanceForRewards) external onlyOwner {  
    minimumBalanceForRewards = _minimumBalanceForRewards * (10 ** 18);  
}
```

### Recommendation

Owner can set minimumBalanceForRewards without any constraints, this relies on the owner setting the correct values, for example, adding one '0' too many can result in people not receiving rewards. It is recommended to have require statements within a certain window.

Error Code	Description
CWE-829	Inclusion of Functionality from Untrusted Control Sphere

● **Low-Risk:** Could be fixed, will not bring problems.

### Avoid relying on `block.timestamp`

`block.timestamp` can be manipulated by miners.

```
function canClose() public view returns (bool) {
    if (block.timestamp >= lastFriday + 1 weeks) {
        return true;
    } else {
        return false;
    }
}
```

### Recommendation

Do not use `block.timestamp`, `now` or `blockhash` as a source of randomness

### Exploit scenario


```
contract Game {

    uint reward_determining_number;

    function guessing() external{
        reward_determining_number = uint256(block.blockhash(10000)) % 10;
    }
}
```

Eve is a miner. Eve calls `guessing` and re-orders the block containing the transaction. As a result, Eve wins the game.

Error Code	Description
SLT: 056	Missing Zero Address Validation

 **Low-Risk:** Could be fixed, will not bring problems.

### No zero address validation for some functions

Detect missing zero address validation.

```
function addOperator(address _operator) external onlyOwner {
    require(operatorWallets[_operator] != true, "LMSTracker: User is already set to this status");
    operatorWallets[_operator] = true;
}
```

### Recommendation

Check that the new address is not zero.

### Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }

    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

Bob calls updateOwner without specifying the newOwner, so Bob loses ownership of the contract.

Error Code	Description
CWE-252	Unchecked Return Value

● **Low-Risk:** Could be fixed, will not bring problems.

## Unchecked transfer

The return value of an external transfer/transferFrom call is not checked.

```
function claimStuckTokens(address token) external onlyOwner {
    if (token == address(0x0)) {
        payable(msg.sender).transfer(address(this).balance);
        return;
    }
    IERC20Upgradeable ERC20token = IERC20Upgradeable (token);
    uint256 balance = ERC20token.balanceOf(address(this));
    ERC20token.transfer(msg.sender, balance);
}
```

## Recommendation

Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

## Exploit scenario

```
contract Token {
    function transferFrom(address _from, address _to, uint256 _value) public returns (bool success);
}
contract MyBank{
    mapping(address => uint) balances;
    Token token;
    function deposit(uint amount) public{
        token.transferFrom(msg.sender, address(this), amount);
        balances[msg.sender] += amount;
    }
}
```

Several tokens do not revert in case of failure and return false. If one of these tokens is used in MyBank, deposit will not revert if the transfer fails, and an attacker can call deposit for free..

Error Code	Description
SLT: 054	Missing Events Arithmetic

● **Low-Risk:** Could be fixed, will not bring problems.

### Missing events arithmetic

Detect missing events for critical arithmetic parameters.

```
function setAllowNewTokens(bool allowed) external onlyOwner {
    allowNewTokens = allowed;
}
```

### Recommendation

Emit an event for critical parameter changes.

### Exploit scenario

```
contract C {

    modifier onlyAdmin {
        if (msg.sender != owner) throw;
        _;
    }

    function updateOwner(address newOwner) onlyAdmin external {
        owner = newOwner;
    }
}
```

updateOwner() has no event, so it is difficult to track off-chain changes in the buy price.

Error Code	Description
SLT: 062	Comparison to boolean constant

● **Low-Risk:** Could be fixed, will not bring problems.

## Boolean equality

Detects the comparison to boolean constants.

```
require(operatorWallets[_operator] == true, "LMSTracker: User is already set to this status");

weeklyTrackers[week].soldOrNewUser[_address] == false

require(weeklyTrackers[week].voted[msg.sender] == false, "LMSTracker: already voted");

if (weeklyTrackers[week].soldOrNewUser[user] == false) {
```

## Recommendation

Remove the equality to the boolean constant.

## Exploit scenario

```
contract A {
    function f(bool x) public {
        // ...
        if (x == true) { // bad!
            // ...
        }
        // ...
    }
}
```

Boolean constants can be used directly and do not need to be compare to true or false.

Error Code	Description
CSM-01	Potential OoG (Out-of-Gas) situation in closeWeek()

● **Medium-Risk:** Should be fixed, could bring problems.

### Potential OoG (Out-of-Gas) situation in closeWeek()

```
for (uint256 i = 0; i < _eligibleBalanceHolders.length(); i++) {  
    address user = _eligibleBalanceHolders.at(i);  
    if (weeklyTrackers[week].soldOrNewUser[user] == false) {  
        weeklyTrackers[week].eligibleUsers.push(user);  
    }  
}
```

### Recommendation

Caution is advised when you expect to have large arrays that grow over time. Actions that require looping across the entire data structure should be avoided. If you absolutely must loop over an array of unknown size, then you should plan for it to potentially take multiple blocks, and therefore require multiple transactions.

Error Code	Description
CSM-02	Testnet values have to be changed before launch

● **Medium-Risk:** Should be fixed, could bring problems.

### Testnet values have to be changed before launch

```
router = IRouter(0xD99D1c33F9fC3444f8101754aBC46c52416550D1); //!< testnet
tokenContract = 0xaF993Cee7dBF102ac93D1Eebca7bf4c9c8b03Bf3; //!< testnet

lastFriday = block.timestamp; //!< testnet will be set to last friday epoch according the launch date
```

### Recommendation

A lot of values are set to testnet values, change them before deployment.



Error Code	Description
CSH-01	Initializable contract

● **High-Risk:** Must be fixed, will bring problems.

## Initializable contract

```
function initialize() initializer public{
    __Ownable_init();
    router = IRouter(0xD99D1c33F9fC3444f8101754aBC46c52416550D1); /// testnet
    tokenContract = 0xaF993Cee7dBF102ac93D1Eebca7bf4c9c8b03Bf3;    /// testnet

    _proposedTokens.add(0x04c4f3f76d0501c977402e081DA1DB34A2796b1b);
    _proposedTokens.add(0xfCCC46ad6d2b3eB4d441bDCa5d6B32e2A7AE6Ede);
    _proposedTokens.add(0xc23583fE07264599068c0229a56dc5B71B6b768d);
    _proposedTokens.add(0x2303CFe3cbd322489D90a74742867CD38D436fec);
    _proposedTokens.add(0xeD8b95A8F0208940B5654B034093B4D83B6E6E99);
    _proposedTokens.add(0x00B0C0043D8bf1c653Bc01e469133d02AF31fd02);
    _proposedTokens.add(0xCA8a64D8414f8a891Cb13249d3B845839FBC2E8c);
    _proposedTokens.add(0x7b652c56AB8bE2EE29a65A018C25ae3B0A2AECa4);
    _proposedTokens.add(0x969faf5BEC994f40986b85c131d59e7219523257);
    _proposedTokens.add(0x242cb22b2524dBC64BA1b81c59AD139Dbe89E080);

    minimumBalanceForRewards = 1e7 * (10**18); /// testnet
    week;
    lastFriday = block.timestamp; /// testnet will be set to last friday epoch according the launch
    weekIndex;
```


## Recommendation

Do not leave an implementation contract uninitialized. An uninitialized implementation contract can be taken over by an attacker.

## Other Owner Privileges Check

Error Code	Description
CEN-100	Centralization: Operator Priviliges

Coinsult lists all important contract methods which the owner can interact with.

 Owner can update minimum token balance for rewards without constraints

# Notes

## Notes by LMS Tracker

No notes provided by the team.

## Notes by Coinsult

Contract is upgradable (proxy)

# Contract Snapshot

This is how the constructor of the contract looked at the time of auditing the smart contract.

```
contract LMSTracker is Initializable, OwnableUpgradeable {
    using EnumerableSetUpgradeable for EnumerableSetUpgradeable.AddressSet;

    address public tokenContract;

    IRouter public router;

    uint256 public minimumBalanceForRewards;
    uint256 public week;
    uint256 public lastFriday;
    uint256 public weekIndex;
    bool public allowNewTokens;

    EnumerableSetUpgradeable.AddressSet private _eligibleBalanceHolders;
    EnumerableSetUpgradeable.AddressSet private _proposedTokens;

    mapping (address => bool) public operatorWallets;

    struct WeeklyTracker {
        IERC20Upgradeable lmsToken;
        uint256 totalBNB;
        uint256 totalReward;

        mapping (address => bool) soldOrNewUser;
        address[] eligibleUsers;
        mapping (address => bool) claimedUser;
        uint256 rewardPerHolder;

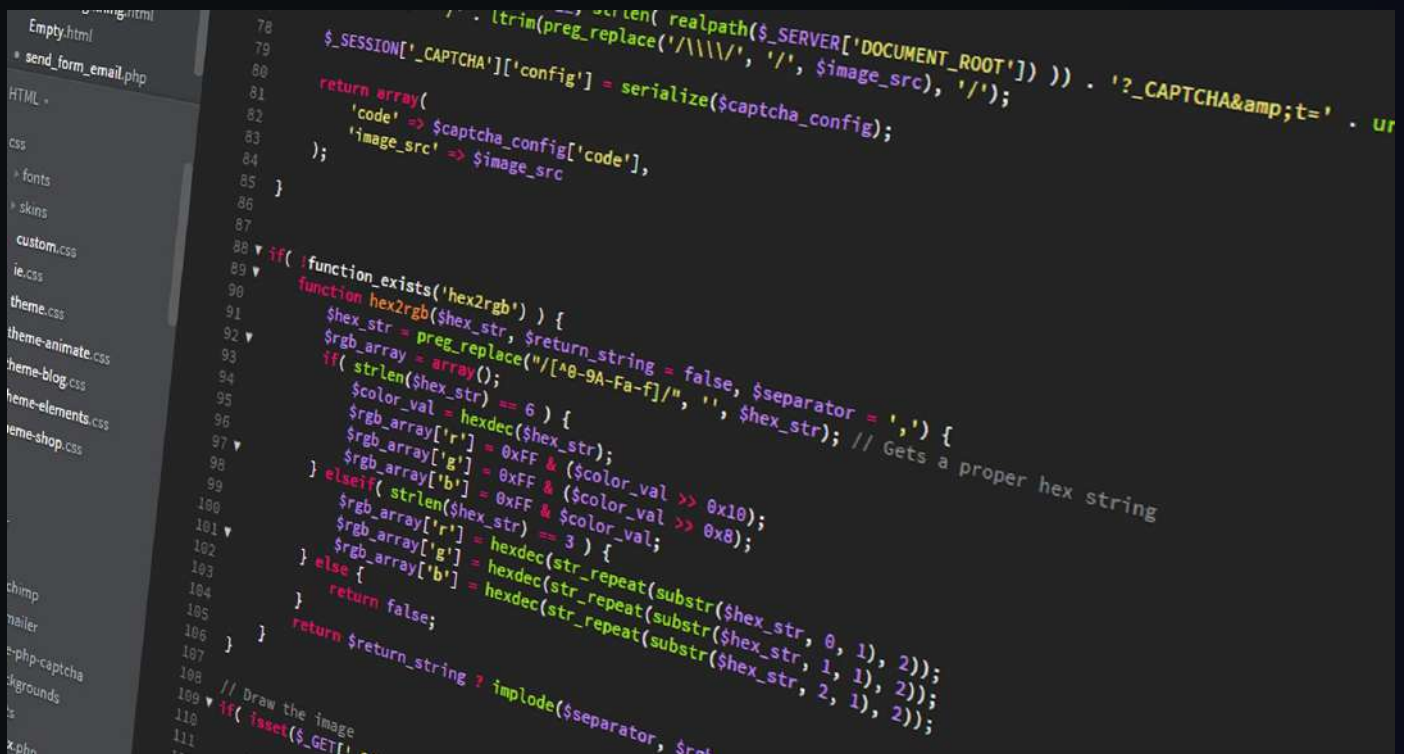
        bool isDistributed;
        bool isClosed;

        mapping (address => uint256) votes;
        mapping (address => bool) voted;
        address winningToken;
    }

    struct Summary {
```

# Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.



Type of check	Description
Mobile friendly?	● The website is mobile friendly
Contains jQuery errors?	● The website does not contain jQuery errors
Is SSL secured?	● The website is SSL secured
Contains spelling errors?	● The website does not contain spelling errors

# Certificate of Proof

● Not KYC verified by Coinsult

## LMS Tracker

Audited by Coinsult.net



Date: 11 October 2022

✓ Advanced Manual Smart Contract Audit

# Disclaimer

This audit report has been prepared by Coinsult's experts at the request of the client. In this audit, the results of the static analysis and the manual code review will be presented. The purpose of the audit is to see if the functions work as intended, and to identify potential security issues within the smart contract.

The information in this report should be used to understand the risks associated with the smart contract. This report can be used as a guide for the development team on how the contract could possibly be improved by remediating the issues that were identified.

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.


Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

# End of report

## **Smart Contract Audit**

 CoinsultAudits

 info@coinsult.net

 coinsult.net

Request your smart contract audit / KYC

**t.me/coinsult\_tg**