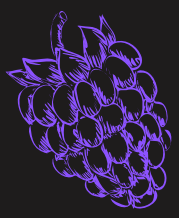


0XDAMORA
AUDITS

FEBRUARY 2023

Lira Security Audit

FOR

Lira Financial

PRESENTED BY

0xDaMora Warden

Table Of Contents:

1. INTRODUCTION

1.1 - Disclaimer

The audit makes no statements or warranties about utility of the code, suitability of the business model, or any other statements about fitness of the contract to purpose, or their bug free status.
The audit documentation is for discussion purposes only.

1.2 - Security Metodology

The auditor is involved in the entire audit process, the code is reviewed and, if necessary, proof of concept is generated.
In case of detected vulnerabilities, the auditor works together with the project to solve them.

1- Proyect Review

- Proyect Documentation Review
- General Code Review
- Webpage Review

Goal:
Identify the business logic and purpose of the code to review.

2- Checking the Code

- Manual Code Cheking in search of more elaborate vulnerabilities.
- Automatic Code Checking using vulnerability analysis tools like Mythril, Slither, etc.

Goal:
Eliminate the possibility of the most typical vulnerabilities such as Reentrancy, flash loan, gas limits, overflow, underflow, etc.

3- Bug-Fixing and Re-Audit

- The client eliminates the vulnerabilities detected by the auditors
- The auditors proceed to make a new audit taking into account the arrangements implemented.

Goal:

A solution to the audit problems is generated and a final public audit is delivered.

Finding Severity Breakdown

All vulnerabilities discovered are clasiffied based on their potential severityand have the following classification:

Severity	Description
Critical	- Direct theft of any user funds, whether at-rest or in-motion, other than unclaimed yield - Direct theft of any user NFTs, whether at-rest or in-motion, other than unclaimed royalties - Permanent freezing of funds - Permanent freezing of NFTs - Unauthorized minting of NFTs - Protocol insolvency
High	- Theft of unclaimed yield - Theft of unclaimed royalties - Permanent freezing of unclaimed yield - Permanent freezing of unclaimed royalties - Temporary freezing of funds - Temporary freezing NFTs
Medium	- Smart contract unable to operate due to lack of token funds - Block stuffing for profit - Griefing (e.g. no profit motive for an attacker, but damage to the users or the protocol) - Theft of gas - Unbounded gas consumption
Low	- Contract fails to deliver promised returns, but doesn't lose value

1.3 - Proyect Overview

Lira Financial proposes solutions to previous cryptocurrency challenges such as high mining costs and maintaining liquidity on decentralized exchanges. Lira suggests using DEX Liquidity Pools as an alternative to mining and reserve funds to capture liquidity. They also suggest using a smart contract to reduce token supply and promote scarcity. These tokenomics can benefit the community and incentivize adoption.

1.4 - Proyect Dashboard

Project Summary and Scope

Title	**Description**
Lira Financial	Lira is a utility token used to purchase goods or services.
Scope	**Link**
Lira Token	https://bscscan.com/token/0xa80a006a48dc7203eb3aa7e0b3816918d242cfc4#code

1.5 - Summary of Findings

Automatic Tools:

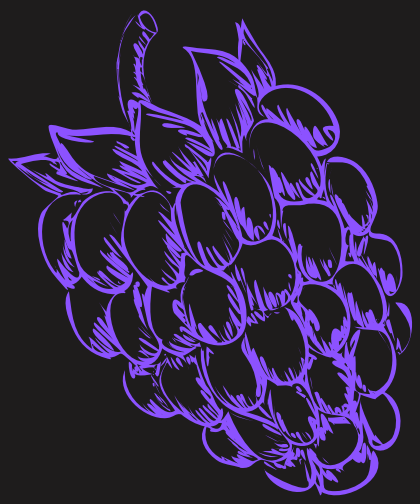
No	Description	Result
1	Compiler Warnings	Passed
2	Re-entrancy	Passed
3	Possible delays in data delivery	Passed
4	Front-running	Passed
5	Timestamp dependence	Passed
6	Integer Overflow and Underflow	Passed
7	DOS with Revert	Passed
8	DOS with block gas limit	Passed
9	Methods Execution permissions	Passed
10	Private User Data Leak	Passed
11	ShadowedStateVariable	Passed
12	UnrestrictedSelfdestruct	Passed
13	UnrestrictedDelegateCall	Passed

Manual Audit:

Severity	# of Findings
Critical	0
High	0
Medium	0
Low	2

1.6 - Conclusion

After conducting a thorough security audit of Lira Financial's platform, we are pleased to report that no major vulnerabilities were found. We found that Lira Financial have followed the best practices when deploying your contracts.



2. Finding Report

2.1 - Critical

Not Found

2.2 - High

Not Found

2.3 - Medium

Not Found

2.4 - Low

Low	Advanced Owner Privileges
File	Lira
Function	mint(address,uint)
Severity	Low
Status	Not Fixed

Description:

The owner can currently mine the amount of tokens they want.

Recommendation:

Think about passing the role of miner to a wallet without access or publish that there is a possibility that more tokens can be mined on the website

2.4 - Low

Low	Owner Can Pause Transfers
File	Lira
Function	pause()
Severity	Low
Status	Not Fixed

Description:

The owner can currently pause all transfers of your token.

Recommendation:

Think about abandoning the role of pause to have more confidence with your clients, but if you need the function for the objectives of the project, notify them of the possibility of pausing transfers.

3. About 0xDaMora Audits

0xDaMora is an emerging auditor who is starting to conduct code audits for Solidity.

By working with 0xDaMora, clients can benefit from a thorough examination of their Solidity code, including manual reviews, automated tests, and specialized tools to identify potential weaknesses.

CONTACTS:

@0xDaMora

danmor800@gmail.com

https://github.com/0xDaMora

0xDaMora#0655