PEX
AUDIT

PEX Audit

RIZQ Finance

May 23rd 2023

AUDIT

Audit Details

RIZQ Finance

Auditor's - PapaExchange

Website - http://www.rizqfinance.com

Blockchain - Binance Smart Chain

Disclaimer

PapaExchange LLP will be referred to as PEX per this report

- **PEX** audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

- **PEX** does not provide any warranty on its released reports.
We should not be used as a decision to invest into an audited project please do your own research. **PEX** provides transparent reports to all its "clients" and to its "clients participants" and will not claim any guarantee of bug-free code within its Smart Contract.

- Each company or project shall be liable for its own security flaws and functionalities.
PEX presence is to analyze, audit and assess the client's smart contract's code.

Scope of Work

- The main focus of this report/audit, is to document an accurate assessment of the condition of
the smart contract and whether it has any security flaws in the implementation of the contract.
RIZQ Finance team agreed and provided us with the files that needed to be tested (Through Github, BscScan, files, etc.). **PEX** will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository where available, which has been provided by the project.
Code is reviewed manually and with the use of software using industry best practices.

Background

- **PEX** was commissioned by **RIZQ Finance** to perform an audit of smart contract:

  • Contract Address
  0xf5F8BC8878191aA0A461da8D0EFdED944E56C2EC

  The purpose of the audit was to achieve the following:
  • **Ensure that the smart contract functions as intended.**
  • **Identify potential security issues with the smart contract.**
  The information in this report should be used to understand the risk exposure of the smart
  contract, and as a guide to improve the security posture of the smart contract by remediating
  the issues that were identified.

RIZQ Finance

RIZQ Finance mission is to align with the principles of ethical finance and serve as a platform for Islamic microfinance and charity distribution. We aim to provide an ethical, inclusive and transparent ecosystem that promotes financial empowerment and social impact.

Social Media

Telegram - https://t.me/RizqFinance

Twitter - https://twitter.com/RIZQ_Finance

Contract Details

Project Name - RIZQ Finance

Token Description - Rewards Token

Compiler Version - v0.8.19

Current Holders - 8

Current Transaction Count - 20

Total Supply - 10000000000 Tokens

Token Ticker - RIZQ

Decimals - 9

Top 100 Holder % - 99.64%

LP Lock - DX Lock 18 Nov 2023

Contract Address

0xf5F8BC8878191aA0A461da8D0EFdED944E56C2EC

Contract Deployer Address

0x330FaD1927998cF2eF1B4da6bAe2963C7f067231

Contract Owner Address

0xd322d5c09438d942124a92e413d12fe641dac176

KYCd by - N/A

Launch Type - Fair

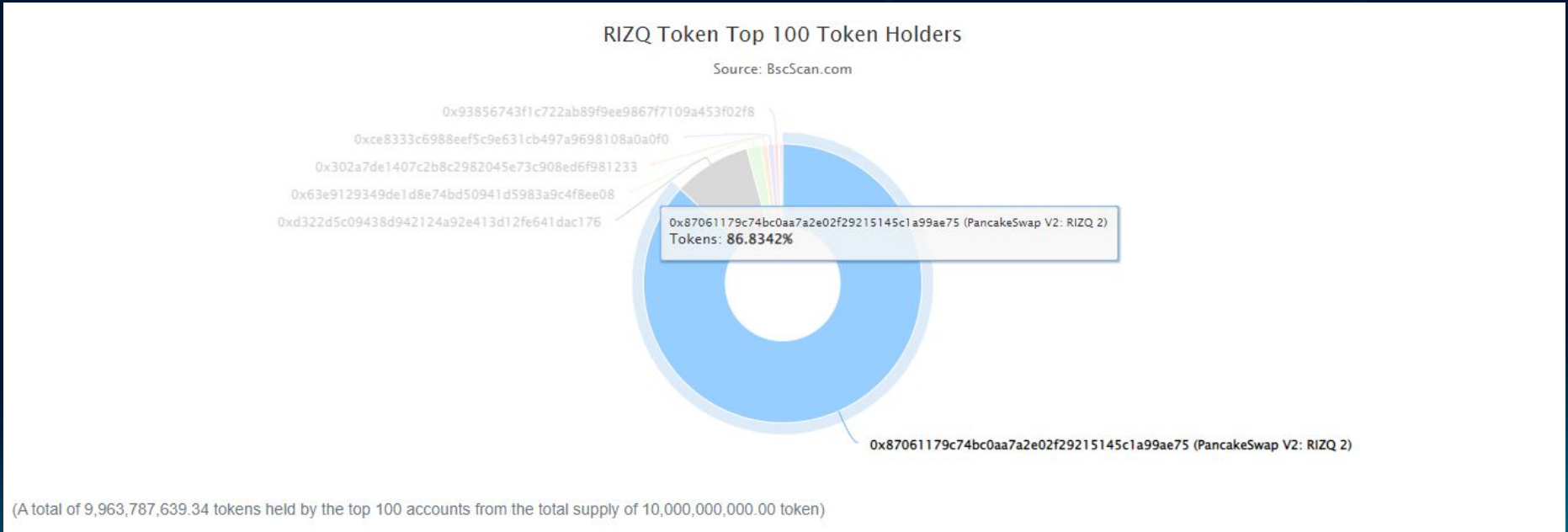
RIZQ LP Token Holders

1. 0x9050395004d000005db4ac8541af077175e0569e

99.0% of LP is Locked with DX Lock

2. 0xb44ea272f317e379567ce54acd94a2891597024e 1.0%

Top 100 Holders



Owner Privileges/Fees

Privileges

Ownership **HAS NOT BEEN** renounced. The owner has privileges or authority to make any changes. Owner entitled to **change Buy/Sell fees, and can exclude wallets from rewards**.

Fees

Buy - 9% Sell - 13%

Owner must keep fees at 15% or lower. This is **BELOW** our recommended max percentage of 25%.

PBX AUDIT

Adjustable Functions

(After Contract Deployment)

1. Contract SetUp 01 Prepare Presale Contract
2. Contract SetUp 02 Fees On Buys
3. Contract SetUp 03 Fees On Sells
4. Contract SetUp 04 Wallet Limits
5. Contract SetUp 05 Bot Protection
6. Contract SetUp 05 Open Trade
7. Contract SetUp 07 Blacklist Bots
8. Contract SetUp 08 End Launch Mode
9. Contract SetUp 09 Add Project Links
10. Maintenance Add Liquidity Pair
11. Maintenance Remove Contract Fee
12. Maintenance Update Wallets
13. Options Deflationary Burn
14. Options No Fee Wallet Transfers
15. Ownership Renounce
16. Ownership Transfer
17. Processing Auto Process
18. Processing Manual Process
19. Processing Remove Random Tokens
20. Processing Swap Trigger Count
21. Rewards Distribution Triggers
22. Rewards Exclude From Wallets
23. Rewards Set Gas
24. Wallet Exclude From Fees
25. Wallet Exempt From Limits
26. Wallet Pre Launch Access
27. Approve
28. Decrease Allowance
29. Increase Allowance
30. Transfer
31. Transfer From

Weakness/Vulnerabilities

SCAN RESULTS

SWC-129 —> Typographical Error = PASSED

SWC-130 —> Right-to-Left Override Control Character = 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 = LOW ISSUE

SWC-136 —> Unencrypted Private Data On-Chain= PASSED

Weakness/Vulnerabilities

CONTINUED

SWC-119 —> Shadowing State Variables = PASSED

SWC-120 —> Weak Source 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

Weakness/Vulnerabilities

CONTINUED

SWC-127 —> Arbitrary Jump with Function Type Variable = PASSED

SWC=128 —> DoS with Block Gas Limit = 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 Value for Time = PASSED

SWC-117 —> Signature Malleability = PASSED

SWC-118 —> Incorrect Constructor Name = PASSED

Weakness/Vulnerabilities

CONTINUED

SWC-105 —> Unprotected Ether Withdrawal = PASSED

SWC=106 —> Unprotected SELF DESTRUCT Instruction = PASSED

SWC-107 —> Reentrancy = PASSED

SWC-108 —> State Variable Default Visibility = LOW ISSUE

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

Weakness/Vulnerabilities

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 —> **Unlocked Call Return Value = PASSED**

Low issue = Low-level weakness/vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution.

SOLHINT LINTER, Solidity Static Analysis using REMIX IDE **did not find** any serious issues.

Overall Assessment

Satisfactory

RIZQ Finance has successfully passed the Pex Audit

Closing Notes

Whilst there are limitless ownable callable functions that have the potential to be dangerous, they are not overtly so. Trust in the team would mitigate many of these risks. Please make sure you do your own research. If in doubt please contact the project team.

Always make sure to inspect **all values and variables.**

This includes, but is not limited to: • Ownership • Proper Ownership Renouncement (if any) • Taxes • Transaction/Wallet Limits • Token Distributions • Timelocks • Liquidity Locks • Any other owner-adjustable settings or variables.