HackSafe

Smart Contract Security Audit Report

Anura finance

May **2022**

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
Anura finance

Deployer address
0x7920622F21a3C277B345c2Cae4ABfc768D90b1A2

Client contacts
Ribbit token team

Blockchain
Avalanche

Website
https://www.anuradao.finance/

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

HeckSafe was commissioned by Anura to perform an audit of smart contracts:

- https://snowtrace.io/address/0x302Abf007C2045F1bC0867a4b7abaaE2152e0EB3#code

Contract Details

Token contract details for 09.05.2022

Contract name	: Ribbit
Contract address	: 0x302Abf007C2045F1bC0867a4b7abaaE2152e0EB3
Total supply	: 200,000,000
Token Ticker	: RIBT
Decimals	: 18
Token Holders	: 113
Transactions count	: 840
Contract deployer address	: 0x7920622F21a3C277B345c2Cae4ABfc768D90b1A2

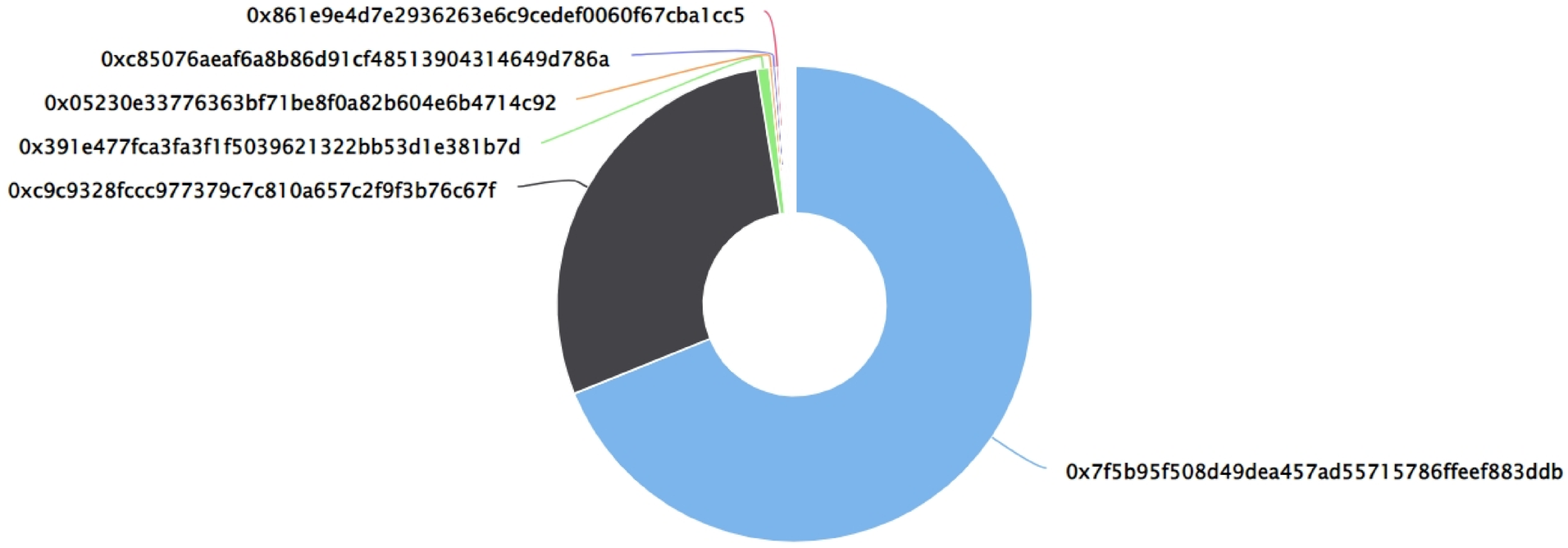
Ribbit Token Distribution

The top 100 holders collectively own 100.00% (199,999,881.63 Tokens) of Ribbit

Token Total Supply: 200,000,000.00 Token | Total Token Holders: 113

Ribbit Top 100 Token Holders

Source: snowtrace.io



Ribbit Top 10 Token Holders

(A total of 199,999,881.63 tokens held by the top 100 accounts from the total supply of 200,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x7f5b95f508d49dea457ad55715786ffeef883ddb	137,765,676.812821497313593236	68.8828%
2	0xc9c9328fccc977379c7c810a657c2f9f3b76c67f	57,188,239.881938173200397199	28.5941%
3	0x391e477fca3fa3f1f5039621322bb53d1e381b7d	1,634,870.377604652593983293	0.8174%
4	0x05230e33776363bf71be8f0a82b604e6b4714c92	466,400.685188231213862048	0.2332%
5	0xc85076aeaf6a8b86d91cf48513904314649d786a	448,415.41426	0.2242%
6	0x861e9e4d7e2936263e6c9cedef0060f67cba1cc5	336,541.725376463343471853	0.1683%
7	0xb1040c22a6d30a7d40453d12552f99fa605e60b1	242,833.270461200656218848	0.1214%
8	0x8e3ae3d689c9bbbdfeb0520c5f9798e82e961dc7	170,000	0.0850%
9	0x515bbfee5d361744542a4bd13b97be7fa35dd9c9	169,629.906	0.0848%
10	0x28e75c2631304cf5662d5db094ecd0e01d1a6fc0	163,875.50959	0.0819%

Contract functions details

+ Context
    <Constructor>
    -[Int] _msgSender
    -[Int] _msgData

+ [Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer
    -[Ext] allowance
    -[Ext] approve
    -[Ext] transferFrom

+ [Int] IERC20Metadata (IERC20)
    -[EXT] name
    -[Ext] symbol
    -[Ext] decimals

+ ERC20 (Context, IERC20, IERC20Metadata)
    -<constructor>
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals
    - [Pub] totalSupply
    - [Pub] balanceOf
    - [Pub] transfer #
    - [Pub] allowance
    - [Pub] approve #
    - [Pub] transferFrom #
    - [Pub] increaseAllowance #
    - [Pub] decreaseAllowance #
    - [Int] _transfer #
    - [Int] _mint #
    - [Int] _burn #
    - [Int] _approve #
    - [Int] _spendAllowance #
    - [Int] _beforeTokenTransfer #
    - [Int] _afterTokenTransfer #

Contract functions details

+ Ribbit (ERC20)
    -< constructor > #

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

Critical Severity Issues

No critical severity issue found.

High Severity Issues

No high severity issue found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version v0.8.0 the contract should contain the following line:

  pragma solidity 0.8.0;

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.