HackSafe

Smart Contract Security Audit Report

PUFFY FINANCE

January 2023

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
PUFFY FINANCE

Deployer address
0x8fed50506520af939ae8b783e1564e36cea881fd

Client contacts
PUFFY FINANCE Team

Blockchain
Polygon

Website
NOT PROVIDED

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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by PUFFY FINANCE to perform an audit of smart contracts:

- https://polygonscan.com/token/0x1dc030780fD54CA0e29E829cD69d6BC23f9d9e57#code

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 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.

Contract Details

Token contract details for 05.01.2023

Token Type	: DEFI
Contract name	: PUFFYFinance
Contract address	: 0x1dc030780fD54CA0e29E829cD69d6BC23f9d9e57
Total supply	: 50,000,000
Token ticker	: PUFFY
Decimals	: 18
Token Holders	: 263
Transactions count	: 295
Compiler version	: v0.4.24+commit.e67f0147
Contract deployer address	: 0x8fed50506520af939ae8b783e1564e36cea881fd
Owner address	: No owner

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“well Secure”**. This token contract does not contain owner control, which do make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 0 low.

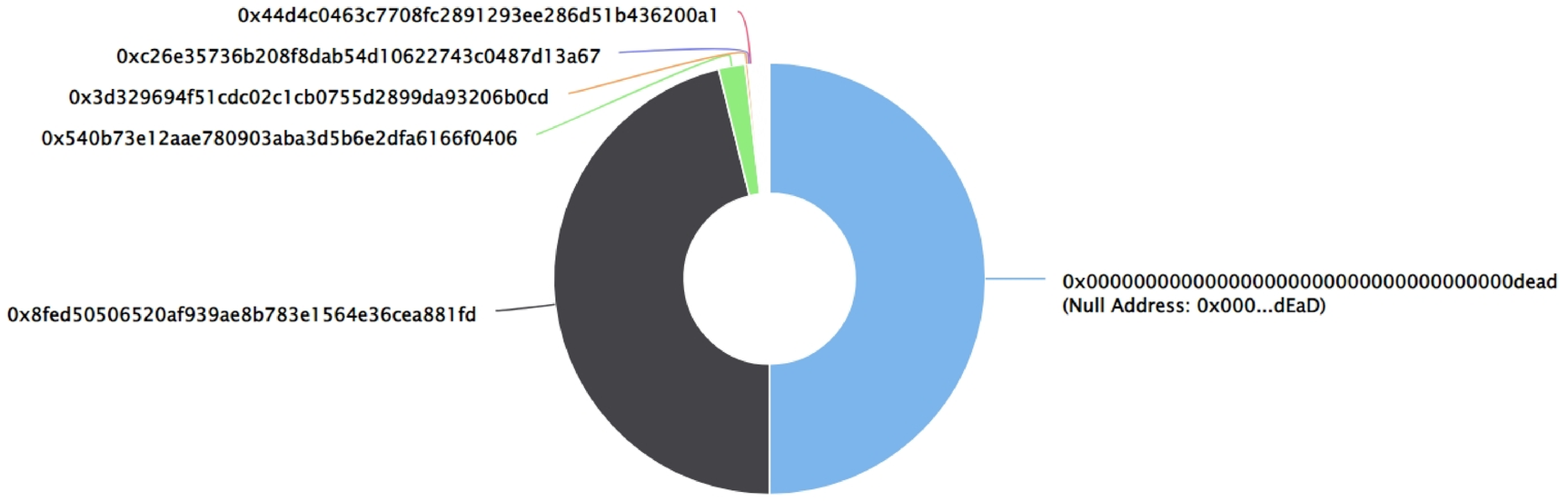
PUFFY FINANCE Token Distribution

The top 100 holders collectively own 99.99% (49,995,832.01 Tokens) of PUFFY Finance

Token Total Supply: 50,000,000.00 Token | Total Token Holders: 263

PUFFY Finance Top 100 Token Holders

Source: polygonscan.com



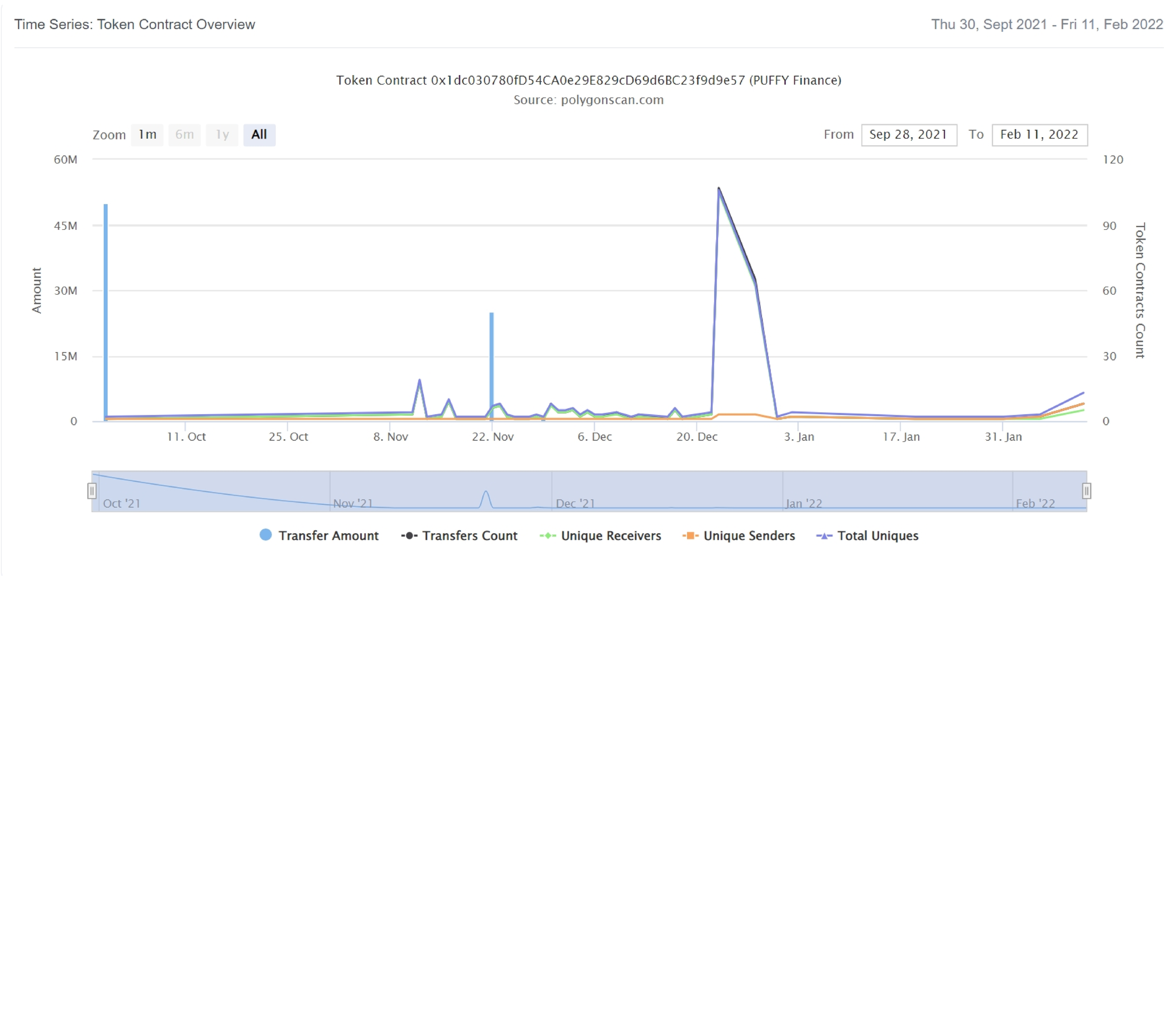
PUFFY FINANCE Top 20 Token Holders

(A total of 49,995,832.01 tokens held by the top 100 accounts from the total supply of 50,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	25,000,000	50.0000%
2	0x8fed50506520af939ae8b783e1564e36cea881fd	23,100,978.38	46.2020%
3	0x540b73e12aae780903aba3d5b6e2dfa6166f0406	1,000,000	2.0000%
4	0x3d329694f51cdc02c1cb0755d2899da93206b0cd	110,360	0.2207%
5	0xc26e35736b208f8dab54d10622743c0487d13a67	62,030	0.1241%
6	0x44d4c0463c7708fc2891293ee286d51b436200a1	58,700	0.1174%
7	0x74e77647103f3999b6c412e0c9e26d27521eea8c	52,310	0.1046%
8	0x273e5a914f5d97f73f008caf70a73d85c759b842	51,000	0.1020%
9	0xf67e547411028a7a0afdff9d0ee82e8ee88a8f5a	46,267	0.0925%
10	0x6f9f5884f28a1f9c5efafb6520bb51658ee77f59	37,100	0.0742%
11	0x6228a8394d870582c97dc84c8021e6a98e70fcba	36,920	0.0738%
12	0x1f7967dc7ca9fa52ecfd3d4959a2f48fb61441d9	35,700	0.0714%
13	0x1366ddbd523205d941ddb7c4b1cd3ab4feecf87d	34,350	0.0687%
14	0x112ad73f15edcd8ace45e44310dd16ff4766692c	31,720	0.0634%
15	0x86d6486bdf0468384a98881458dd35e00581083d	29,050	0.0581%
16	0x685e0e466216aa112eb01e250a7a1d80a5938ce6	28,730	0.0575%
17	0xdd8652a3fd0bbc7f560f4a0d25f993a179c58741	27,320	0.0546%
18	0xca0f081ca58e078c698e1f680cd79d9b0e90c0e3	26,800	0.0536%
19	0x43106b4a0707e77bda833348f7044c03c682e28d	22,320	0.0446%
20	0x330a927668b55377ff4372c2a8b6dd751f40899d	15,500	0.0310%

PUFFY FINANCE Token Distribution

PUFFY FINANCE Contract Overview



Contract functions details

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

+ [Lib] SafeMath
    - [Int] add
    - [Int] sub
    - [Int] mul
    - [Int] div
    - [Int] mod

+ ERC20 (IERC20)
    - [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] _burnFrom #

+ PUFFYFinance (ERC20)
    - [Pub] <constructor> $
    - [Pub] burn #
    - [Pub] name
    - [Pub] symbol
    - [Pub] decimals

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
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
20.	Too old version	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 issue found.
- **Low Severity Issues**
  No low severity issue found.

Conclusion

Smart contract contains no 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.