



Smart Contract Security Audit Report

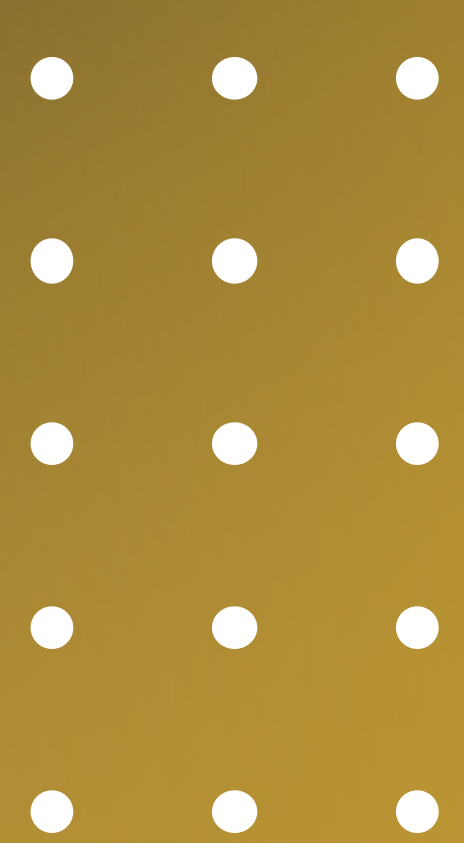
VIKINGS INU

December 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

VIKINGS INU



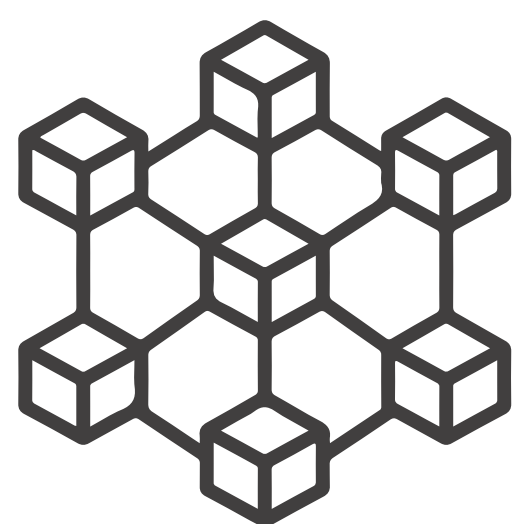
Deployer address

0xdd17cd4421c129405656d8bb664f991f59b9ccdb



Client contacts

VIKINGS INU Team



Blockchain

Binance smart chain



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 VIKINGS INU to perform an audit of smart contracts:

- <https://bscscan.com/token/0xc3583c8328ecb4dc8751c7e4fe7bcc18e558a4b6#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 understood 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.

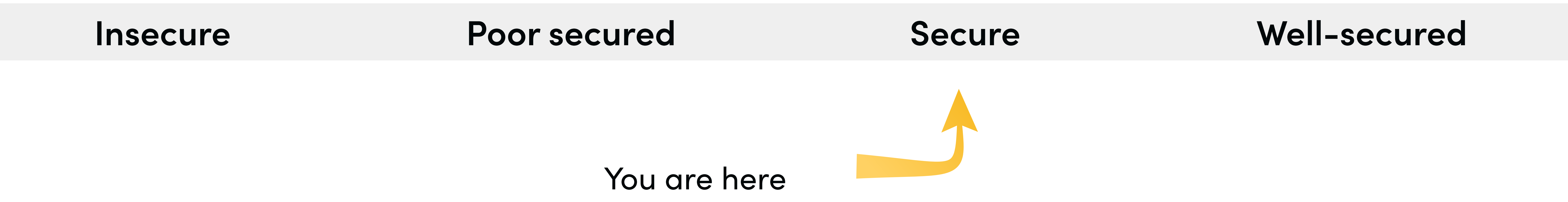
Contract Details

Token contract details for 17.12.2022

Token Type	: DEFI
Contract name	: VIKINGS
Contract address	: 0xc3583C8328eCB4DC8751C7e4fe7bCC18E558A4b6
Total supply	: 100,000,000,000,000
Token ticker	: VIKINGS
Decimals	: 9
Token Holders	: 73,619
Transactions count	: 99,981
Compiler version	: v0.6.12+commit.27d5176
Contract deployer address	: 0xdd17cd4421c129405656d8bb664f991f59b9ccdb
Owner address	: 0x00

Audit Summary

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



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, 1 medium and 1 low.

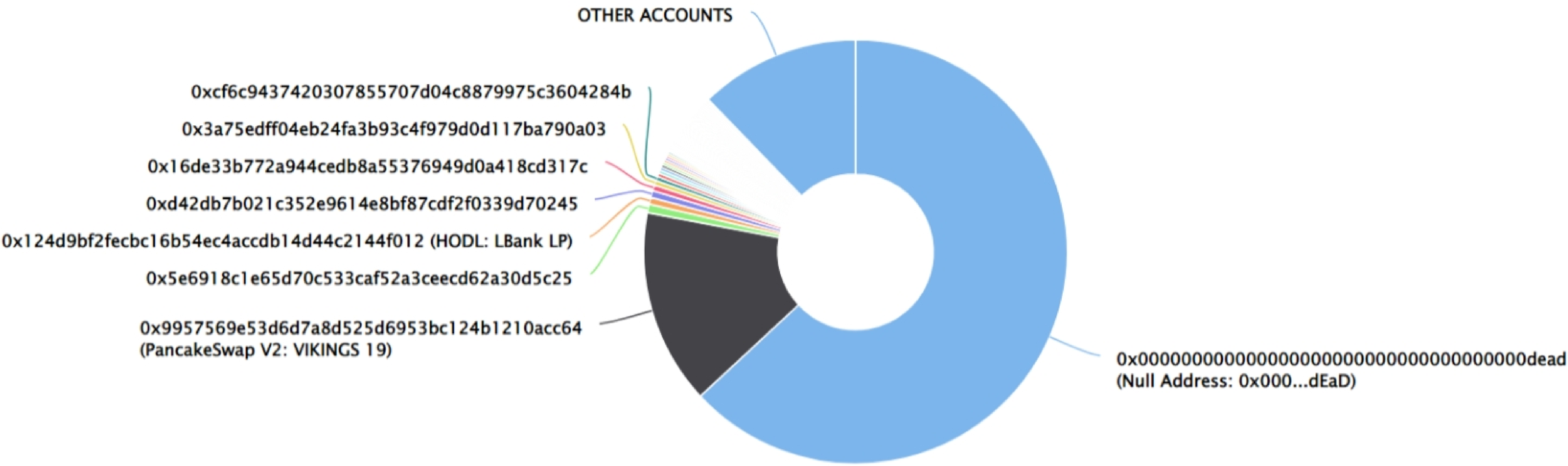
VIKINGS INU Token Distribution

The top 100 holders collectively own 87.77% (87,773,873,086,514.50 Tokens) of Vikings Inu

Token Total Supply: 100,000,000,000,000.00 Token | Total Token Holders: 73,619

Vikings Inu Top 100 Token Holders

Source: BscScan.com



VIKINGS INU Top 20 Token Holders

(A total of 87,773,873,086,514.50 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	63,109,508,477,636.148548565	63.1095%
2	PancakeSwap V2: VIKINGS 19	14,852,277,346,434.316287536	14.8523%
3	0x5e6918c1e65d70c533caf52a3ceecd62a30d5c25	659,823,427,469.793671113	0.6598%
4	HODL: LBank LP	527,480,307,807.239506812	0.5275%
5	0xd42db7b021c352e9614e8bf87cdf2f0339d70245	516,549,556,585.277557272	0.5165%
6	0x16de33b772a944cedb8a55376949d0a418cd317c	453,540,603,182.575289974	0.4535%
7	0x3a75edff04eb24fa3b93c4f979d0d117ba790a03	340,043,151,665.529131408	0.3400%
8	0xcf6c9437420307855707d04c8879975c3604284b	324,104,760,407.794923674	0.3241%
9	0x7a4e3e7604de12022c5b223ee22e89ed213438eb	265,765,662,025.596448409	0.2658%
10	0xf4ace8214ec8d7412fa1cacf4027ad732de6f085	262,525,691,235.385403275	0.2625%
11	0xa9c7e5d79d243705ecbc6fbe6aefa64419945fe0	238,413,989,923.71825612	0.2384%
12	0xb0416b8c72dd011bf67aa676d24be8ce5da9fb5c	212,166,516,873.635072709	0.2122%
13	0x56588c9bfab863d4c3d4ac7c5ed82a5c5b5eb39d	204,380,316,049.719940924	0.2044%
14	0xfcc8316fb3c0b4204244649c8544a8a1cc110716	196,743,357,616.220168672	0.1967%
15	0x00dd03a1740936ee2953051468e72509d4492a8d	190,834,731,350.600297524	0.1908%
16	0xb21a817be01556f3d82ac63fe2f4dd775ac2420d	186,830,370,091.25087431	0.1868%
17	0x308d9bb2260e171da43d4be0d5567c3c103f1f16	172,398,139,532.653285613	0.1724%
18	0x4749a82445727915ba4c955ec0a26c7dbb150752	153,734,219,229.520886924	0.1537%
19	0x6ba4fc0e7670fa1fa794b27bcbfedb4bf7595806	123,766,964,073.992450236	0.1238%
20	0x82c6ef8e0d5bc7c39e505e01d9bf247bc84b096a	122,415,399,795.11422101	0.1224%

VIKINGS INU Token Distribution

VIKINGS INU Contract Overview



Contract functions details

+Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] Address

- [Int] isContract
- [Int] sendValue #
- [Int] functionCall #
- [Int] functionCall #
- [Int] functionCallWithValue #
- [Int] functionCallWithValue #
- [Pvt] _functionCallWithValue

+Ownable (Context)

- [Pub] <Constructor > #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner

Contract functions details

+VIKINGS (Context, IERC20, Ownable)

- [Pub] <constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] allowance
- [Pub] approve #
- [Pub] transferFrom #
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] isExcluded
- [Pub] totalFees
- [Ext] setMaxTxPercent #
 - modifiers: onlyOwner
- [Pub] reflect #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
 - modifiers: onlyOwner
- [Ext] includeAccount #
 - modifiers: onlyOwner
- [Pvt] _approve #
- [Pvt] _transfer #
- [Pvt] _transferStandard #
- [Pvt] _transferToExcluded #
- [Pvt] _transferFromExcluded #
- [Pvt] _transferBothExcluded #
- [Pvt] _reflectFee #
- [Pvt] _getValues
- [Pub] burnOwnerTokens #
 - modifiers: onlyOwner,ownershipNotTransferred
- [Pub] _transferFrom #
 - modifiers: onlyOwner,ownershipNotTransferred
- [Pvt] _getTValues
- [Pvt] _getRValues

Contract functions details

- [Pvt] _getRValues
- [Pvt] _getRate
- [Pvt] _getCurrentSupply
- [Ext] setUniswapPair #
 - modifiers: onlyOwner

(\$) = 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.	Medium Issue
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

One medium severity issue found.

1. Out of gas

• Description

The function `includeInAccount()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

• Recommendation

Check that the excluded array length is not too big.

✔ 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 `^0.6.12` the contract should contain the following line:

```
pragma solidity 0.6.12;
```

Notes:

- Transfers can go to zero address.

Centralization

Owner privileges :

- VIKINGS INU Contract:
 - Owner can change max transaction amount.
 - Owner can include in and exclude from reward.
 - Owner can burn owner tokens.
 - Owner can transfer from any address to any address.
 - Owner can change Uniswap pair.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would not create trouble, as smart contract ownership has been renounced. Following are Admin functions:

- renounceOwnership
- transferOwnership
- setmaxTxPercent
- excludeAccount
- includeAccount
- burnOwnerTokens
- setUniswapPair
- _transferFrom

Conclusion

Smart contract contains low and medium 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.