



Smart Contract Security Audit Report

Vaulty Token

September 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Vaulty Token



Deployer address

0xeba5e937F85a77363e63bD2C633a89fD67447441



Client contacts

Vaulty Token Team



Blockchain

Binance Smart Chain



Website

<https://vaulty.fi/>

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 Vaulty Token to perform an audit of smart contracts:

- <https://bscscan.com/address/0x38A5cbe2FB53d1d407Dd5A22C4362daF48EB8526#code>

The purpose of the audit was to achieve the

- 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 15.09.2022

Token Type	: ERC20
Contract name	: RewardToken
Contract address	: 0x38A5cbe2FB53d1d407Dd5A22C4362daF48EB8526
Compiler version	: v0.6.12+commit.27d51765
Total supply	: 15,000,000
Token ticker	: VLTY
Decimals	: 18
Token holders	: 1,271
Transactions count	: 32,345
Contract deployer address	: 0xeba5e937F85a77363e63bD2C633a89fD67447441
Owner address	: 0xeba5e937f85a77363e63bd2c633a89fd67447441

Social profiles

Github profile	: https://github.com/VaultyFinance
linkedin profile	: https://www.linkedin.com/company/vaultyfi
Telegram profile	: https://t.me/VaultyCHAT_NEW
Coinmarketcap profile	: https://coinmarketcap.com/currencies/vaulty-finance/
Coingecko profile	: https://www.coingecko.com/en/coins/vaulty-token/

Audit Summary

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

Insecure	Poor	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 1 low and some very low-level issues. These issues are not critical ones.

Vaulty Token Token Distribution

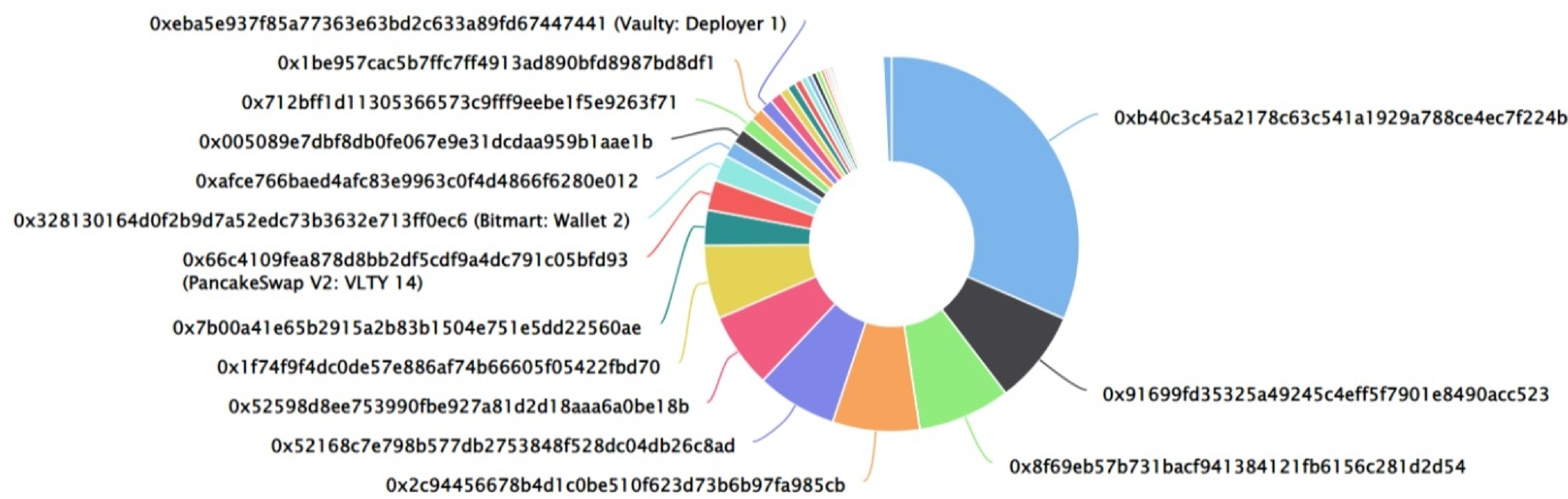
 The top 100 holders collectively own 99.24% (14,886,366.80 Tokens) of Vaulty Token

 Token Total Supply: 15,000,000.00 Token

Total Token Holders: 1,271








Vaulty Token Top 100 Token Holders

Source: BscScan.com



Vaulty Token Top 20 Token Holders

(A total of 14,886,366.80 tokens held by the top 100 accounts from the total supply of 15,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 0xb40c3c45a2178c63c541a1929a788ce4ec7f224b	4,728,098.360655737704917777	31.5207%
2	 0x91699fd35325a49245c4eff5f7901e8490acc523	1,213,236.332952050472346705	8.0882%
3	 0x8f69eb57b731bacf941384121fb6156c281d2d54	1,200,000	8.0000%
4	 0x2c94456678b4d1c0be510f623d73b6b97fa985cb	1,125,000	7.5000%
5	 0x52168c7e798b577db2753848f528dc04db26c8ad	1,041,580.855142355133021227	6.9439%
6	0x52598d8ee753990fbe927a81d2d18aaa6a0be18b	973,000.0000000000000097936	6.4867%
7	0x1f74f9f4dc0de57e886af74b66605f05422fbd70	953,882.939554577400740573	6.3592%
8	0x7b00a41e65b2915a2b83b1504e751e5dd22560ae	454,426.229508196721311452	3.0295%
9	 PancakeSwap V2: VLTy 14	389,133.867993684300919423	2.5942%
10	Bitmart: Wallet 2	337,410.643799095687729281	2.2494%
11	0xafce766baed4afc83e9963c0f4d4866f6280e012	205,012.200326768720000287	1.3667%
12	0x005089e7dbf8db0fe067e9e31dcdaa959b1aae1b	194,118	1.2941%
13	0x712bff1d11305366573c9fff9eebe1f5e9263f71	178,512.6900000000002328306	1.1901%
14	0x1be957cac5b7ffc7ff4913ad890bfd8987bd8df1	170,000.809999999997671694	1.1333%
15	Vaulty: Deployer 1	163,635.557310693393695317	1.0909%
16	0x4e6037e4172eaa18d89aacf626d59ffa6c8ae58	156,274.813858525218853179	1.0418%
17	 0x2af376040742eba16315c8b6c7ae37319583b0ba	112,499.876901969384	0.7500%
18	0x885bb7c0fc016657043b7f54c803fb326c8d3101	107,451	0.7163%
19	0x4a5bb1c9347a0d4f7e06a29239162f03647d9232	89,649.4706	0.5977%
20	0x2769698e204ad16c30dff373139e07176358585a	78,920.3909774436	0.5261%

Contract functions details

RewardToken.sol

+ RewardToken (BEP20, MinterRole)

-< constructor>

-[Pub] mint #

-modifiers: onlyOwner

BEP20.sol

+BEP20 (Context, IBEP20, Ownable)

-[Pub] <constructor>

-[Ext] getOwner

-[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] _beforeTokenTransfer #

-[Int] _mint#

-[Int] _burn #

-[Int] _approve #

-[Int] _burnFrom #

MinterRole.sol

+ MinterRole (Context)

-[Int] <constructor>

-[Pub] isMinter

-[Pub] addMinter #

-modifiers: onlyMinter

-[Pub] renounceMinter #

-[Int] _addMinter #

-[Int] _removeMinter #

Contract functions details

Ownable.sol

+ Ownable (Context)

- [Pub] <constructor>
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Int] _transferOwnership #

IBEP20.sol

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

Context.sol

+ Context

- [Pub] <constructor>
- [Int] _msgSender
- [Int] _msgData

SafeMath.sol

+ [Lib] SafeMath

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

Contract functions details

-[Int] min

-[Int] sqrt

Address.sol

+[Lib] Address

-[Int] isContract

-[Int] sendValue

-[Int] functionCall

-[Int] functionCall

-[Int] functionCallWithValue

-[Int] functionCallWithValue

Roles.sol

+[Lib] Roles

-[Int] add

-[Int] remove

-[Int] has

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	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	Low issue

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. Old compiler version

- **Description**

Contract has been deployed using too old solidity version.

- **Recommendation**

It is advisable to deploy contract using any of the latest version of solidity.

Centralization

Owner/Minter Privileges :

- Vaulty Token Contract:
 - Owner can renounce and transfer ownership.
 - Minter can mint tokens.
 - Minter can add minter

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

- Transferownership
- Renounceownership
- Addminter
- Mint

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.