HackSafe

Smart Contract Security Audit Report

DotDot

April **2022**

Security Status

★★★★½

www.hacksafe.io

Audit Details

Audited project
DotDot

Deployer address
0xDDdEE11246506Dd446D91d75CA2FEa886dAB8F5d

Client contacts
DotDot token team

Blockchain
Binance smart chain

Website
Not provided by dotdot token team.

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 DotDot to perform an audit of smart contracts:

- https://bscscan.com/address/0x84c97300a190676a19D1E13115629A11f8482Bd1#code

Contract Details

Token contract details for 25.04.2022

Contract name	: DotDot
Contract address	: 0x84c97300a190676a19D1E13115629A11f8482Bd1
Total supply	: 30,734,215.709609
Token Ticker	: DDD
Decimals	: 18
Token Holders	: 712
Transactions count	: 12,564
Contract deployer address	: 0xDDdEE11246506Dd446D91d75CA2FEa886dAB8F5d
Owner address	: 0x0000000000000000000000000000000000000000

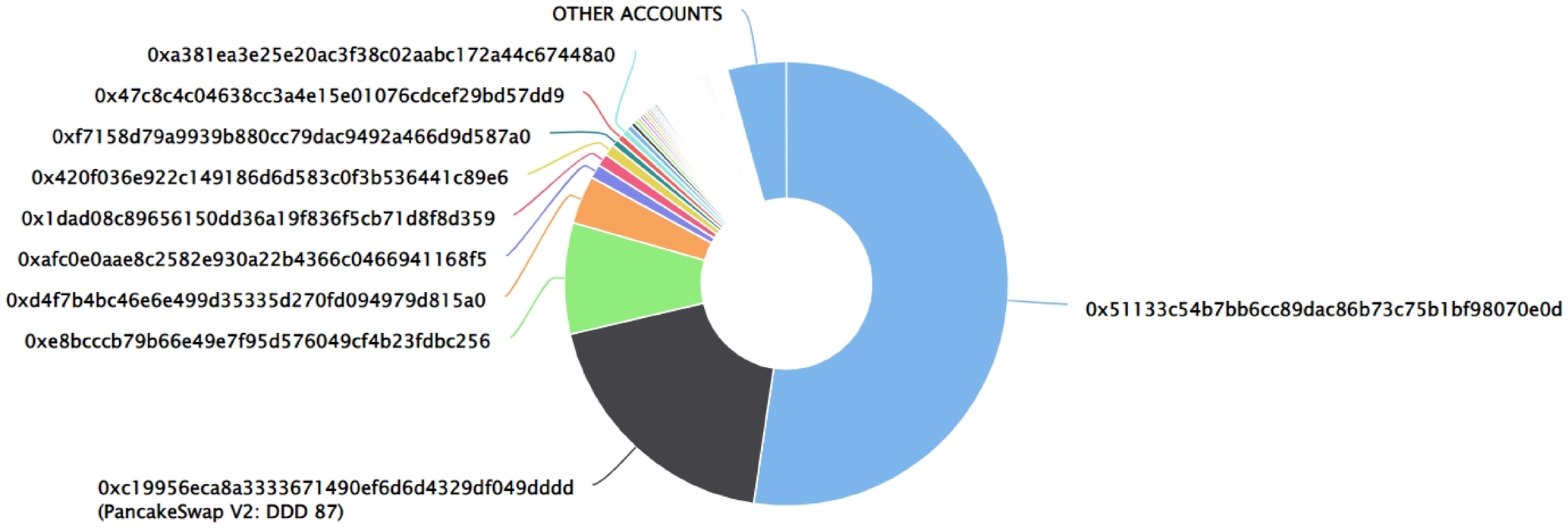
DotDot Token Distribution

The top 100 holders collectively own 95.72% (29,420,815.64 Tokens) of DotDot

Token Total Supply: 30,737,582.63 Token | Total Token Holders: 739

DotDot Top 100 Token Holders

Source: BscScan.com



DotDot Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x51133c54b7bb6cc89dac86b73c75b1bf98070e0d	16,101,118.778037611801060611	52.3825%
2	PancakeSwap V2: DDD 87	5,835,031.820741777078516806	18.9834%
3	0xe8bcccb79b66e49e7f95d576049cf4b23fdbc256	2,482,047.605479747629653098	8.0750%
4	0xd4f7b4bc46e6e499d35335d270fd094979d815a0	1,084,605.265747470798857543	3.5286%
5	0xafc0e0aae8c2582e930a22b4366c0466941168f5	308,660.569337847384609044	1.0042%
6	0x1dad08c89656150dd36a19f836f5cb71d8f8d359	279,550.012457468935829509	0.9095%
7	0x420f036e922c149186d6d583c0f3b536441c89e6	257,792.34852484254418403	0.8387%
8	0xf7158d79a9939b880cc79dac9492a466d9d587a0	162,573.851754423762025679	0.5289%
9	0x47c8c4c04638cc3a4e15e01076cdcef29bd57dd9	153,916.61299816279143175	0.5007%
10	0xa381ea3e25e20ac3f38c02aabc172a44c67448a0	150,100.976555547450643447	0.4883%

Contract functions details

DddToken.sol
+ DotDot (IERC20, Ownable)
    - <constructor>
    -[Ext] setMinters #
      -modifiers: onlyOwner
    -[Ext] mint #
    -[Ext] approve #
    -[Int] _transfer #
    -[Pub] transfer #
    -[Pub] transferFrom #

Ownable.sol
+ Ownable
    -<Constructor> #
    -[Pub] owner
    -[Pub] renounceOwnership #
      -modifiers: onlyOwner
    -[Pub] transferOwnership #
      -modifiers: onlyOwner

IERC20.sol
+ [Int] IERC20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer #
    -[Ext] allowance
    -[Ext] approve #
    -[Ext] transferFrom #
    -[Ext] name
    -[Ext] symbol
    -[Ext] decimals

($) = 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.	Medium issue
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

One medium severity issues found.

1. Design logic

- **Description:**

  In contract DddToken.sol, in constructor there is and event called transfer which transferring 0 amount to (oxo) address, which does not mean anything.

- **Location:**

  DdToken.sol -> constructor

- **Recommendation:**

  We advise you to remove that constructor as emitting an event which doesn't mean anything can cost a gas fees.

Low Severity Issues

No low severity issues found.

Conclusion

Smart contract contains 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.