



Smart Contract Security Audit Report

OddzToken

August 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

OddzToken



Deployer address

0xCD89C8ff8b7B01Ba842b7A5De9270F0CF0f75F51



Client contacts

Oddz Token team



Blockchain

Avalanche



Website

<https://oddz.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 Oddz to perform an audit of smart contract:

- <https://snowtrace.io/address/0xb0a6e056b587d0a85640b39b1cb44086f7a26a1e#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 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 08.08.2022

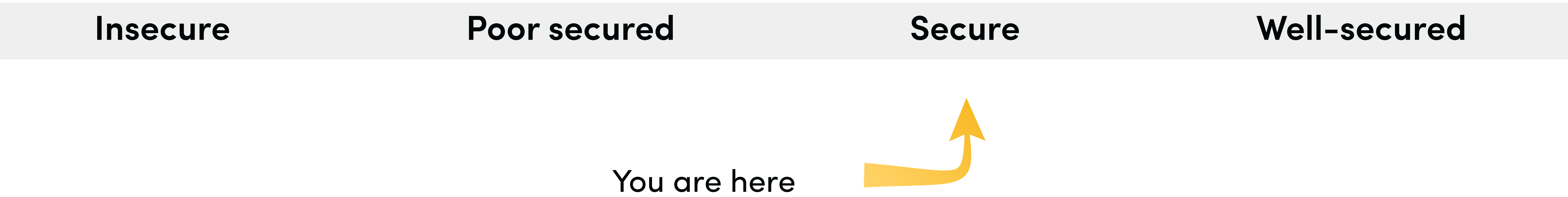
Token Type	: ERC20
Contract name	: ERC677
Contract address	: 0xB0a6e056B587D0a85640b39b1cB44086F7a26A1E
Compiler version	: v0.7.6+commit.7338295f
Total supply	: 10,720,425.836992
Token Ticker	: ODDZĂ
Decimals	: 18
Token Holders	: 476Ă
Top 100 token holder's dominance	: 99.76%
Transactions count	: 12,762
Contract deployer address	: 0xCD89C8ff8b7B01Ba842b7A5De9270F0CF0f75F51
Owner address	: 0x7a082fdb0c0a4678dc5d5b0d38c404e7d55b8628

Social profiles

Coinmarketcap profile	: https://coinmarketcap.com/currencies/oddz/
Coingecko profile	: https://www.coingecko.com/en/coins/oddz/
Twitter profile	: https://twitter.com/oddz_finance
Github profile	: https://github.com/oddz-finance
Telegram profile	: https://t.me/oddz_finance

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.



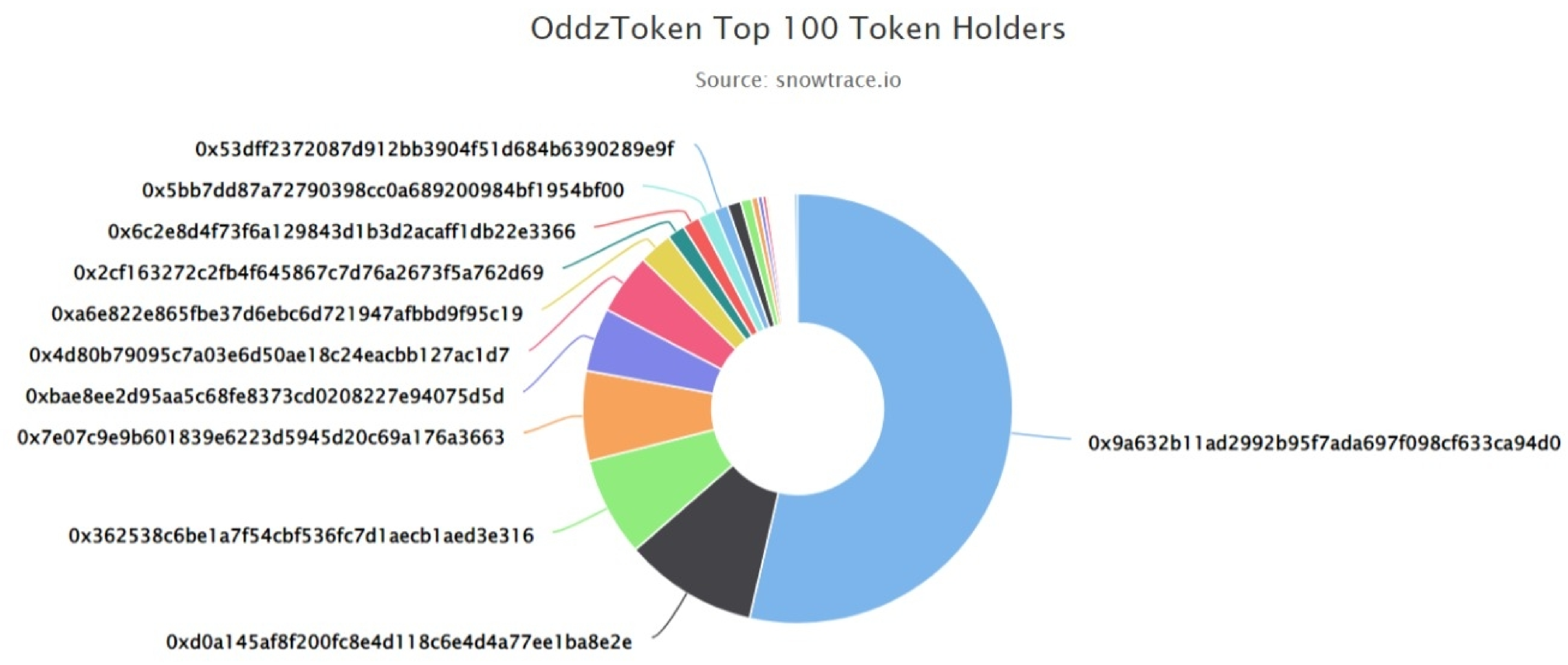
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

Oddz Token Distribution












 The top 100 holders collectively own 99.76% (10,694,614.98 Tokens) of OddzToken

 Token Total Supply: 10,720,425.84 Token | Total Token Holders: 476



Oddz Token Top 20 Token Holders

(A total of 10,694,614.98 tokens held by the top 100 accounts from the total supply of 10,720,425.84 token)

Rank	Address	Quantity (Token)	Percentage
1	 0x9a632b11ad2992b95f7ada697f098cf633ca94d0	5,746,241.0889840799999993744	53.6009%
2	 0xd0a145af8f200fc8e4d118c6e4d4a77ee1ba8e2e	1,073,992.969982023721958	10.0182%
3	0x362538c6be1a7f54cbf536fc7d1aecb1aed3e316	799,121.498500557264075077	7.4542%
4	0x7e07c9e9b601839e6223d5945d20c69a176a3663	724,838.863255505666977	6.7613%
5	 0xbae8ee2d95aa5c68fe8373cd0208227e94075d5d	514,433.802042776508536222	4.7986%
6	 0x4d80b79095c7a03e6d50ae18c24eacbb127ac1d7	491,212.640336242438928081	4.5820%
7	 0xa6e822e865fbe37d6ebc6d721947afbbd9f95c19	271,420.203426443273455663	2.5318%
8	 0x2cf163272c2fb4f645867c7d76a2673f5a762d69	143,000	1.3339%
9	0x6c2e8d4f73f6a129843d1b3d2acaff1db22e3366	140,573.359451238318059072	1.3113%
10	0x5bb7dd87a72790398cc0a689200984bf1954bf00	138,269.531398973836426352	1.2898%
11	 0x53dff2372087d912bb3904f51d684b6390289e9f	110,172.852429276382597097	1.0277%
12	 0x48ca54f44e1e25957d47216ecedebe6411f2d7fc	108,633.194809243301179988	1.0133%
13	 0xb61550a6640228d63d0fce197d6a1a42fe920d5c	89,037.326018875	0.8305%
14	0x423a614b057b1c43f08464cf7a45caf3c9e9276c	52,018.320953927763130181	0.4852%
15	0xabd41b007cb631dc17ba4f22ca141bcacd02ac3	36,854.121670002673569297	0.3438%
16	 0xdf6e2ca39faad5feb3336d60ed9aab1404f2d36d	31,036.281637495412176299	0.2895%
17	0x55977f1e06422af6611853b2f2c87ae01c6804f1	18,062.70678125	0.1685%
18	0x92191b2d10dfb8cbb220f17590707a96fe853bf2	16,203.44636249017080806	0.1511%
19	 0x14faf13925dfcdc4c459e1fa0a3b9c8b2f57d7e7	14,179.353655069169579208	0.1323%
20	0xb68226672b49976ce8a1aaa85c2b86ffdb7d354b	13,417.722014853507579904	0.1252%

Contract functions details

ERC677.sol

+ ERC677 (ERC20, Ownable)

-<constructor>

-[Pub] mint #

-modifiers: onlyOwner

-[Pub] burn #

-modifiers: onlyOwner

-[Int] _beforeTokenTransfer

-[Ext] transferAndCall

Misc.sol

+ [Lib] Misc

-[Ext] isContract

-[Ext] today

Context.sol

+ Context

-[Int] _msgSender

-[Int] _msgData

IERC20.sol

+ [Int] IERC20

-[Ext] totalSupply

-[Ext] balanceOf

-[Ext] transfer

-[Ext] allowance

-[Ext] approve

-[Ext] transferFrom

ERC20.sol

+ ERC20 (Context, IERC20)

-[Pub] <constructor>

-[Pub] name

-[Pub] symbol

-[Pub] decimals

-[Pub] totalSupply

-[Pub] balanceOf

-[Pub] transfer #

-[Pub] allowance

-[Pub] approve #

Contract functions details

- [Pub] transferFrom #
- [Pub] increaseAllowance
- [Pub] decreaseAllowance
- [Int] _transfer #
- [Int] _mint#
- [Int] _burn #
- [Int] _approve #
- [Int] _setupDecimals #
- [Int] _beforeTokenTransfer #

SafeMath.sol

+[Lib] SafeMath

- [Int] tryAdd
- [Int] trySub
- [Int] tryMul
- [Int] tryDiv
- [Int] tryMod
- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] mod
- [Int] sub
- [Int] div
- [Int] mod

Ownable.sol

+Ownable (Context)

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

(\$) = 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.	Low issue
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

Two low severity issue found.

1. Too old compiler version.

- **Description**

Contract has been deployed using too old compiler version.

- **Recommendation**

It is advisable that the compiler version of solidity should be among the new compiler versions.

2. Safe Open Zeppelin contracts implementation and usage.

- **Description**

The SamuraiLegendsNFTs.sol contract has direct imported openzeppelin file.

- **Recommendation**

We advise you to not use direct import of any github repository because any changes in that file may effect your contract too.

Centralization

Owner privileges:

- Oddz Contract:
 - Owner can remove and transfer ownership.
 - Owner can mint new tokens.
 - Owner can burn their tokens.

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 create trouble but smart contract ownership has been renounced. Following are Admin functions functions:

- Transferownership
- Renounceownership
- Mint
- Burn

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.