



Smart Contract Security Audit Report

Shiba Token

June 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Shiba Token



Deployer address

0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08



Client contacts

Shiba Token



Blockchain

Binance Smart Chain



Website

<https://shibatoken.com/>

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 Shiba Token to perform an audit of smart contract:

- <https://bscscan.com/address/0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE#code>

Contract Details

Token contract details for 01.06.2022

Contract name	: TokenMintERC20Token
Contract address	: 0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE
Compiler version	: v0.5.0+commit.1d4f565a
Max Total supply	: 999,991,506,805,250.637003571285309628
Token Ticker	: SHIB
Decimals	: 18
Token Holders	: 1,172,880
Transactions count	: 7,687,713
Contract deployer address	: 0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08
owner address	: 0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08
Fee receiver address	: 0x6603cb70464ca51481d4edBb3B927F66F53F4f42

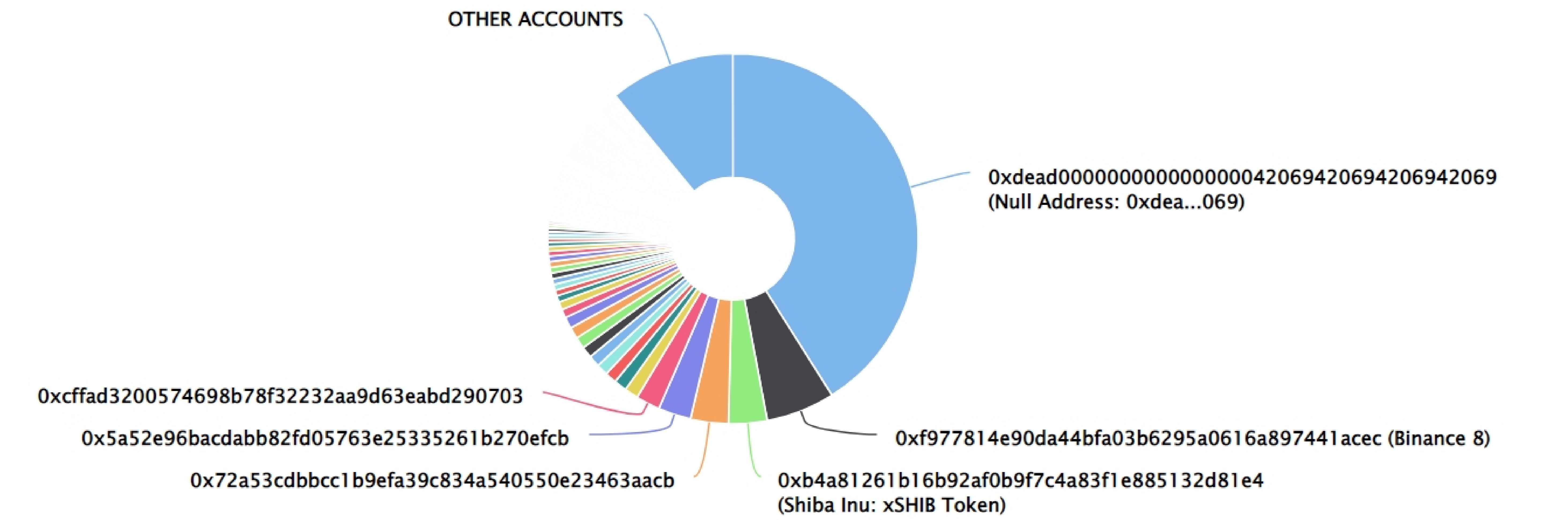
Social profiles

UniSwap profile	https://v2.info.uniswap.org/pair/0x811beed0119b4afce20d2583eb608c6f7af1954f/
CoinGecko profile	: https://www.coingecko.com/en/coins/shiba-inu
CoinMarketCap profile	: https://coinmarketcap.com/currencies/shiba-inu/
Telegram profile	: https://t.me/shibainuthedogecoinkiller



SHIBA INU Token Distribution

SHIBA INU Top 500 Token Holders

Source: Etherscan.io



SHIBA INU Top 20 Token Holders

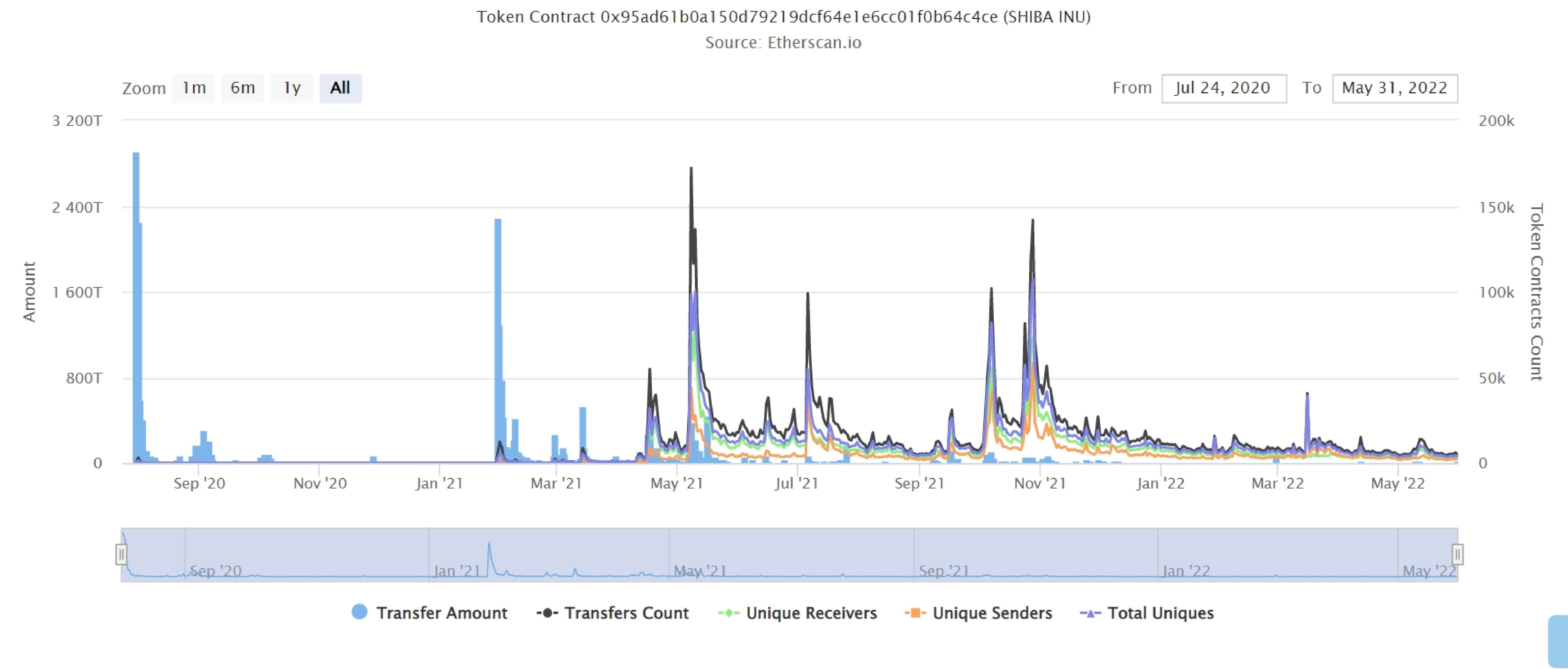
Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0xdea...069	410,318,476,786,158.804206917308114527	41.0322%
2	Binance 8	60,000,000,000,000	6.0001%
3	 Shiba Inu: xSHIB Token	33,610,060,488,125.190946567655785176	3.3610%
4	0x72a53cdbbcc1b9efa39c834a540550e23463aacb	32,971,011,995,001.00000061	3.2971%
5	0x5a52e96bacdabb82fd05763e25335261b270efcb	28,732,607,947,509.594991043653905515	2.8733%
6	0xcffad3200574698b78f32232aa9d63eabd290703	20,937,198,273,553	2.0937%
7	0x2efb50e952580f4ff32d8d2122853432bbf2e204	12,115,998,359,411.09000048	1.2116%
8	 0x422193843fe209faa94f5cc1780e04965e77cb7f	11,140,398,724,484.3	1.1140%
9	0x1406899696adb2fa7a95ea68e80d4f9c82fcdedd	10,200,003,370,217.047101987682715194	1.0200%
10	0xf28d22c8b25ff8fa961e305bba701918ddc3339a	10,000,001,252,958.153846153846153846	1.0000%
11	0xc1cae0a347db30cf2cbbd80127fe2182804f8a9e	10,000,000,317,405.10657545	1.0000%
12	0x99c1406452470cfce0fadd355c41077593680e76	10,000,000,199,911	1.0000%
13	0x31987132665ae1cbbb64b73f728cc81340486cef	10,000,000,199,210.11	1.0000%
14	0x5ee8e72d606779a6f3cd8bba1c6bd4818b8bad0f	10,000,000,000,837.4998447	1.0000%
15	0x09eab02d34393d2ac666fd9525443dba9713b155	10,000,000,000,008	1.0000%
16	Crypto.com	7,412,897,049,276.577392820037183835	0.7413%
17	OKEx	7,143,385,786,417.612545514898253481	0.7143%
18	0xbc44b3d04c978bfc071dff27a30c76a151fa1b4	5,500,000,400,000	0.5500%
19	0x2d7af085f2256f114c8a9f540969f0e0ab1c2e5e	5,000,004,289,798.5840046569	0.5000%
20	0xe1474359c74e78fa8387d9cb58f393693e378de3	5,000,000,000,062.11	0.5000%

SHIBA INU Token Distribution

SHIBA INU Token Transfer Data

Time Series: Token Contract Overview

Fri 31, Jul 2020 - Tue 31, May 2022



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 #

+ TokenMintERC20Token (ERC20)

- [Pub] <constructor> \$
- [Pub] burn #
- [Pub] name
- [Pub] symbol
- [Pub] decimals

(\$) = 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.	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

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. 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 ^0.5.0 the contract should contain the following line:

```
pragma solidity 0.5.0;
```

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.