MOONAUDIT

Smart Contract Audit Report

SHIBA INU (SHIB)

ERC20 on Ethereum

May 1st, 2022

https://MoonAudit.org

Table of Contents

1.Overview

- 1.1 Project Summary
- 1.2 Audit Summary
- 1.3 Vulnerability Summary

2.Findings

- 2.1 Fully Sanity Checks
- 2.2 Source Code Analysis
- 2.3 Contract Ownership
- 2.4 Liquidity Ownership
- 2.5 Mint Function
- 2.6 Burn Function

3.Project Overview

- 3.1 Present Mode
- 3.2 Team Location
- 3.3 General Web Security

4.Disclaimer

5.About

Overview

Project Summary	
Project Name	SHIBA INU (SHIB)
Platform	Ethereum
Language	Solidity v0.5.0
Contract Type	ERC20
Contract Address	0x95aD61b0a150d79219dCF64E1E6Cc01f0B64C4cE
Contract Owner	0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08
Block Explorer	https://etherscan.io/

Audit Summary	
Delivery Date	May 1st, 2022 UTC+0
Block Number	10569013
Static Analysis	Yes
Graphic Analysis	Yes
Logic Disassemble	Yes
Mannual Review	Yes

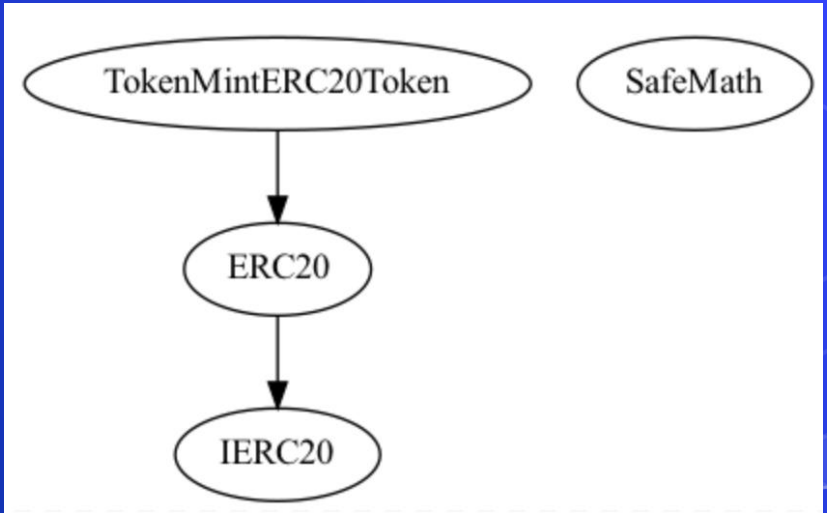
Vulnerability Summary

Severity Level	Total	Acknowledged	Alleviated	Resolved
Critical	0	0	0	0
Major	0	0	0	0
Medium	0	0	0	0
Minor	0	0	0	0
Informational	3	3	0	0
Discussion	1	1	0	0

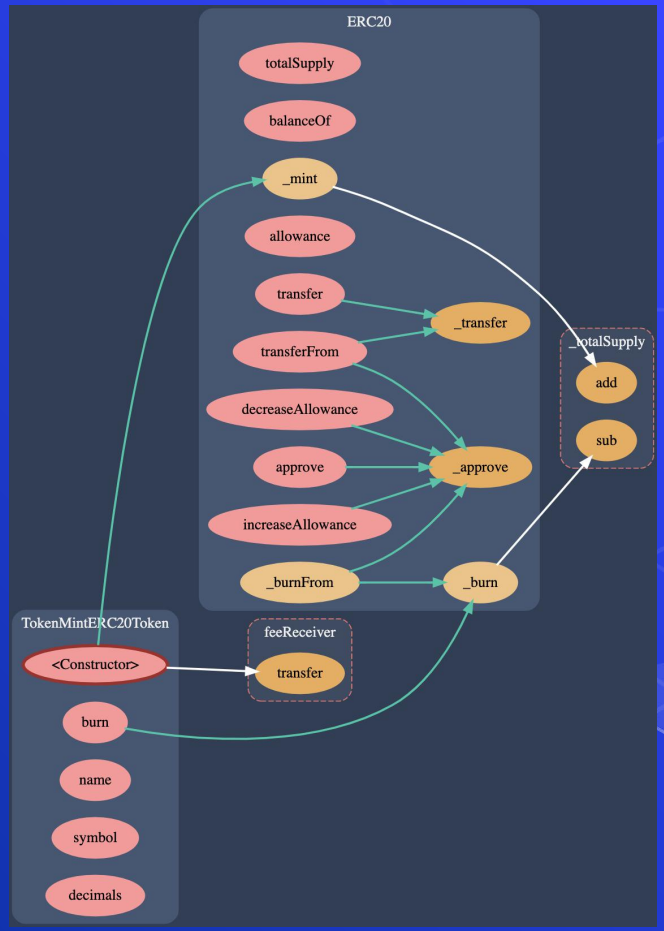
Fully Sanity Checks

	Read	Write	AI Scanned	Human Reviewed	Result	Suggested	Resolved
constructor		Yes	Completed	Completed	Low Risk	Missing-Zero-Address-Validation	
name()	Yes		Completed	Completed	No Risk		
symbol()	Yes		Completed	Completed	No Risk		
balanceOf()	Yes		Completed	Completed	No Risk		
decimals()	Yes		Completed	Completed	No Risk		
totalSupply()	Yes		Completed	Completed	No Risk		
allowance()	Yes		Completed	Completed	No Risk		
approve()		Yes	Completed	Completed	No Risk		
burn()		Yes	Completed	Completed	No Risk		
decreaseAllowance()		Yes	Completed	Completed	✓ Low/No Risk		
increaseAllowance()		Yes	Completed	Completed	✓ Low/No Risk		
transfer()		Yes	Completed	Completed	✓ Low/No Risk		
transferFrom()		Yes	Completed	Completed	✓ Low/No Risk		

Source Code Analysis



We've found 2 contracts, 1 interface and 1 library in SHIBA INU project source code and their logic and inheritance correlations as shown in the left side. TokenMintERC20Token, ERC20, IERC20 and SafeMath respectively.



ERC20 Contract

- totalSupply()
- balanceOf()
- allowance()

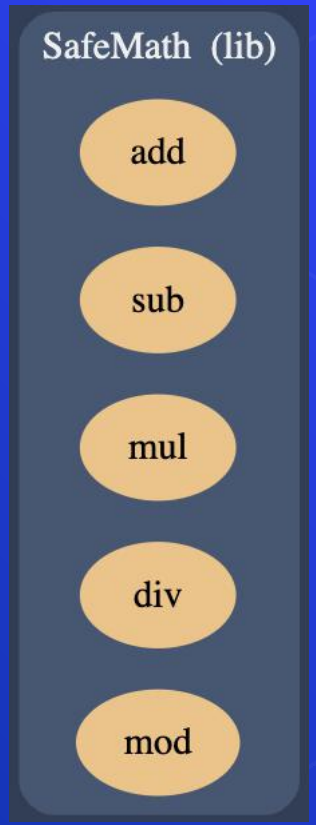
Read functions are running as expected while analyzing at the time of this writing.

- transfer()
- transferFrom()
- decreaseAllowance()
- approve()
- increaseAllowance()

Write functions are in no risk at the time of this writing

TokenMintERC20Token Contract

- constructor(): **missing zero address validation, the parameters in constructor method are in local variables shadowing.**
- burn()
- name()
- symbol()
- decimals()



SafeMath Library

- add()
- sub()

The operation of add and sub work as expected.

- mul()
- div()
- mod()

For the unused operations of mul, div, mod, should be considered to remove

Contract Ownership

Contract Ownership Has Not Been Renounced at the Time of Audit.

The contract ownership is not currently renounced.

We just placed the contract of the owner address below for you to look up:

0xB8f226dDb7bC672E27dffB67e4adAbFa8c0dFA08

Some feasible suggestions that would also mitigate the potential risk at a different level for priviledged ownership.

- Time-lock with reasonable latency, e.g., 48 hours for awareness on priviledged operations
- Assignment of priviledged roles to multi-signature wallets to prevent a single point of failure, for example, due to the private key compromised

Liquidity Ownership

No Lock/Unlock Liquidity Logic for Owner Has Been Found.

This page will contain links to locked liquidity for the project if we are able to locate that information.

Locked liquidity information was neither found on the project's website nor inside the contracts.

Mint Function

The Contract Cannot Mint New $SHIB Tokens.

We do understand that Mint functions are crucial to the functionality of the project, it's core related to its investors.

But a mint function was not found in the contract code.

Burn Function

The Contract Has a Burn Function.

The Burn function works well as expected according to the roadmap.

A burn function was found in the contract code.

```
/**
 * @dev Burns a specific amount of tokens.
 * @param value The amount of lowest token units to be burned.
 */
ftrace | funcSig
function burn(uint256 value) public {
    _burn(msg.sender, value);
}
```

```
/**
 * @dev Destroys `amount` tokens from `account`, reducing the
 * total supply.
 *
 * Emits a `Transfer` event with `to` set to the zero address.
 *
 * Requirements
 *
 * - `account` cannot be the zero address.
 * - `account` must have at least `amount` tokens.
 */
ftrace | funcSig
function _burn(address account, uint256 value) internal {
    require(account != address(0), "ERC20: burn from the zero address");

    _totalSupply = _totalSupply.sub(value);
    _balances[account] = _balances[account].sub(value);
    emit Transfer(account, address(0), value);
}
```

Present Mode

The left image is an actual snapshot of the current live website.

The website was registered on Jun-21-2021.

Team Location

Shiba Inu Official Website: https://shibatoken.com

General Web Security

DOMAIN

A valid domain hosted by Cloudflare.

Registered on 21-Jun-2021

shibatoken.com

Social Media Accounts

A bundle of social media accounts was found.

Twitter: https://twitter.com/shibtoken
Telegram: https://t.me/Shibalnu_Dogecoinkiller

A legal SSL certificate was found.
Issued at 21-Jun-2021

Signature Algorithm is

ECDSA-With-SHA256

SSL CERTIFICATE

No malware found.
No injected spam found.
No internal server errors.

Domain is marked clean by Google and McAfee.

SPAM/MALWARE

Disclaimer

The opinions expressed in this document are for general informational purposes only and are not intended to provide specific advice or recommendations for any individual or on any specific investment. It is only intended to provide education and public knowledge regarding to this projects. This audit is only applied to the type of auditing specified in this report and the scope of given in the results. Other unknown security vulnerabilities are beyond responsibility. MoonAudit only issues this report based on the attacks or vulnerabilities that already existed or occurred before the issuance of this report. For the emergence of new attacks or vulnerabilities that exist or occur in the future, MoonAudit lacks the capability to judge its possible impact on the security status of smart contracts, thus taking no responsibility for them. The smart contract analysis and other contents of this report are based solely on the documents and materials that the contract provider has provided to MoonAudit or was publicly available before the issuance of this report (issuance of report recorded via block number on cover page), if the documents and materials provided by the contract provider are missing, tampered, deleted, concealed or reflected in a situation that is inconsistent with the actual situation, or if the documents and materials provided are changed after the issuance of this report, MoonAudit assumes no responsibility for the resulting loss or adverse effects. Due to the technical limitations of any organization, this report conducted by MoonAudit still has the possibility that the entire risk cannot be completely detected. MoonAudit disclaims any liability for the resulting losses.

MoonAudit provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Even projects with a low risk score have been known to pull liquidity, sell all team tokens, or exit scam. Please exercise caution when dealing with any cryptocurrency related platforms. The final interpretation of this statement belongs to MoonAudit.

MoonAudit highly advises against using cryptocurrencies as speculative investments and they should be used solely for the utility they aim to provide.

About

MoonAudit has founded in 2021 by a squad of elite geeks on blockchain research and we analyze the loopholes in most smart contracts in ethereum-based chains. We offer the best-in-class report for your smart contracts auditing. Customer trusts smart contract, the more trust security assessment report.

Thank You

MOONAUDIT ORG. HAS BEEN COMPLETED FOR SHIBAINU($SHIB) AT BLOCK NUMBER: 10569013

THIS AUDIT IS ONLY VALID IF VIEWED ON HTTPS://MOONAUDIT.ORG

https://MoonAudit.org

https://t.me/MoonAudit