# RugFreeCoins Audit

# White Shiba Token

# Smart Contract Security Audit

# July 12, 2021

# Contents

# Audit details

**Audited project**

White Shiba Token

**Contract Address**

0xa409f482227cb5cbd98eb3c1baf2f94dbf10d3a2

**Client contact**

White Shiba Team

**Blockchain**

Ethereum Smart Chain

**Project website**

https://whiteshiba.io/

# 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 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 Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins 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 Rugfreecoins 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, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, 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

Rugfreecoins was commissioned by White Shiba to perform an audit of the smart contract.

**https://etherscan.io/address/0xa409f482227cb5cbd98eb3c1baf2f94dbf10d3a2**

The focus of this audit is to verify that the smart contract is secure, resilient and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, long term sustainability and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

# About the project

WSHIBA is a decentralized, community-owned ERC-20 token. It launched May 15th, 2021 and was soon soft rugged by the original dev. 58% of the LP was burned, and the ownership was renounced. However, instead of euthanizing this project, the community stepped up to take over the project.

The project is more community-oriented, where the community itself makes decisions together adding utility to the token and the ecosystem.

## Tokenomics

- 2% of trade goes to holders pockets.

## Roadmap

### PHASE 1: LAUNCH

✔ Website Launch
✔ Contract Deployed
✔ 50% Supply Burned
✔ Ownership Renounced
✔ 1,000 Holders
✔ 1,000 Telegram Members
✔ Community Marketing Fund

### PHASE 2: GROWTH

✔ CoinGecko Listing
✔ CoinMarketCap Listing
✔ WSHIBA staking
✔ Marketing Campaign
✔ Website Reconstructed

### PHASE 3: EXPANSION

✔ CEX Listing
✔ Massive Marketing Campaign
✔ Charity giveaway
✔ Partnership with another project that has the same values as us

### PHASE 4: UTILITY

✔ 2 more CEX Listing
✔ Marketing campaign in order to increase holders,
TG members and Twitter followers
✔ NFT Campaign

# Target market and the concept

## Target market

- Anyone who's ready to actively take part with the token and ecosystem development process.
- Anyone who's interested in Crypto space with long term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.

## Core concept

Still, the project is in the seeding stage, and decisions are yet to be made for the future of the project. Currently, White Shiba is a project that enables anyone to make trades and use it as currency pair for any financial purpose.

## Community-driven

The project was fully taken over by the community, and they are collectively making collaborative decisions. Everyone in the community has a voice over the decisions they make, which has great diversity and that enables them to make optimal decisions for the project's future.

# Potential to grow with score points

| | | |
|---|---|---|
| 1. | Project efficiency | 6/10 |
| 2. | Project uniqueness | 6/10 |
| 3 | Information quality | 7/10 |
| 4 | Service quality | 710 |
| 5 | System quality | 7/10 |
| 6 | Impact on the community | 8/10 |
| 7 | Impact on the business | 6/10 |
| 8 | Preparing for the future | 5/10 |
| Total Points | | **6.5/10** |

# Contract details

## Token contract details for 12ᵗʰ July 2021

| | |
|---|---|
| **Contract name** | White Shiba |
| **Contract address** | 0xa409f482227cb5cbd98eb3c1baf2f94dbf10d3a2 |
| **Token supply** | 100,000,000,000,000,000 |
| **Token ticker** | WSHIBA |
| **Decimals** | 9 |
| **Token holders** | 793 |
| **Transaction count** | 3,483 |
| **Top 100% holders dominance** | 93.82% |
| **Contract deployer address** | 0xb27e0081e7bc1467e75578d1f86943ebbf70f843 |
| **Contract's current owner address** | 0x0000000000000000000000000000000000000000 |

# Top token holders

## Top 10 Token Holders – 12ᵗʰ July 2021

♀ The top 10 holders collectively own 83.08% (83,077,794,624,729,200.00 Tokens) of White Shiba    |    ♀ Token Total Supply: 100,000,000,000,000,000.00 Token    |    Total Token Holders: 791

### White Shiba Top 10 Token Holders
Source: Etherscan.io

OTHER ACCOUNTS

0x011ea68c15f4a8316da45c1e7844311cdd0ba149
0xa7442537e5237d4ef6fa5b48bc3981528d2840dd
0xd8c0b95d8d349828809e4a64aa67b7ea2f7407a9
0x0caa48ac80e474d357927ff8676b2a7d01aae708
0x7dbc86c24cd3c73f4bba04a697644d040e21719d
0x632929883dba963d693ecebccab6b3cac0bec088
0x3f52d0f3d251b3a3c0edddc18510634f21c4ebb2
0x461019883ffa618a3111186adfcb09c4bfd29be5
0x85788388a42c0f16533c0b84d2bcb2f4662c6a0b (Uniswap V2: WSHIBA 2)

0x0000000000000000000000000000000000000dead (0x0000...dEaD)

(A total of 83,077,794,624,729,200.00 tokens held by the top 10 accounts from the total supply of 100,000,000,000,000,000.00 token)

| Rank | Address | Quantity (Token) | Percentage |
| --- | --- | --- | --- |
| 1 | 0x0000...dEaD | 59,758,551,307,847,100.494969818 | 59.7586% |
| 2 | 📄 Uniswap V2: WSHIBA 2 | 8,496,495,421,226,830.383337084 | 8.4965% |
| 3 | 0x461019883ffa618a3111186adfcb09c4bfd29be5 | 3,383,553,613,361,150.221561736 | 3.3836% |
| 4 | 0x3f52d0f3d251b3a3c0edddc18510634f21c4ebb2 | 3,131,302,091,490,220.744509712 | 3.1313% |
| 5 | 0x632929883dba963d693ecebccab6b3cac0bec088 | 2,329,586,227,038,270.46439808 | 2.3296% |
| 6 | 0x7dbc86c24cd3c73f4bba04a697644d040e21719d | 2,272,481,817,377,660.561066844 | 2.2725% |
| 7 | 0x0caa48ac80e474d357927ff8676b2a7d01aae708 | 1,039,581,928,325,550.346482304 | 1.0396% |
| 8 | 0xd8c0b95d8d349828809e4a64aa67b7ea2f7407a9 | 990,079,880,906,555.555165312 | 0.9901% |
| 9 | 0xa7442537e5237d4ef6fa5b48bc3981528d2840dd | 882,397,908,677,429.104674638 | 0.8824% |
| 10 | 0x011ea68c15f4a8316da45c1e7844311cdd0ba149 | 793,764,428,478,343.983971191 | 0.7938% |

# Token distribution

**Top 100 Token Holders**
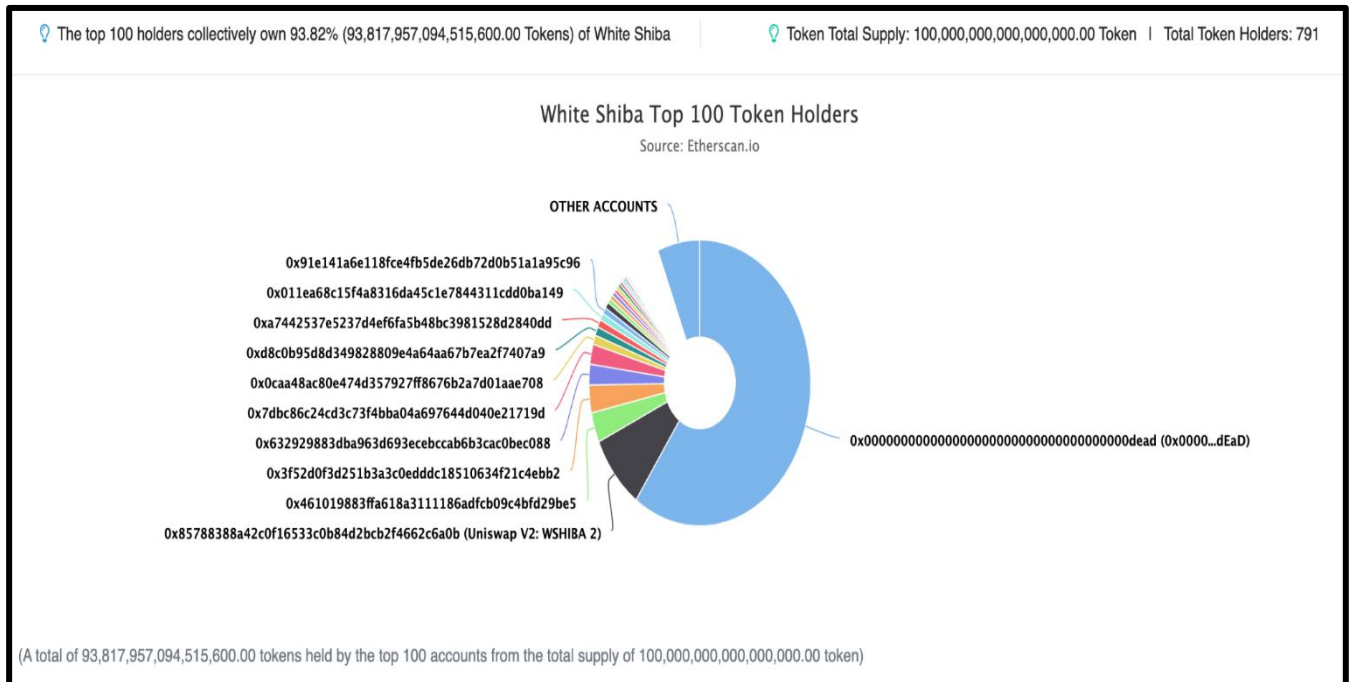


# Contract interaction details
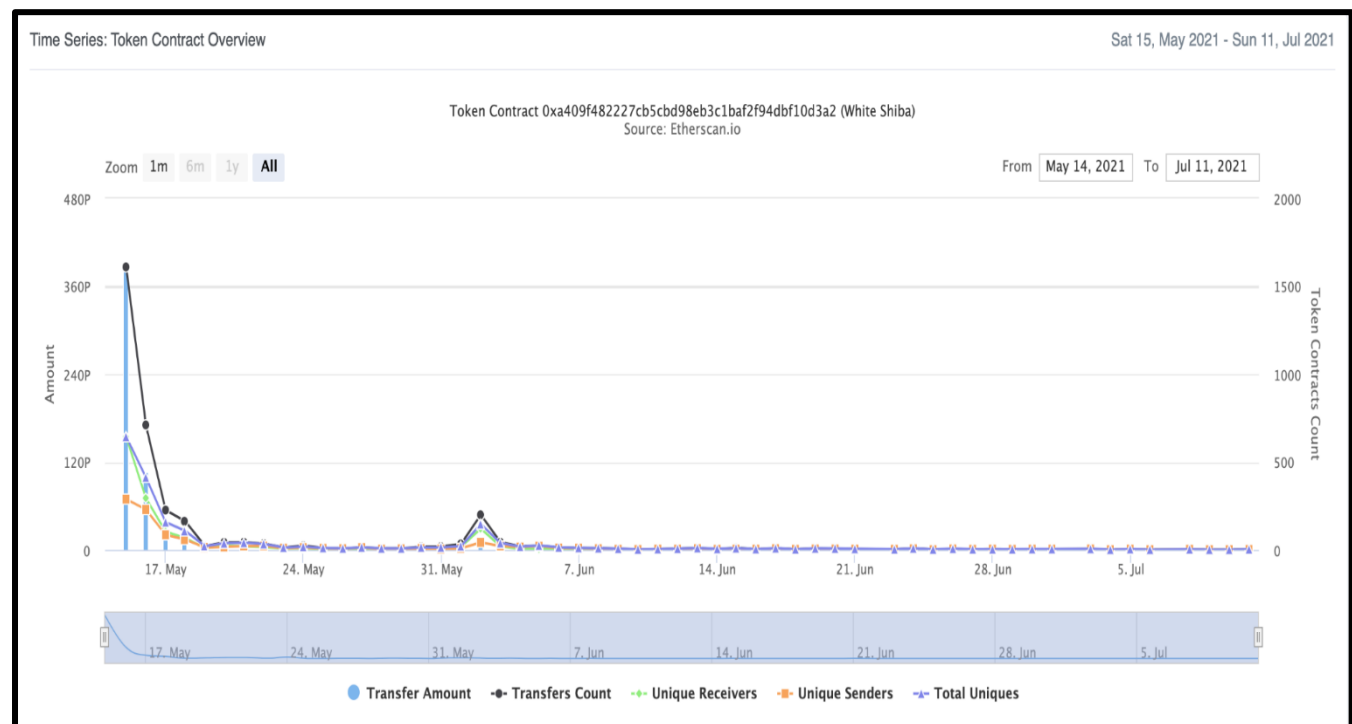
# Contract code function details

| No | Category | Item | Result |
|---|---|---|---|
| 1 | Coding conventions | BRC20 Token standards | pass |
| | | compile errors | pass |
| | | Compiler version security | pass |
| | | visibility specifiers | pass |
| | | Gas consumption | low issues |
| | | SafeMath features | pass |
| | | Fallback usage | pass |
| | | tx.origin usage | pass |
| | | deprecated items | pass |
| | | Redundant code | pass |
| | | Overriding variables | pass |
| 2 | Function call audit | Authorization of function call | pass |
| | | Low level function (call/delegate call) security | pass |
| | | Returned value security | pass |
| | | Selfdestruct function security | pass |
| 3 | Business security | Access control of owners | pass |
| | | Business logics | pass |
| | | Business implementations | pass |
| 4 | Integer overflow/underflow | | pass |
| 5 | Reentrancy | | pass |
| 6 | Exceptional reachable state | | pass |
| 7 | Transaction ordering dependence | | pass |
| 8 | Block properties dependence | | pass |
| 9 | Pseudo random number generator (PRNG) | | pass |
| 10 | DoS (Denial of Service) | | pass |
| 11 | Token vesting implementation | | pass |
| 12 | Fake deposit | | pass |
| 13 | Event security | | pass |

# Contract description table

Below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions and implementations with its visibility and mutability.

| Contract | Type | Bases | | |
|----------|------|-------|---|---|
| L | Function Name | Visibility | Mutability | Modifiers |
| | | | | |
| **Context** | **Implementation** | | | |
| L | _msgSender | Internal 🔒 | | |
| L | _msgData | Internal 🔒 | | |
| | | | | |
| **IERC20** | **Interface** | | | |
| L | totalSupply | External ❗ | | NO❗ |
| L | balanceOf | External ❗ | | NO❗ |
| L | transfer | External ❗ | 🛑 | NO❗ |
| L | allowance | External ❗ | | NO❗ |
| L | approve | External ❗ | 🛑 | NO❗ |
| L | transferFrom | External ❗ | 🛑 | NO❗ |
| | | | | |
| **SafeMath** | **Library** | | | |
| L | add | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | sub | Internal 🔒 | | |
| L | mul | Internal 🔒 | | |
| L | div | Internal 🔒 | | |
| L | div | Internal 🔒 | | |
| L | mod | Internal 🔒 | | |

| | | | | |
|---|---|---|---|---|
| L | mod | Internal 🔒 | | |
| | | | | |
| **Address** | **Library** | | | |
| L | isContract | Internal 🔒 | | |
| L | sendValue | Internal 🔒 | 🛑 | |
| L | functionCall | Internal 🔒 | 🛑 | |
| L | functionCall | Internal 🔒 | 🛑 | |
| L | functionCallWithValue | Internal 🔒 | 🛑 | |
| L | functionCallWithValue | Internal 🔒 | 🛑 | |
| L | _functionCallWithValue | Private 🔐 | 🛑 | |
| | | | | |
| **Ownable** | **Implementation** | **Context** | | |
| L | | Internal 🔒 | 🛑 | |
| L | owner | Public ❗ | | NO❗ |
| L | renounceOwnership | Public ❗ | 🛑 | onlyOwner |
| L | transferOwnership | Public ❗ | 🛑 | onlyOwner |
| | | | | |
| **WSHIBA** | **Implementation** | **Context, IERC20, Ownable** | | |
| L | | Public ❗ | 🛑 | NO❗ |
| L | name | Public ❗ | | NO❗ |
| L | symbol | Public ❗ | | NO❗ |
| L | decimals | Public ❗ | | NO❗ |
| L | totalSupply | Public ❗ | | NO❗ |
| L | balanceOf | Public ❗ | | NO❗ |
| L | transfer | Public ❗ | 🛑 | NO❗ |
| L | allowance | Public ❗ | | NO❗ |

| | | | | |
|---|---|---|---|---|
| └ | approve | Public ❗ | 🛑 | NO❗ |
| └ | transferFrom | Public ❗ | 🛑 | NO❗ |
| └ | increaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | decreaseAllowance | Public ❗ | 🛑 | NO❗ |
| └ | isExcluded | Public ❗ | | NO❗ |
| └ | totalFees | Public ❗ | | NO❗ |
| └ | setMaxTxPercent | External ❗ | 🛑 | onlyOwner |
| └ | rescueFromContract | External ❗ | 🛑 | onlyOwner |
| └ | reflect | Public ❗ | 🛑 | NO❗ |
| └ | reflectionFromToken | Public ❗ | | NO❗ |
| └ | tokenFromReflection | Public ❗ | | NO❗ |
| └ | excludeAccount | External ❗ | 🛑 | onlyOwner |
| └ | includeAccount | External ❗ | 🛑 | onlyOwner |
| └ | _approve | Private 🔒 | 🛑 | |
| └ | _transfer | Private 🔒 | 🛑 | |
| └ | _transferStandard | Private 🔒 | 🛑 | |
| └ | _transferToExcluded | Private 🔒 | 🛑 | |
| └ | _transferFromExcluded | Private 🔒 | 🛑 | |
| └ | _transferBothExcluded | Private 🔒 | 🛑 | |
| └ | _reflectFee | Private 🔒 | 🛑 | |
| └ | _getValues | Private 🔒 | | |
| └ | _getTValues | Private 🔒 | | |
| └ | _getRValues | Private 🔒 | | |
| └ | _getRate | Private 🔒 | | |
| └ | _getCurrentSupply | Private 🔒 | | |

| Symbol | Meaning |
|--------|---------|
| 🛑 | **Function can modify state** |
| 💵 | **Function is payable** |

# Inheritance Hierarchy
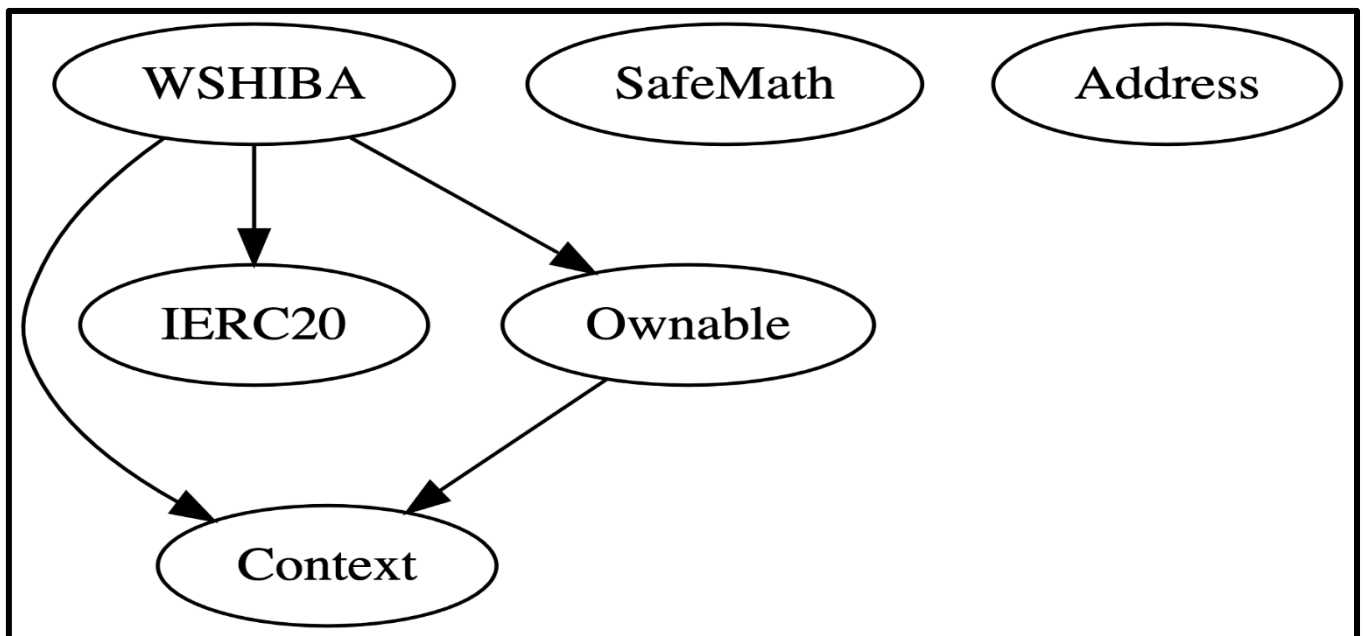
# Security issue checking status

❖ **High severity issues**
No high severity issues found.

❖ **Medium severity issues**
No medium severity issues found.

❖ **Low severity issues**

1. **Out of gas**

➢ The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long-excluded addresses list.

```
ftrace | funcSig
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

**Recommendation**
Check that the excluded array length is not too big.

# Owner privileges

Ownership has been renounced and the owner doesn't have any privileges and has no authority to make any changes now.

**Ownership privileges owner had**

❖ Owner can transfer the ownership.

```
ftrace | funcSig
function transferOwnership(address newOwner↑) public virtual onlyOwner {
    require(
        newOwner↑ != address(0),
        "Ownable: new owner is the zero address"
    );
    emit OwnershipTransferred(_owner, newOwner↑);
    _owner = newOwner↑;
}
```

❖ Owner can renounce the ownership.

```
ftrace | funcSig
function renounceOwnership() public virtual onlyOwner {
    emit OwnershipTransferred(_owner, address(0));
    _owner = address(0);
}
```

❖ Owner can transfer full contract balance to his account.

```
ftrace | funcSig
function rescueFromContract() external onlyOwner {
    address payable _owner = _msgSender();
    _owner.transfer(address(this).balance);
}
```

❖ Owner can change maximum transaction amount.

```
ftrace | funcSig
function setMaxTxPercent(uint256 maxTxPercent↑) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent↑).div(10**2);
}
```

# Audit conclusion

While conducting the audit of the White Shiba smart contract, it was observed that there is nothing alarming with the code and the contract only contains low severity issues.

Liquidity locking details can be found through the below link.

**https://etherscan.io/tx/0x48c098be4cd28aee456d775dd041dc986af8b2fe7f55d565ccd919 a7fff41414**