RugFreeCoins Audit

Santa Token
Smart Contract Security Audit

September 13 2022

Contents

Audit details

Audited project
Santa Token

Contract Address
0xfDdEA7d2764BE1a23f24971eba7602d8182620D4

Client contact
Santa Team

Blockchain
Binance smart chain

Project website
https://santaclub.xyz/

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.

Overview

✅ No mint function found; the owner cannot mint tokens after initial deployment.

✅ There’s no max tx limits and max wallet limits in the contract.

✅ The owner can’t pause trading.

✅ The owner can't change fees.

✅ Owner can't blacklist wallets.

✅ The owner can’t claim the contract’s balance of its own token.

Background

Rugfreecoins was commissioned by the Santa Team to perform an audit of the smart contract.

https://bscscan.com/address/0xfDdEA7d2764BE1a23f24971eba7602d8182620D4

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, and long-term sustainability, and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

.

Tokenomics

5% when buying & selling

- 1% of trade goes to the marketing wallet in BUSD.
- 3% of trade goes to the distribution of rewards among investors in BUSD.
- 0.5% of trade goes to the development wallet in BUSD.
- 0.5% of trade goes to the Donation wallet in BUSD.

Target market and the concept

Target market

- Anyone who’s interested in the 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.
- Anyone who’s ready to staking and receive rewards.
- Anyone who’s interested in taking part in the future plans of the Santa token
- Anyone who’s interested in trading NFTs and take part with the Santa NFT ecosystem.
- Anyone who’s interested in making financial transactions with any other party using Santa Token as the currency.

Potential to grow with score points

1.	Project efficiency	8/10
2.	Project uniqueness	8/10
3	Information quality	9/10
4	Service quality	8/10
5	System quality	9/10
6	Impact on the community	8/10
7	Impact on the business	9/10
8	Preparing for the future	9/10
9	Smart contract security	10/10
10	Smart contract functionality assessment	10/10
Total Points		**9/10**

Contract details

Token contract details for 13th of September 2022

Contract name	Santa
Contract address	0xfDdEA7d2764BE1a23f24971eba7602d8182620D4
Token supply	100,000,000,000
Token ticker	SANTA
Decimals	18
Token holders	1
Transaction count	1
Development wallet	0x36be502349b8a965fbc6f242ea3704d85a96cfa9
Donation wallet	0xb62d70dbcd64df72cf60e425c85b98c3a06b0df6
Marketing & DAO wallet	0x8588baaa8c32d53567b824ad81c9b44e1f86a167
Dividend tracker	0xcd67792e6283bdb4b048aa431b79825863ab6d52
Contract deployer address	0x900a644fcc3C631f066B75FEc850537268dffE6c
Contract’s current owner address	0x900a644fcc3c631f066b75fec850537268dffe6c

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	pass
		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
		Self-destruct function security	pass
3	Business security	Access control of owners	
		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

The 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 their visibility and mutability.

Contract	**Type**	**Bases**		
L	Function Name	Visibility	Mutability	Modifiers
Santa	**Implementation**	**IERC20, Ownable**		
L		Public ❗	🛑	NO❗
L		External ❗	💵	NO❗
L	totalSupply	External ❗		NO❗
L	name	Public ❗		NO❗
L	symbol	Public ❗		NO❗
L	decimals	Public ❗		NO❗
L	balanceOf	Public ❗		NO❗
L	getHolderDetails	Public ❗		NO❗
L	getLastProcessedIndex	Public ❗		NO❗
L	getNumberOfTokenHolders	Public ❗		NO❗
L	totalDistributedRewards	Public ❗		NO❗
L	allowance	External ❗		NO❗
L	approve	Public ❗	🛑	NO❗
L	_approve	Internal 🔒	🛑	

L	approveMax	External ❗	🛑	NO❗
L	transfer	External ❗	🛑	NO❗
L	transferFrom	External ❗	🛑	NO❗
L	_transferFrom	Internal 🔒	🛑	
L	takeFee	Internal 🔒	🛑	
L	_basicTransfer	Internal 🔒	🛑	
L	shouldTakeFee	Internal 🔒		
L	setEnableAntiBot	External ❗	🛑	onlyOwner
L	shouldDoContractSwap	Internal 🔒		
L	enableTrading	Public ❗	🛑	onlyOwner
L	___claimRewards	Public ❗	🛑	NO❗
L	claimProcess	Public ❗	🛑	NO❗
L	isRewardExcluded	Public ❗		NO❗
L	isFeeExcluded	Public ❗		NO❗
L	doContractSwap	Internal 🔒	🛑	swapping
L	swapTokensForBUSD	Private 🔐	🛑	
L	setIsDividendExempt	External ❗	🛑	onlyOwner
L	setIsFeeExempt	External ❗	🛑	onlyOwner
L	addAuthorizedWallet	External ❗	🛑	onlyOwner
L	setDoContractSwap	External ❗	🛑	onlyOwner
L	setDistributionCriteria	External ❗	🛑	onlyOwner

L	setDistributorSettings	External ❗	🛑	onlyOwner
Ownable	**Implementation**	**Context**		
L		Public ❗	🛑	NO❗
L	owner	Public ❗		NO❗
L	_checkOwner	Internal 🔒		
L	renounceOwnership	Public ❗	🛑	onlyOwner
L	transferOwnership	Public ❗	🛑	onlyOwner
L	_transferOwnership	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❗
IUniswapV2 Router02	**Interface**	**IUniswapV2 Router01**		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO❗

└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗		NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
IUniswapV2 Factory	**Interface**			
└	feeTo	External ❗		NO❗
└	feeToSetter	External ❗		NO❗
└	getPair	External ❗		NO❗
└	allPairs	External ❗		NO❗
└	allPairsLength	External ❗		NO❗
└	createPair	External ❗	🛑	NO❗
└	setFeeTo	External ❗	🛑	NO❗
└	setFeeToSetter	External ❗	🛑	NO❗
IDividend Distributor	**Interface**			
└	setDistributionCriteria	External ❗	🛑	NO❗
└	setShare	External ❗	🛑	NO❗
└	deposit	External ❗	🛑	NO❗
└	process	External ❗	🛑	NO❗
Dividend Distributor	**Implementation**	**IDividend Distributor**		

L		Public ❗	🛑	NO❗
L		External ❗	💵	NO❗
L	setDistributionCriteria	External ❗	🛑	onlyToken
L	setShare	External ❗	🛑	onlyToken
L	deposit	External ❗	🛑	onlyToken
L	process	External ❗	🛑	onlyToken
L	shouldDistribute	Internal 🔒		
L	distributeDividend	Internal 🔒	🛑	
L	claimDividend	External ❗	🛑	NO❗
L	getUnpaidEarnings	Public ❗		NO❗
L	getHolderDetails	Public ❗		NO❗
L	getCumulativeDividends	Internal 🔒		
L	getLastProcessedIndex	External ❗		NO❗
L	getNumberOfTokenHolders	External ❗		NO❗
L	getShareHoldersList	External ❗		NO❗
L	totalDistributedRewards	External ❗		NO❗
L	addShareholder	Internal 🔒	🛑	
L	removeShareholder	Internal 🔒	🛑	
IPinkAntiBot	**Interface**			
L	setTokenOwner	External ❗	🛑	NO❗

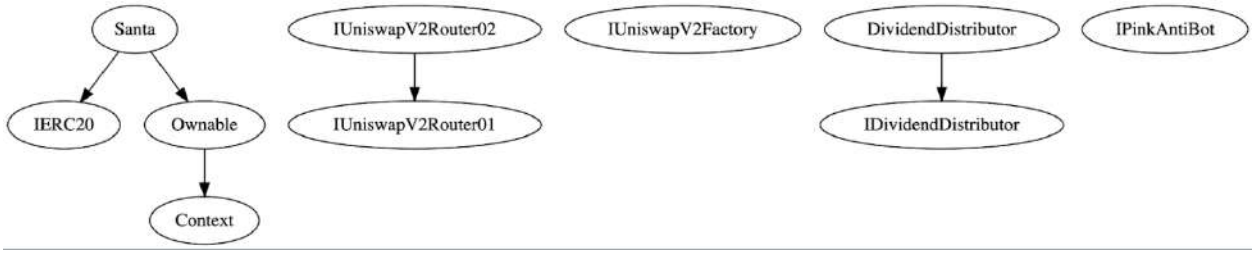
L	onPreTransferCheck	External ❗	🛑	NO❗
Context	**Implementation**			
L	_msgSender	Internal 🔒		
L	_msgData	Internal 🔒		
IUniswapV2 Router01	**Interface**			
L	factory	External ❗		NO❗
L	WETH	External ❗		NO❗
L	addLiquidity	External ❗	🛑	NO❗
L	addLiquidityETH	External ❗	💵	NO❗
L	removeLiquidity	External ❗	🛑	NO❗
L	removeLiquidityETH	External ❗	🛑	NO❗
L	removeLiquidityWithPermit	External ❗	🛑	NO❗
L	removeLiquidityETHWithPermit	External ❗	🛑	NO❗
L	swapExactTokensForTokens	External ❗	🛑	NO❗
L	swapTokensForExactTokens	External ❗	🛑	NO❗
L	swapExactETHForTokens	External ❗	💵	NO❗
L	swapTokensForExactETH	External ❗	🛑	NO❗
L	swapExactTokensForETH	External ❗	🛑	NO❗
L	swapETHForExactTokens	External ❗	💵	NO❗

L	quote	External ❗		NO❗
L	getAmountOut	External ❗		NO❗
L	getAmountIn	External ❗		NO❗
L	getAmountsOut	External ❗		NO❗
L	getAmountsIn	External ❗		NO❗

Legend

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**
  No low severity issues found

- **Centralization Risk**
  No Centralization Risk found

Owner privileges

- Owner can include/exclude wallets from dividends

```
ftrace | funcSig
function setIsDividendExempt(address holder↑, bool exempt↑)
    external
    onlyOwner
{
    require(
        holder↑ != address(this) && holder↑ != pair,
        "can not add pair and token address as share holder"
    );
    isDividendExempt[holder↑] = exempt↑;
    if (exempt↑) {
        dividendTracker.setShare(holder↑, 0);
    } else {
        dividendTracker.setShare(holder↑, _balances[holder↑]);
    }

    emit SetIsDividendExempt(holder↑, exempt↑);
}
```

- Owner can include/exclude wallets from fees

```
ftrace | funcSig
function setIsFeeExempt(address holder↑, bool exempt↑) external onlyOwner {
    isFeeExempt[holder↑] = exempt↑;

    emit SetIsFeeExempt(holder↑, exempt↑);
}
```

❖ Owner can enable/disable swapping

```
ftrace | funcSig
function setDoContractSwap(bool _enabled⬆) external onlyOwner {
    contractSwapEnabled = _enabled⬆;
    lastContractSwapTime = block.timestamp;

    emit SetDoContractSwap(_enabled⬆);
}
```

Audit conclusion

RugFreeCoins team has performed in-depth testings, line-by-line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASS**

Number of risk issues: **0**

Solidity code functional issue level: **PASS**

Number of owner privileges: **3**

Centralization risk correlated to the active owner: **LOW**

Smart contract active ownership: **YES**