

TechRate
August, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Techrate_audits



Techrate



Techrate1

Audit Details



Audited project

FlokiGrow



Deployer address

0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2



Client contacts:

FlokiGrow team



Blockchain

Binance Smart Chain



Project website:

Not provided

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

TechRate was commissioned by FlokiGrow to perform an audit of smart contracts:

<https://bscscan.com/address/0xc6082790554478ff3bcd264adc1cfaea6de7e64c#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand 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.

Contracts Details

Token contract details for 13.08.2022

Contract name FlokiGrow

Contract address 0xc6082790554478fF3bcD264AdC1CfAEA6dE7E64C

Total supply 1,000,000,000,000,000

Token ticker FlokiGrow

Decimals 9

Token holders 2,880

Transactions count 26,506

Top 100 holders dominance 93.52%

Cooldown time 10

Donation wallet 0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2

Marketing wallet 0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2

Uniswap V2 pair 0x8ea7b592ef5d55b410e2aadc55e2383e194d5aca

Contract deployer address 0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2

Owner address 0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2

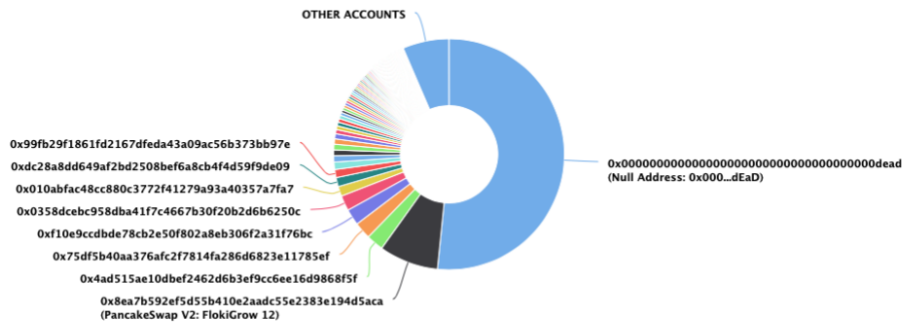
FlokiGrow Token Distribution

The top 100 holders collectively own 93.52% (935,172,779,751,334.00 Tokens) of FlokiGrow

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 2,880

FlokiGrow Top 100 Token Holders

Source: BscScan.com



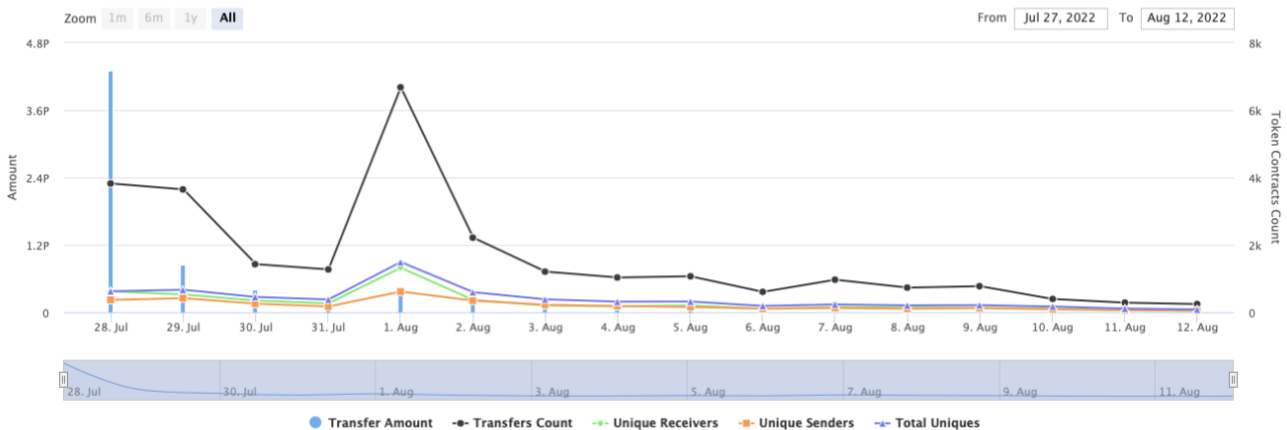
(A total of 935,172,779,751,334.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)

FlokiGrow Contract Interaction Details

Time Series: Token Contract Overview

Thu 28, Jul 2022 - Fri 12, Aug 2022

Token Contract 0xc6082790554478ff3bcd264adc1cfaea6de7e64c (FlokiGrow)
Source: BscScan.com



FlokiGrow Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	516,166,400,598,875.604323209	51.6166%
2	PancakeSwap V2: FlokiGrow 12	83,010,230,818,520.529419458	8.3010%
3	0x4ad515ae10dbef2462d6b3ef9cc6ee16d9868f5f	24,153,080,431,373.948246072	2.4153%
4	0x75df5b40aa376afc2f7814fa286d6823e11785ef	23,826,730,392,786.5619709	2.3827%
5	0xf10e9ccdbde78cb2e50f802a8eb306f2a31f76bc	22,712,253,901,580.421398663	2.2712%
6	0x0358dcebc958dba41f7c4667b30f20b2d6b6250c	21,308,116,551,144.901312298	2.1308%
7	0xd10abfac48cc880c3772f41279a93a40357a7fa7	13,748,848,229,524.667127204	1.3749%
8	0xdc28a8dd649af2bd2508bef6a8cb4f4d59f9de09	12,715,997,393,733.236081109	1.2716%
9	0x99fb29f1861fd2167dfeda43a09ac56b373bb97e	11,196,898,737,800.963266149	1.1197%
10	0x0d6c4a9f5e2f4d4c313dfbeb8da749412b551e	10,463,820,961,144.673294089	1.0464%

FlokiGrow LP Token Holders

Rank	Address	Quantity	Percentage
1	0xae7e6cabad8d80f0b4e1c4dde2a5db7201ef1252	3,402.311806086484450997	96.8521%
2	0x8b8244603387e106d6fcc5b75d6ac1a9d4e77cd2	110.467019684735216752	3.1446%
3	0x0ed943ce24baebf257488771759f9bf482c39706	0.114516232177463814	0.0033%
4	Null Address: 0x000...000	0.0000000000000001	0.0000%

Contract functions details

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ Context

- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Prv] _setOwner #

+ [Int] IFactory

- [Ext] createPair #

+ [Int] IRouter

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidityETH (\$)
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Lib] Address

- [Int] sendValue #

+ FlokiGrow (Context, IERC20, Ownable)

- [Pub] <Constructor> #
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] approve #

- modifiers: antiBot
- [Pub] transferFrom #
 - modifiers: antiBot
- [Pub] increaseAllowance #
 - modifiers: antiBot
- [Pub] decreaseAllowance #
 - modifiers: antiBot
- [Pub] transfer #
 - modifiers: antiBot
- [Pub] isExcludedFromReward
- [Pub] reflectionFromToken
- [Ext] setTradingStatus #
 - modifiers: onlyOwner
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
 - modifiers: onlyOwner
- [Ext] includeInReward #
 - modifiers: onlyOwner
- [Pub] excludeFromFee #
 - modifiers: onlyOwner
- [Pub] includeInFee #
 - modifiers: onlyOwner
- [Pub] isExcludedFromFee
- [Pub] setTaxes #
 - modifiers: onlyOwner
- [Pub] setSellTaxes #
 - modifiers: onlyOwner
- [Prv] _reflectRfi #
- [Prv] _takeLiquidity #
- [Prv] _takeMarketing #
- [Prv] _takeDonation #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues1
- [Prv] _getRValues2
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _tokenTransfer #
- [Prv] swapAndLiquify #
 - modifiers: lockTheSwap
- [Prv] addLiquidity #
- [Prv] swapTokensForBNB #
- [Ext] airdropTokens #

- modifiers: onlyOwner
- [Ext] bulkExcludeFee #
 - modifiers: onlyOwner
- [Ext] updateMarketingWallet #
 - modifiers: onlyOwner
- [Ext] updateDonationWallet #
 - modifiers: onlyOwner
- [Ext] updateCooldown #
 - modifiers: onlyOwner
- [Ext] updateSwapTokensAtAmount #
 - modifiers: onlyOwner
- [Ext] updateSwapEnabled #
 - modifiers: onlyOwner
- [Ext] updateIsBlacklisted #
 - modifiers: onlyOwner
- [Ext] bulkIsBlacklisted #
 - modifiers: onlyOwner
- [Ext] updateAllowedTransfer #
 - modifiers: onlyOwner
- [Ext] updateMaxTxLimit #
 - modifiers: onlyOwner
- [Ext] updateMaxWalletlimit #
 - modifiers: onlyOwner
- [Ext] updateRouterAndPair #
 - modifiers: onlyOwner
- [Ext] rescueBNB #
 - modifiers: onlyOwner
- [Pub] rescueAnyBEP20Tokens #
 - modifiers: onlyOwner
- [Ext] <Fallback> (\$)

(\$) = payable function

= non-constant function

Issues Checking Status

Issue description	Checking status
1. Compiler errors.	Passed
2. Race conditions and Reentrancy. Cross-function race conditions.	Passed
3. Possible delays in data delivery.	Passed
4. Oracle calls.	Passed
5. Front running.	Passed
6. Timestamp dependence.	Passed
7. Integer Overflow and Underflow.	Passed
8. DoS with Revert.	Passed
9. DoS with block gas limit.	Low issues
10. Methods execution permissions.	Passed
11. Economy model of the contract.	Passed
12. The impact of the exchange rate on the logic.	Passed
13. Private user data leaks.	Passed
14. Malicious Event log.	Passed
15. Scoping and Declarations.	Passed
16. Uninitialized storage pointers.	Passed
17. Arithmetic accuracy.	Passed
18. Design Logic.	Passed
19. Cross-function race conditions.	Passed
20. Safe Open Zeppelin contracts implementation and usage.	Passed
21. Fallback function security.	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.
- 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.

Recommendation:

Check that the excluded array length is not too big.

Issue:

- The function `bulkExcludeFee()` uses the loop to add excluded addresses from the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.
- The function `bulksBlacklisted()` uses the loop to add blacklisted addresses from the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long addresses list.

Recommendation:























Check that the array length is not too big.

Owner privileges (In the period when the owner is not renounced)



- Owner can change trading and swapping status.
- Owner can exclude from the fee.
- Owner can change taxes.
- Owner can airdrop tokens.
- Owner can change fee receivers.
- Owner can change cooldown settings.
- Owner can change swapTokensAtAmount.
- Owner can blacklist addresses.
- Owner can include addresses in transfer allowance array.
- Owner can change the maximum buy/sell and wallet amounts.
- Owner can withdraw ERC20 tokens and BNBs.
- Owner can change router address.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
FlokiGrow	Implementation	Context, IERC20, Ownable		
L	approve	Public !		antiBot
L	transferFrom	Public !		antiBot
L	transfer	Public !		antiBot
L	setTradingStatus	External !		onlyOwner
L	excludeFromReward	Public !		onlyOwner
L	includeInReward	External !		onlyOwner
L	excludeFromFee	Public !		onlyOwner
L	includeInFee	Public !		onlyOwner
L	setTaxes	Public !		onlyOwner
L	setSellTaxes	Public !		onlyOwner
L	airdropTokens	External !		onlyOwner
L	updateMarketingWallet	External !		onlyOwner
L	updateDonationWallet	External !		onlyOwner
L	updateCooldown	External !		onlyOwner
L	updateSwapTokensAtAmount	External !		onlyOwner
L	updateSwapEnabled	External !		onlyOwner
L	updateIsBlacklisted	External !		onlyOwner
L	updateAllowedTransfer	External !		onlyOwner
L	updateMaxTxLimit	External !		onlyOwner
L	updateMaxWalletlimit	External !		onlyOwner
L	updateRouterAndPair	External !		onlyOwner
L	rescueBNB	External !		onlyOwner
L	rescueAnyBEP20Tokens	Public !		onlyOwner

Legend

Symbol	Meaning
	Function can modify state
	Function is payable

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are NOT provided by the team.

TechRate 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.