



KISHIELD

Security Audit

SIFUINU Token

March 28, 2022





Table of Contents

1 Audit Summary

2 Project Overview

2.1 Token Summary

2.2 Main Contract Assessed

3 Smart Contract Vulnerability Checks

4 Contract Ownership

4.1 Privileged Functions

5 Important Notes To The Users

6 Findings Summary

6.1 Classification of Issues

6.1 Findings Table

01 Repetitive Code

02 Unused Code

03 Public function that could be declared external

04 Variables could be declared as constant

05 Incorrect Error

7 Statistics

7.1 Liquidity

7.2 Token Holders

7.3 Liquidity Holders

8 Liquidity Ownership

9 Disclaimer



Audit Summary

This report has been prepared for SIFUINU Token on the Binance Chain network. KISHIELD provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user's funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Project Overview

Token Summary

Parameter	Result
Address	0x16DAE78F8b13fc7f86Dfd8711E768E37D10A674F
Name	SIFUINU
Token Tracker	SIFUINU (SIFU)
Decimals	18
Supply	2,500,000,000
Platform	Binance Chain
compiler	v0.8.12+commit.f00d7308
Optimization	Yes with 200 runs
LicenseType	Unlicense
Language	Solidity
Codebase	https://bscscan.com/ address/0x16DAE78F8b13fc7f86Dfd8711E768E37D10A674F
Url	https://sifuinu.io/

Main Contract Assessed

Name	Contract	Live
SIFUINU.sol	0x16DAE78F8b13fc7f86Dfd8711E768E37D10A674F	Yes

Smart Contract Vulnerability Checks

Vulnerability	Automatic Scan	Manual Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	✓ Low / No Risk
Code With No Effects	Complete	Complete	✓ Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	✓ Low / No Risk
Hash Collisions With Multiple Variable Length Arguments	Complete	Complete	✓ Low / No Risk
Unexpected Ether balance	Complete	Complete	✓ Low / No Risk
Presence of unused variables	Complete	Complete	✓ Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	✓ Low / No Risk
Typographical Error	Complete	Complete	✓ Low / No Risk
DoS With Block Gas Limit	Complete	Complete	✓ Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	✓ Low / No Risk
Insufficient Gas Griefing	Complete	Complete	✓ Low / No Risk
Incorrect Inheritance Order	Complete	Complete	✓ Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	✓ Low / No Risk
Requirement Violation	Complete	Complete	✓ Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	✓ Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	✓ Low / No Risk

Vulnerability	Automatic Scan	Manual Scan	Result
Authorization through tx.origin	Complete	Complete	✓ Low / No Risk
Delegatecall to Untrusted Callee	Complete	Complete	✓ Low / No Risk
Use of Deprecated Solidity Functions	Complete	Complete	✓ Low / No Risk
Assert Violation	Complete	Complete	✓ Low / No Risk
Reentrancy	Complete	Complete	✓ Low / No Risk
Unprotected SELFDESTRUCT Instruction	Complete	Complete	✓ Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	✓ Low / No Risk
Unchecked Call Return Value	Complete	Complete	✓ Low / No Risk
Outdated Compiler Version	Complete	Complete	✓ Low / No Risk
Integer Overflow and Underflow	Complete	Complete	✓ Low / No Risk
Function Default Visibility	Complete	Complete	✓ Low / No Risk

Contract Ownership

The contract ownership of SIFUINU is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x7675e0650cc93F92b2Fd84Ec18cCa713eb237AE2 which can be viewed from: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions chart below, if the owner wallet is compromised this privileges could be exploited.

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

Important Notes To The Users:

- The owner cannot mint tokens after initial deployment.
- The transfer function is implemented correctly.
- The owner can stop Trading.
- The owner can change the max tx amount.
- The owner can blacklist addresses.
- The owner can add/remove addresses from the rewards and fees.
- The owner can change the liquidity, dev, marketing, and charity fees amount.
- The owner can transfer, approve and withdraw tokens to the contract.
- The team has locked 89.8% of LP tokens in PinkSale.
- Once the owner renounce ownership of the contract, no changes can be made to the tx fees, and max tx amount and no one could stop trading.
- No high-risk Exploits/Vulnerabilities Were Found in token Source Code.

Audit Passed



Findings Summary

Classification of Issues

All Issues Found are Informational

Severity	Description
● High	Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency
● Medium	Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.
● Low	Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.
● Info	Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

Findings

Severity	Found
● High	0
● Medium	0
● Low	0
● Info	5
Total	5

Findings

Repetitive Code

ID	Severity	Contract	Function
01	● Informational	SIFUINU	function sendToken, releaseToken

Description

Gas Optimization. Both functions implement the exact same logic

Recommendation

Create a single function with the functionality and use it as needed.

Unused Code

ID	Severity	Contract	Function
02	● Informational	SIFUINU	function swapETHForTokens(uint256 amount)

Description

Private Function is not called by the contract.

Recommendation

We advise deleting this function or setting the view state to external.

Public function that could be declared external

ID	Severity	Contract	Function
03	Informational	SIFUINU	Functions totalFees(), enable_blacklist(), manage_blacklist(), isExcludedFromReward()

Description

Gas Optimization. Public function that could be declared external

Recommendation

Public functions that are never called by the contract should be declared external to save gas.

Variables could be declared as constant

ID	Severity	Contract	Function
04	Informational	SIFUINU	variables name, symbol, decimals


Description

Gas Optimization. Variables that are never changed could be declared as constant.

Recommendation

We recommend declaring those variables as constant.

Incorrect Error

ID	Severity	Contract	Function
05	 Informational	SIFUINU	function multiTransferFixed(address[] calldata addresses, uint256 tokens)

Description

Error name does not match the require code, GAS Error: max airdrop limit is 500 addresses but the code allows addresses.length to be 800

Recommendation

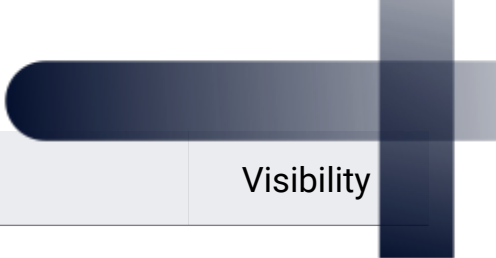
We advice updating the error to showcase the correct max value

Privileged Functions (onlyOwner)

Function Name	Parameters	Visibility
renounceOwnership	none	public
transferOwnership	address newOwner	public
lock	uint256 time	public
openTrade	none	external
stopTrade	none	external
includeToWhiteList	calldata _users	external
enable_blacklist	bool _status	public
manage_blacklist	calldata addresses, bool status	public
setEnableAntiBot	bool _enable	external
excludeFromReward	address account	public
includeInReward	address account	external
_transfer	none	private
swapAndLiquify	none	public
excludeFromFee	address account	public
includeInFee	address account	public
setAllFeePercent	uint256 taxFee, uint256 liquidityFee, uint256 devFee, uint256 marketingFee, uint256 charityFee	external

Function Name	Parameters	Visibility
setSaleFeePercent	uint256 taxFee, uint256 liquidityFee, uint256 devFee, uint256 marketingFee, uint256 charityFee	external
setSaleLiquidityFeePercent	uint256 liquidityFee	external
setMaxTxAmount	uint256 maxTxAmount	external
setNumTokensSellToAddToLiquidity	uint256 _minimumTokensBeforeSwap	external
setMarketingWalletAddress	address _marketingWallet	external
setCharityWalletAddress	address _charityWallet	external
setDevWalletAddress	address _devWallet	external
setpinkAntiBotAddress	address _AntiBotAddress	external
setSwapAndLiquifyEnabled	bool _enabled	public
sendSameValue	address _tokenAddress, calldata _to, uint256 _value	external
sendSameValueContract	address _tokenAddress, calldata _to, uint256 _value	external
sendDifferentValue	address _tokenAddress, calldata _to, calldata _value	external
ApproveERC20Token1	address _tokenAddress, uint256 _value	external
recoverETHfromContract	none	external
multiTransfer	calldata addresses, calldata tokens	external
multiTransferFixed	calldata addresses, uint256 tokens	external





Function Name	Parameters	Visibility
recoverTokenFromContract	none	public
manualBurn	uint256 burnAmount	public
ethSendSameValue	calldata _to, uint256 _value	external
ethSendDifferentValue	calldata _to, calldata _value	external

Statistics

Liquidity Info

Parameter	Result
Pair Address	0x9B640639f0F8E05D0384b98996Fa3d617F193fc0
SIFU Reserves	308814886.23 SIFU
BNB Reserves	114.23 BNB
Liquidity Value	\$49,849.972 USD

Token (SIFU) Holders Info

Parameter	Result
SIFU Percentage Burnt	0.00%
SIFU Amount Burnt	0 SIFU
Top 10 Percentage Own	59.94%
Top 10 Amount Owned	1,498,389,830.412 SIFU
Top 10 Aprox Value	\$241,875.293 USD

LP (SIFU/BNB) Holders Info

Parameter	Result
SIFU/BNB % Burnt	0.00%
SIFU/BNB Amount Burnt	0 SIFU
Top 10 Percentage Owned	100.00%
Top 10 Amount Owned	186,517.935 SIFU
Locked Tokens Percentage	89.86%
Locked Tokens Amount	167,596.603 SIFU

* All the data displayed above was taken on-chain at block 16457400

* The tokens on industry-standard burn wallets are not included on the top 10 wallets calculations

Liquidity Ownership

The token does not have liquidity at the moment of the audit, block 16457400

KISHIELD



Disclaimer

KISHIELD has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocacy for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and KISHIELD is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will KISHIELD or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by KISHIELD is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.