



**SAFU AUDIT**  
SMART CONTRACT AUDITING

## GIVERFI SMART CONTRACT AUDIT



March 23, 2022

# INTRODUCTION

---

<b>Client</b>	GiverFi (Giverfi)
<b>Language</b>	Solidity
<b>Contract Address</b>	0xe9b11B398A39d2A454F1bF52CAB5Eb47737208F
<b>Decimals</b>	5
<b>Supply</b>	431,000
<b>Platform</b>	Binance Smart Chain
<b>Compiler</b>	v0.7.4+commit.3f05b770
<b>Optimization</b>	Yes, with 200 runs
<b>Website</b>	<a href="https://giverfi.com/">https://giverfi.com/</a>
<b>Telegram</b>	<a href="https://t.me/GiverFi">https://t.me/GiverFi</a>
<b>Twitter</b>	<a href="https://twitter.com/GiverFi">https://twitter.com/GiverFi</a>

## Description

\$GiverFi model is an experimental approach to The Circular Economy concept, consisting of an Auto-staking feature enabled just by holding the token, plus a fixed APY that is sustainable over time and backed by a reserve of funds that ensures the perpetuity of the protocol.

# TABLE OF CONTENTS

## 01 INTRODUCTION

---

Introduction	02
Approach	04
Risk classification	05

## 02 ABSTRACT

---

Abstract	06
----------	----

## 03 VULNERABILITIES TEST

---

Vulnerabilities Test	07
----------------------	----

## 04 MANUAL ANALYSIS

---

Manual analysis	09
Contract Inspection	10
Inheritance Tree	14
Important Snippets	15
Good Practices	16

## 05 WEBSITE

---

Website Audit	17
---------------	----

## 06 CONCLUSIONS

---

Disclaimer	18
Audit Results	19
Score	20
Summary	21

# Approach

---



## Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

---



## Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

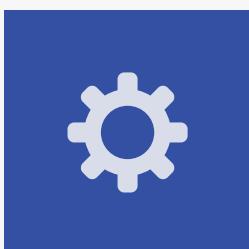
---



## Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
  - Back-doors
  - Vulnerability
  - Accuracy
  - Readability
- 



## Tools

- Remix IDE
- MythX, Mytrhl
- SWC Registry
- Open Zeppelin Code Analyzer
- Solidity Code Complier

# RISK CLASSIFICATION

---

## CRITICAL

---

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## MEDIUM

---

Issues on this level could potentially bring problems and should eventually be fixed.

## MINOR

---

Issues on this level are minor details and warning that can remain unfixed but would be better fixed at some point in the future

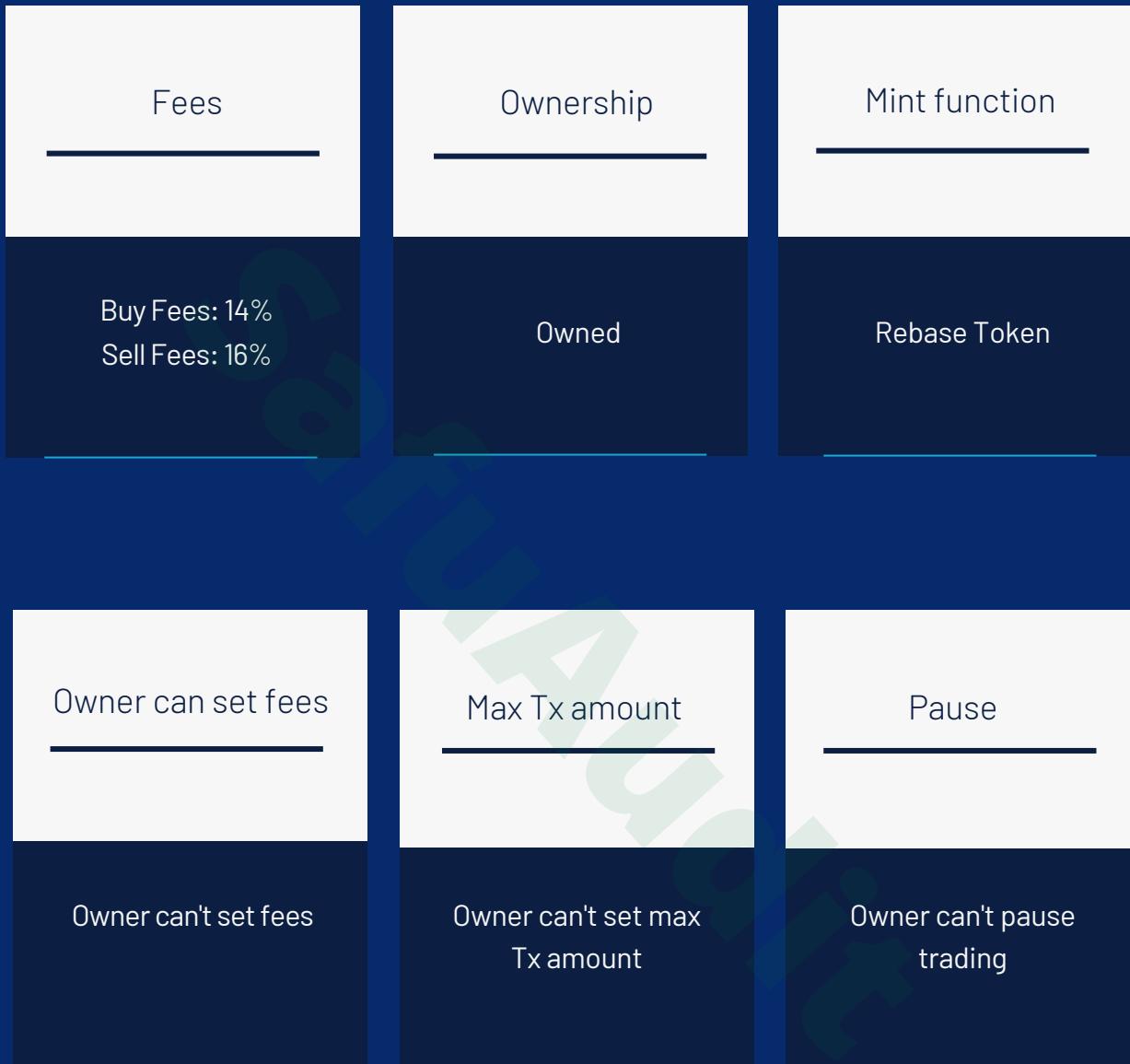
## INFORMATIONAL

---

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

# ABSTRACT

---



# Vulnerabilities Test

SWC ID	Description	
<b>SWC-100</b>	Function Default Visibility	<b>Passed</b>
<b>SWC-101</b>	Integer Overflow and Underflow	<b>Passed</b>
<b>SWC-102</b>	Outdated Compiler Version	<b>Passed</b>
<b>SWC-103</b>	FloatingPragma	<b>Minor</b>
<b>SWC-104</b>	Unchecked Call Return Value	<b>Passed</b>
<b>SWC-105</b>	Unprotected Ether Withdrawal	<b>Passed</b>
<b>SWC-106</b>	Unprotected SELF-DESTRUCT Instruction	<b>Passed</b>
<b>SWC-107</b>	Re-entrancy	<b>Passed</b>
<b>SWC-108</b>	State Variable Default Visibility	<b>Minor</b>
<b>SWC-109</b>	Uninitialized Storage Pointer	<b>Passed</b>
<b>SWC-110</b>	Assert Violation	<b>Passed</b>
<b>SWC-111</b>	Use of Deprecated Solidity Functions	<b>Passed</b>
<b>SWC-112</b>	Delegate Call to Untrusted Callee	<b>Passed</b>
<b>SWC-113</b>	DoS with Failed Call	<b>Passed</b>
<b>SWC-114</b>	Transaction Order Dependence	<b>Passed</b>
<b>SWC-115</b>	Authorization through tx.origin	<b>Passed</b>

<b>SWC-116</b>	Block values as a proxy for time	<b>Passed</b>
<b>SWC-117</b>	Signature Malleability	<b>Passed</b>
<b>SWC-118</b>	Incorrect Constructor Name	<b>Passed</b>
<b>SWC-119</b>	Shadowing State Variables	<b>Passed</b>
<b>SWC-120</b>	Weak Sources of Randomness from Chain Attributes	<b>Passed</b>
<b>SWC-121</b>	Missing Protection against Signature Replay Attacks	<b>Passed</b>
<b>SWC-122</b>	Lack of Proper Signature Verification	<b>Passed</b>
<b>SWC-123</b>	Requirement Violation	<b>Passed</b>
<b>SWC-124</b>	Write to Arbitrary Storage Location	<b>Passed</b>
<b>SWC-125</b>	Incorrect Inheritance Order	<b>Passed</b>
<b>SWC-126</b>	Insufficient Gas Griefing	<b>Passed</b>
<b>SWC-127</b>	Arbitrary Jump with Function Type Variable	<b>Passed</b>
<b>SWC-128</b>	DoS With Block Gas Limit	<b>Passed</b>
<b>SWC-129</b>	Typographical Error	<b>Passed</b>
<b>SWC-130</b>	Right-To-Left-Override control character (U+202E)	<b>Passed</b>
<b>SWC-131</b>	Presence of unused variables	<b>Passed</b>
<b>SWC-132</b>	Unexpected Ether balance	<b>Passed</b>
<b>SWC-133</b>	Hash Collisions With Multiple Variable Length Arguments	<b>Passed</b>
<b>SWC-134</b>	Message call with the hardcoded gas amount	<b>Passed</b>
<b>SWC-135</b>	Code With No Effects (Irrelevant/Dead Code)	<b>Passed</b>
<b>SWC-136</b>	Unencrypted Private Data On-Chain	<b>Passed</b>

# MANUAL ANALYSIS

The contract is verified to check if functions do and work as they should and malicious code is not inserted.

	Tested	Result
<b>Transfer</b>	Yes	<b>Passed</b>
<b>Total Supply</b>	Yes	<b>Passed</b>
<b>Buy Back</b>	Yes	<b>N/A</b>
<b>Burn</b>	Yes	<b>N/A</b>
<b>Mint</b>	Yes	<b>N/A</b>
<b>Rebase</b>	Yes	<b>Passed</b>
<b>Pause</b>	Yes	<b>N/A</b>
<b>Blacklist</b>	Yes	<b>Passed</b>
<b>Lock</b>	Yes	<b>N/A</b>
<b>Max Transaction</b>	Yes	<b>N/A</b>
<b>Transfer Ownership</b>	Yes	<b>Passed</b>
<b>Renounce Ownership</b>	Yes	<b>Passed</b>

MANUAL AUDIT

# CONTRACT INSPECTION



\*\*SafeMathInt\*\*	Library				
L	mul	Internal 🔒			
L	div	Internal 🔒			
L	sub	Internal 🔒			
L	add	Internal 🔒			
L	abs	Internal 🔒			
\*\*SafeMath\*\*	Library				
L	add	Internal 🔒			
L	sub	Internal 🔒			
L	sub	Internal 🔒			
L	mul	Internal 🔒			
L	div	Internal 🔒			
L	div	Internal 🔒			
L	mod	Internal 🔒			
\*\*IERC20\*\*	Interface				
L	totalSupply	External 🚫	NO 🚫		
L	balanceOf	External 🚫	NO 🚫		
L	allowance	External 🚫	NO 🚫		
L	transfer	External 🚫	🔴 NO 🚫		
L	approve	External 🚫	🔴 NO 🚫		
L	transferFrom	External 🚫	🔴 NO 🚫		
\*\*IPancakeSwapPair\*\*	Interface				
L	name	External 🚫	NO 🚫		
L	symbol	External 🚫	NO 🚫		
L	decimals	External 🚫	NO 🚫		
L	totalSupply	External 🚫	NO 🚫		
L	balanceOf	External 🚫	NO 🚫		
L	allowance	External 🚫	NO 🚫		
L	approve	External 🚫	🔴 NO 🚫		
L	transfer	External 🚫	🔴 NO 🚫		
L	transferFrom	External 🚫	🔴 NO 🚫		
L	DOMAIN\_SEPARATOR	External 🚫	NO 🚫		
L	PERMIT\_TYPEHASH	External 🚫	NO 🚫		

```
| L | nonces | External | | NO | |
| L | permit | External | |  | NO |  
| L | MINIMUM_LIQUIDITY | External | | NO |  
| L | factory | External | | NO |  
| L | token0 | External | | NO |  
| L | token1 | External | | NO |  
| L | getReserves | External | | NO |  
| L | price0CumulativeLast | External | | NO |  
| L | price1CumulativeLast | External | | NO |  
| L | kLast | External | | NO |  
| L | mint | External | |  | NO |  
| L | burn | External | |  | NO |  
| L | swap | External | |  | NO |  
| L | skim | External | |  | NO |  
| L | sync | External | |  | NO |  
| L | initialize | External | |  | NO |
```

|||||

```
| **IPancakeSwapRouter** | 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 |
```

L   removeLiquidityETHSupportingFeeOnTransferTokens   External !	●	NO!
L   removeLiquidityETHWithPermitSupportingFeeOnTransferTokens   External !	●	NO!
L   swapExactTokensForTokensSupportingFeeOnTransferTokens   External !	●	NO!
L   swapExactETHForTokensSupportingFeeOnTransferTokens   External !	●	NO!
L   swapExactTokensForETHSupportingFeeOnTransferTokens   External !	●	NO!
**IPancakeSwapFactory**   Interface		
L   feeTo   External !     NO!		
L   feeToSetter   External !     NO!		
L   getPair   External !     NO!		
L   allPairs   External !     NO!		
L   allPairsLength   External !     NO!		
L   createPair   External !   ●   NO!		
L   setFeeTo   External !   ●   NO!		
L   setFeeToSetter   External !   ●   NO!		
**Ownable**   Implementation		
L   <Constructor>   Public !   ●   NO!		
L   owner   Public !     NO!		
L   isOwner   Public !     NO!		
L   renounceOwnership   Public !   ●   onlyOwner		
L   transferOwnership   Public !   ●   onlyOwner		
L   _transferOwnership   Internal 🔒   ●		
**ERC20Detailed**   Implementation   IERC20		
L   <Constructor>   Public !   ●   NO!		
L   name   Public !     NO!		
L   symbol   Public !     NO!		
L   decimals   Public !     NO!		
**giverfi**   Implementation   ERC20Detailed, Ownable		
L   <Constructor>   Public !   ●   ERC20Detailed Ownable		
L   rebase   Internal 🔒   ●		
L   transfer   External !   ●   validRecipient		
L   transferFrom   External !   ●   validRecipient		
L   _basicTransfer   Internal 🔒   ●		
L   transferFrom   Internal 🔒   ●		

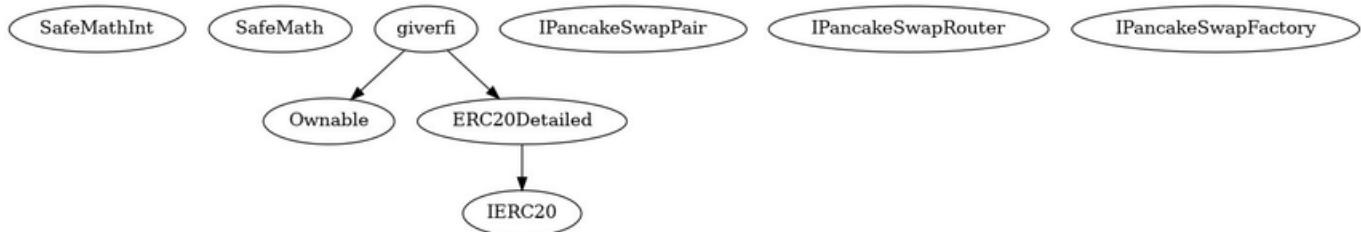
```

| L | takeFee | Internal 🔒 | ○ | || |
| L | addLiquidity | Internal 🔒 | ○ | swapping |
| L | swapBack | Internal 🔒 | ○ | swapping |
| L | withdrawAllTorevenue | External ! | ○ | swapping onlyOwner |
| L | shouldTakeFee | Internal 🔒 | || |
| L | shouldRebase | Internal 🔒 | || |
| L | shouldAddLiquidity | Internal 🔒 | || |
| L | shouldSwapBack | Internal 🔒 | || |
| L | setAutoRebase | External ! | ○ | onlyOwner |
| L | setAutoAddLiquidity | External ! | ○ | onlyOwner |
| L | allowance | External ! | | NO! | |
| L | decreaseAllowance | External ! | | ○ | NO! | |
| L | increaseAllowance | External ! | | ○ | NO! | |
| L | approve | External ! | | ○ | NO! | |
| L | checkFeeExempt | External ! | | NO! | |
| L | getCirculatingSupply | Public ! | | NO! | |
| L | isNotInSwap | External ! | | NO! | |
| L | manualSync | External ! | | ○ | NO! | |
| L | setFeeReceivers | External ! | | ○ | onlyOwner |
| L | getLiquidityBacking | Public ! | | NO! | |
| L | setWhitelist | External ! | | ○ | onlyOwner |
| L | setBotBlacklist | External ! | | ○ | onlyOwner |
| L | setPairAddress | Public ! | | ○ | onlyOwner |
| L | setLP | External ! | | ○ | onlyOwner |
| L | totalSupply | External ! | | NO! | |
| L | balanceOf | External ! | | NO! | |
| L | isContract | Internal 🔒 | || |
| L | <Receive Ether> | External ! | | 💸 | NO! | |

```

Symbol	Meaning
○	Function can modify state
💸	Function is payable
🔒	Private function
🔓	Internal function
NO!	Function has no modifier

# INHERITANCE TREE



Inheritance is a feature of the object-oriented programming language. It is a way of extending the functionality of a program, used to separate the code, reduces the dependency, and increases the re-usability of the existing code. Solidity supports inheritance between smart contracts, where multiple contracts can be inherited into a single contract.

# Important Snippets



## Auto rebase

```
function setAutoRebase(bool _flag) external onlyOwner {
    if (_flag) {
        _autoRebase = _flag;
        _lastRebasedTime = block.timestamp;
    } else {
        _autoRebase = _flag;
    }
}
```

## Blacklisted contracts are not permitted to transfer their tokens

```
function setBotBlacklist(address _botAddress, bool _flag) external onlyOwner {
    require(isContract(_botAddress), "only contract address, not allowed externally owned account");
    blacklist[_botAddress] = _flag;
}
```

## Transfer tokens left in contract to revenue address

```
function withdrawAllToTreasury() external swapping onlyOwner {

    uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);
    require( amountToSwap > 0, "There is no given token deposited in token contract");
    address[] memory path = new address[](2);
    path[0] = address(this);
    path[1] = router.WETH();
    router.swapExactTokensForETHSupportingFeeOnTransferTokens(
        amountToSwap,
        0,
        path,
        treasuryReceiver,
        block.timestamp
    );
}
```

# GOOD PRACTICES ✓

---

- The owner cannot stop or pause the smart contract
- The owner cannot set the fees
- The owner cannot set max Tx
- The smart contract utilizes "SafeMath" to prevent overflows

```
library SafeMath {
    function add(uint256 a, uint256 b) internal pure returns (uint256) {
        uint256 c = a + b;
        require(c >= a, "SafeMath: addition overflow");

        return c;
    }

    function sub(uint256 a, uint256 b) internal pure returns (uint256) {
        return sub(a, b, "SafeMath: subtraction overflow");
    }

    function sub(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        require(b <= a, errorMessage);
        uint256 c = a - b;

        return c;
    }

    function mul(uint256 a, uint256 b) internal pure returns (uint256) {
        if (a == 0) {
            return 0;
        }

        uint256 c = a * b;
        require(c / a == b, "SafeMath: multiplication overflow");

        return c;
    }

    function div(uint256 a, uint256 b) internal pure returns (uint256) {
        return div(a, b, "SafeMath: division by zero");
    }

    function div(
        uint256 a,
        uint256 b,
        string memory errorMessage
    ) internal pure returns (uint256) {
        require(b > 0, errorMessage);
        uint256 c = a / b;

        return c;
    }

    function mod(uint256 a, uint256 b) internal pure returns (uint256) {
        require(b != 0);
        return a % b;
    }
}
```

# WEBSITE



<b>Website</b>	<a href="https://giverfi.com/">https://giverfi.com/</a>
<b>Domain Registry</b>	<a href="https://domains.google.com">https://domains.google.com</a>
<b>Domain Expiry Date</b>	2023-03-20
<b>Response Code</b>	200
<b>SSL Checker and HTTPS Test</b>	Passed
<b>Deprecated HTML tags</b>	Passed
<b>Robots.txt</b>	Medium
<b>Sitemap Test</b>	Medium
<b>SEO Friendly URL</b>	Passed
<b>Responsive Test</b>	Passed
<b>JS Error Test</b>	Minor
<b>Console Errors Test</b>	Passed
<b>Site Loading Speed Test</b>	1.34 seconds - Passed
<b>HTTP2 Test</b>	Passed
<b>Safe Browsing Test</b>	Passed

# DISCLAIMER

---

SafuAudit.com is not a financial institution and the information provided on this website does not constitute investment advice, financial advice, trading advice or any other sort of advice. You should not treat any of the website's content as such. Investing in crypto assets carries a high level of risk and does not hold guarantees for not sustaining financial loss due to their volatility.

## Accuracy of Information

SafuAudit will strive to ensure accuracy of information listed on this website although it will not hold any responsibility for any missing or wrong information. SafuAudit provides all information as is. You understand that you are using any and all information available here at your own risk. Any use or reliance on our content and services is solely at your own risk and discretion.

The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project.

While we have used all the information available to us for this straightforward investigation, you should not rely on this report only – we recommend proceeding with several independent audits. Be aware that smart contracts deployed on a blockchain aren't secured enough against external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, SafuAudit does not guarantee the explicit security of the audited smart contract. 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.

# AUDIT RESULTS

---

## CRITICAL

---

No critical severity issues have been found.

## MEDIUM

---

No medium severity issues have been found.

## MINOR

---

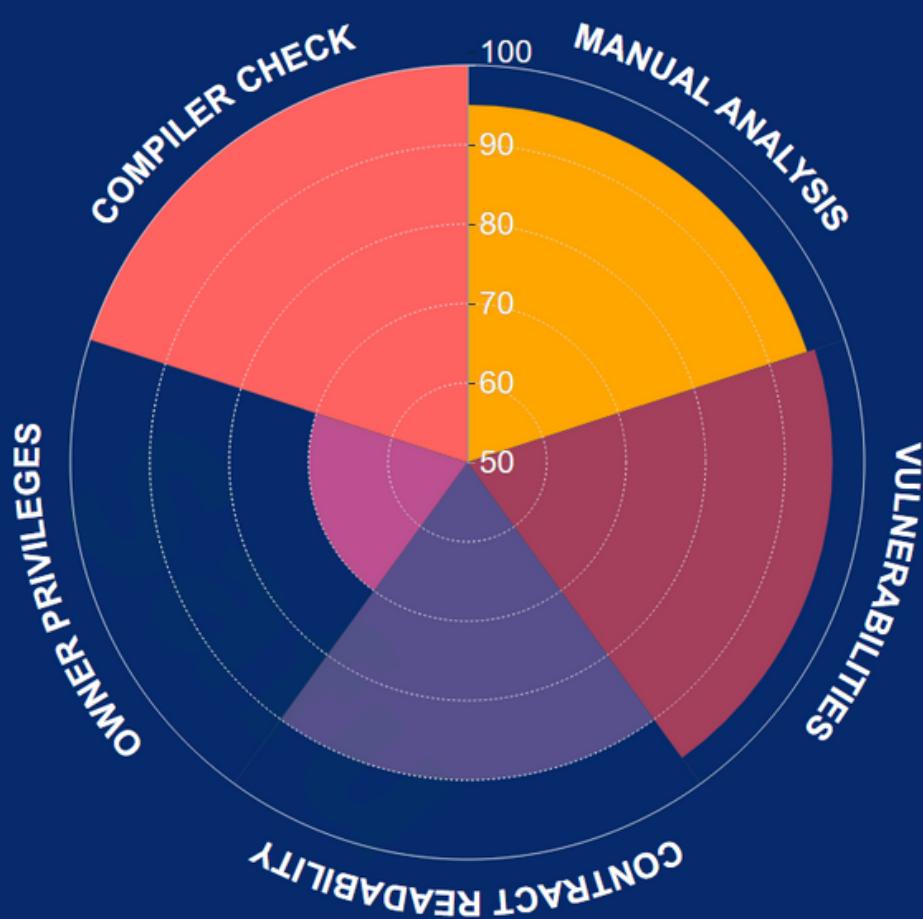
- A floating pragma is set. It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.
- State variable visibility is not set for: \_isFeeExempt, inSwap, DEAD, ZERO

## INFORMATIONAL

---

- The owner can toggle liquidity add and rebase functionality at any time.
- The owner can swap all \$Giverfi in the contract for BNB and withdraw it from the contract to the revenueReceiver address at any time.

# SCORE



Manual Analysis



Vulnerabilities



Contract Readability



Owner Privileges



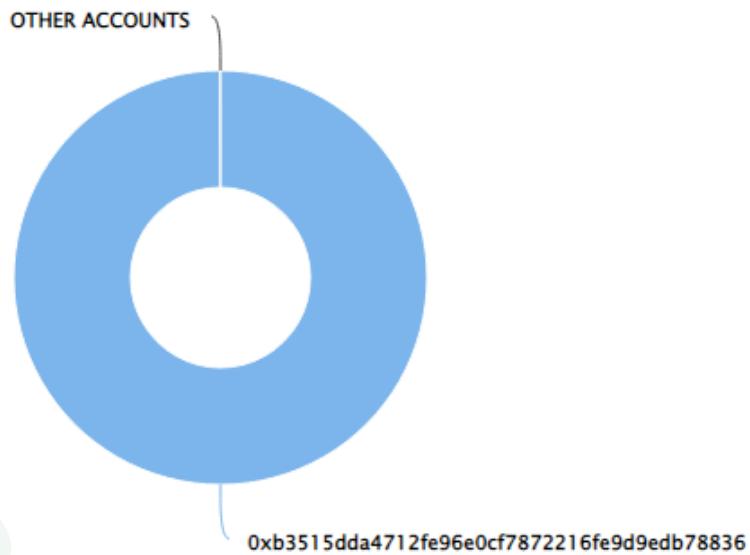
Compiler Check

**Final Score: 90.2**

# SUMMARY

---

## Top 10 holders



Rank	Address	Quantity (Token)	Percentage
1	0xb3515dda4712fe96e0cf7872216fe9d9edb78836	431,000	100.0000%

## Conclusion

Project GiverFi does not contain any severe issues or risk characteristics.

This is a rebase token: the owner can toggle liquidity adds and rebases from occurring at any time.

SafuAudit has tested the security based on manual and automated tests.

Please note that we don't offer any warranties for business model.



**SafuAudit.com**

