RugFreeCoins Audit

HODL Token
Smart Contract Security Audit

April 6th ,2023

Contents

Audit details

Audited project
HODL Token

Contract Address
0x0E9766dF73973abCfEDDE700497c57110ee5c301

Client contact
HODL Team

Blockchain
Binance smart chain

Project website
https://hodltoken.net/

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.

✅ The owner can’t set a max transaction limit to a very low value

✅ The owner can’t pause trading.

✅ The owner can’t set fees over 25%.

✅ The owner can't blacklist wallets.

✅ The owner can’t set a max wallet limit

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

Note: The token smart contract is implemented as a proxy contract, and as such, it is designed to be upgradeable. More information regarding this aspect can be found in the audit report, which accurately reflects the state of affairs at the time of the audit.

Background

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

https://bscscan.com/token/0x0E9766dF73973abCfEDDE700497c57110ee5c301

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 smart contract's security posture by remediating the identified issues.

.

Roadmap

Phase 01

CONTRACT INNOVATION

- UPGRADABLE CONTRACT
- GAS FEES OPTIMIZED

STAKING & FARMING

- INVEST HODL FUNDS

EXCHANGE LISTING

- CEX & DEX LISTINGS
- LISTINGS OPTIMIZATION

PARTNERSHIPS

- MOONSCAN
- STAYSAFU

PRODUCTS

- DASHBOARD
- MERCH STORE
- PHYSICAL COINS

NFTS

- HODL HANDS NFTS
- BUY NFTS ON CARD

GAMES

- HODL NINJA
- HODL CRUSH

BETTING

- HODL BET

LEGAL

- OFAC SANCTION BLOCKS

Phase 02

CONTRACT INNOVATION

- CONTRACT FUNCTIONS OPTIMIZED
- REWARD STACKING
- BURN LOTTERY

STAKING & FARMING

- HODL DEFI HUB

EXCHANGE LISTING

- TRADING TEAM
- ADVANCED MARKET-MAKING

PARTNERSHIPS

- COINVOTE
- MOBULA

PRODUCTS

- WEBSITE V2
- DEFI HUB

NFTS

- MIGRATED TO BSC
- NFT STAKING

GAMES

- HODL GRABBER
- MOONSHOT

BETTING

- BETTING PLATFORM INTEGRATION

LEGAL

- COMPANY REGISTRATION

Phase 03

CONTRACT INNOVATION

- MULTIPLE REWARD OPTIONS
- REINVESTMENT BONUS
- HODL VAULT

STAKING & FARMING

- STAKE TOKENS TO EARN NFTS

EXCHANGE LISTING

- TOP 10 CEX LISTING

PARTNERSHIPS

- CHAINLINK LABS
- LAKEVIEW META

PRODUCTS

- DASHBOARD V2
- FIAT ON AND OFF RAMPS
- HODL APP

NFTS

- NFTS GET BONUS $HODL

GAMES

- NEW GAME FEATURES
- SOLITAIRE

BETTING

- APP INTEGRATION

LEGAL

- AML ANALYTICS

Phase 04

CONTRACT INNOVATION

- REFER AND EARN
- CROSS-CHAIN

STAKING & FARMING

- INTEGRATE DEFI HUB

EXCHANGE LISTING

- TOP 5 CEX LISTING

PARTNERSHIPS

- FLOOZ
- GLOBAL PARTNERSHIPS

PRODUCTS

- MERCH STORE V2
- TEXAS HODL
- HODL PAY

NFTS

- POKER INTEGRATION
- HODL HANDS 2

GAMES

- COMPETITION BOT
- PLAY-TO-EARN GAMING
- STUDIO GAME

BETTING

- NEW BETTING GAMES

LEGAL

- LIVE AML CHECKS

Tokenomics

10% tax when buying & selling

- 5% of trade distributes among holders as rewards in BNB.
- 2% of trade distributes among holders as rewards in tokens.
- 1.5% of trade goes to the liquidity pool
- 1% of trade goes to the company wallet in tokens.
- 0.5% of trade goes to the lottery in tokens.

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 winning the lottery jackpot.
- Anyone who’s interested in taking part in the HODL ecosystem.
- Anyone who’s interested in taking part in the future plans of HODL Token.
- Anyone who’s interested in making financial transactions with any other party using HODL Token as the currency.

Potential to grow with score points

1.	Project efficiency	10/10
2.	Project uniqueness	9/10
3	Information quality	10/10
4	Service quality	10/10
5	System quality	10/10
6	Impact on the community	10/10
7	Impact on the business	10/10
8	Preparing for the future	10/10
9	Smart contract security	9/10
10	Smart contract functionality assessment	10/10
Total Points		**9.8/10**

Contract details

Token contract details for 6th of April 2023

Contract name	HODL
Contract address	0x0E9766dF73973abCfEDDE700497c57110ee5c301
Token supply	1,000,000,000,000,000
Token ticker	HODL
Decimals	9
Token holders	26,420
Transaction count	101,148
Contract deployer address	0x3ba9685E02247bF459ec777898CEF384C906A385
Contract's current owner address	0x3ba9685e02247bf459ec777898cef384c906a385
Proxy	0x0E9766dF73973abCfEDDE700497c57110ee5c301
Implementation	0x7b73700373AdF01e1865Cb8c392377C9Ef39D810
HODLX token	0xaebdbcc7d6821e3924ee5167b4138a43c19cf681
HODLX Router	0xd4dd4bf4abe7454a1c04199321aaefd85a7beae1
HODL Hands	0x7e82123bcb6465133d6e9e1ad94d0115de041b3d
HODL Master Chef	0x33e3406f2594ac4c2a8f3f573ca0adafb6c80fdb
Company wallet	0x894606f1eea0e37f5537a190da291b855fe685b1

Lottery wallet	0xaee863d491758e352349820e65edabc9df417f1e
Reinvest wallet	0xd217ca1d16b0bbbd30d438cf620f94e38a799b86
Staking wallet	0xcf99b7c6189caf2cbdcac07280e0490827418221
Trigger wallet	0x3ba9685e02247bf459ec777898cef384c906a385

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
		Selfdestruct 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
14	Centralisation		High

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
VRFCoordinator V2 Interface	**Interface**			
L	getRequestConfig	External !		NO !
L	requestRandomWords	External !	🛑	NO !
L	createSubscription	External !	🛑	NO !
L	getSubscription	External !		NO !
L	requestSubscriptionOwnerTransfer	External !	🛑	NO !
L	acceptSubscriptionOwnerTransfer	External !	🛑	NO !
L	addConsumer	External !	🛑	NO !
L	removeConsumer	External !	🛑	NO !
L	cancelSubscription	External !	🛑	NO !
L	pendingRequestExists	External !		NO !
VRFConsumerBaseV2	**Implementation**			
L		Public !	🛑	NO !

L	fulfillRandomWords	Internal 🔒	🛑	
L	rawFulfillRandomWords	External ❗	🛑	NO ❗
IBEP20	**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 ❗
IWBNB	**Interface**			
L	name	External ❗		NO ❗
L	symbol	External ❗		NO ❗
L	decimals	External ❗		NO ❗
L	balanceOf	External ❗		NO ❗
L	allowance	External ❗		NO ❗
L		External ❗	💵	NO ❗
L	deposit	External ❗	💵	NO ❗
L	withdraw	External ❗	🛑	NO ❗
L	totalSupply	External ❗		NO ❗
L	approve	External ❗	🛑	NO ❗

L	transfer	External !	🛑	NO !
L	transferFrom	External !	🛑	NO !
SafeMath	**Library**			
L	tryAdd	Internal 🔒		
L	trySub	Internal 🔒		
L	tryMul	Internal 🔒		
L	tryDiv	Internal 🔒		
L	tryMod	Internal 🔒		
L	add	Internal 🔒		
L	sub	Internal 🔒		
L	mul	Internal 🔒		
L	div	Internal 🔒		
L	mod	Internal 🔒		
L	sub	Internal 🔒		
L	div	Internal 🔒		
L	mod	Internal 🔒		
Context	**Implementation**			
L	_msgSender	Internal 🔒		
Initializable	**Implementation**			

L	isConstructor	Private 🔐		
Ownable	**Implementation**	**Context, Initializable**		
L		Public ❗	🛑	NO ❗
L	initOwner	Public ❗	🛑	initializer
L	owner	Public ❗		NO ❗
L	renounceOwnership	Public ❗	🛑	onlyOwner
L	transferOwnership	Public ❗	🛑	onlyOwner
Ipancake Factory	**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 ❗
IPancakePair	**Interface**			
L	name	External ❗		NO ❗
L	symbol	External ❗		NO ❗

└	decimals	External ❗		NO ❗
└	totalSupply	External ❗		NO ❗
└	balanceOf	External ❗		NO ❗
└	allowance	External ❗		NO ❗
└	approve	External ❗	🛑	NO ❗
└	transfer	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
└	DOMAIN_SEPARATOR	External ❗		NO ❗
└	PERMIT_TYPEHASH	External ❗		NO ❗
└	nonces	External ❗		NO ❗
└	permit	External ❗	🛑	NO ❗
└	MINIMUM_LIQUIDITY	External ❗		NO ❗
└	factory	External ❗		NO ❗
└	token0	External ❗		NO ❗
└	token1	External ❗		NO ❗
└	getReserves	External ❗		NO ❗
└	price0CumulativeLast	External ❗		NO ❗
└	price1CumulativeLast	External ❗		NO ❗
└	kLast	External ❗		NO ❗
└	mint	External ❗	🛑	NO ❗
└	burn	External ❗	🛑	NO ❗

└	swap	External ❗	🛑	NO ❗
└	skim	External ❗	🛑	NO ❗
└	sync	External ❗	🛑	NO ❗
└	initialize	External ❗	🛑	NO ❗
IPancake Router01	**Interface**			
└	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗
└	addLiquidity	External ❗	🛑	NO ❗
└	addLiquidityETH	External ❗	💵	NO ❗
└	removeLiquidity	External ❗	🛑	NO ❗
└	removeLiquidityETH	External ❗	🛑	NO ❗
└	removeLiquidityWithPermit	External ❗	🛑	NO ❗
└	removeLiquidityETHWithPermit	External ❗	🛑	NO ❗
└	swapExactTokensForTokens	External ❗	🛑	NO ❗
└	swapTokensForExactTokens	External ❗	🛑	NO ❗
└	swapExactETHForTokens	External ❗	💵	NO ❗
└	swapTokensForExactETH	External ❗	🛑	NO ❗
└	swapExactTokensForETH	External ❗	🛑	NO ❗
└	swapETHForExactTokens	External ❗	💵	NO ❗
└	getAmountOut	External ❗		NO ❗

L	getAmountIn	External !		NO !
L	getAmountsOut	External !		NO !
L	getAmountsIn	External !		NO !
IPancake Router02	**Interface**	**IPancake Router01**		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External !	🛑	NO !
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External !	🛑	NO !
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External !	🛑	NO !
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External !	💵	NO !
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External !	🛑	NO !
Utils	**Library**			
L	calculateBNBReward	Public !		NO !
L	calculateTopUpClaim	Public !		NO !
L	swapTokensForEth	Public !	🛑	NO !
L	swapETHForTokens	Public !	🛑	NO !
L	swapTokensForTokens	Public !	🛑	NO !
L	getAmountsout	Public !		NO !
L	addLiquidity	Public !	🛑	NO !
L	calcStacked	Public !		NO !
L	calcReward	Public !		NO !

L	_getValues	Public !		NO !
L	_getTValues	Private		
L	_getRValues	Private		
L	getBonus	Public !		NO !
Pancake Library	**Library**			
L	sortTokens	Internal		
L	getReserves	Internal		
L	quote	Internal		
Reentrancy Guard	**Implementation**			
L		Public !		NO !
HODL	**Implementation**	**Context, IBEP20, Ownable, Reentrancy Guard, VRF Consumer BaseV2**		
L		Public !		VRFConsumerBaseV2
L	getPancakePair	Public !		NO !
L	getPancakeRouter	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 ❗
L	approve	Public ❗	🛑	NO ❗
L	transferFrom	Public ❗	🛑	NO ❗
L	increaseAllowance	Public ❗	🛑	NO ❗
L	decreaseAllowance	Public ❗	🛑	NO ❗
L	isExcludedFromReward	Public ❗		NO ❗
L	totalFees	Public ❗		NO ❗
L	excludeFromReward	External ❗	🛑	onlyOwner
L	includeInReward	External ❗	🛑	onlyOwner
L	includeExcludeFromFee	External ❗	🛑	onlyOwner
L		External ❗	💵	NO ❗
L	_reflectFee	Private 🔐	🛑	
L	getRate	Public ❗		NO ❗
L	_takeLiquidity	Private 🔐	🛑	
L	removeAllFee	Private 🔐	🛑	
L	restoreAllFee	Private 🔐	🛑	
L	isExcludedFromFee	External ❗		NO ❗
L	_approve	Private 🔐	🛑	

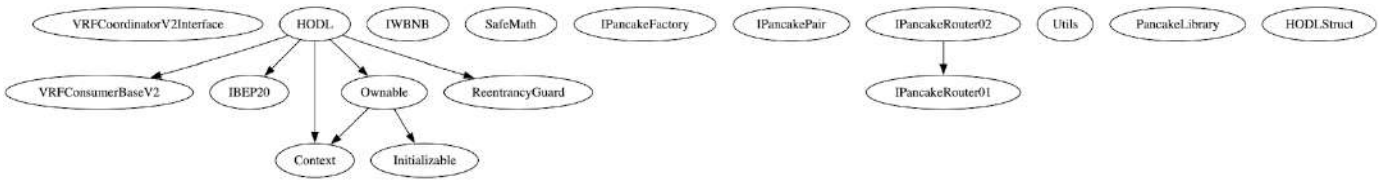
L	_transfer	Private 🔐	🛑	
L	_tokenTransfer	Private 🔐	🛑	
L	getMaxTxAmount	Public ❗		NO ❗
L	getLotteryInfo	Public ❗		NO ❗
L	LotteryTickets	Public ❗		NO ❗
L	setExcludeFromMaxTx	External ❗	🛑	onlyOwner
L	calculateBNBReward	External ❗		NO ❗
L	redeemRewards	External ❗	🛑	isHuman nonReentrant
L	topUpClaimCycleAfterTransfer	Private 🔐	🛑	
L	ensureMaxTxAmount	Private 🔐	🛑	
L	swapAndLiquify	Private 🔐	🛑	lockTheSwap
L	triggerSwapAndLiquify	External ❗	🛑	lockTheSwap
L	doSwapAndLiquify	Private 🔐	🛑	
L	changeAnyValue	External ❗	🛑	onlyOwner
L	changeTaxes	External ❗	🛑	onlyOwner
L	updatePairAddress	External ❗	🛑	onlyOwner
L	updatePoolAddress	External ❗	🛑	onlyOwner
L	updateVbAddress	External ❗	🛑	onlyOwner
L	startStacking	External ❗	🛑	NO ❗
L	getStacked	Public ❗		NO ❗

L	stopStackingAndClaim	External !	🛑	nonReentrant
L	fulfillRandomWords	Internal 🔒	🛑	
L	burnTokens	Private 🔐	🛑	
L	getAllTickets	External !		NO !
L	requestRandomWords	Private 🔐	🛑	
L	evaluatePendingLottery	External !	🛑	onlyOwner
L	changeHHBonus	External !	🛑	onlyOwner
L	getUserReinvested	External !		NO !
L	getReinvestBonus	External !		NO !
HODLStruct	**Library**			

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Inheritance Hierarchy

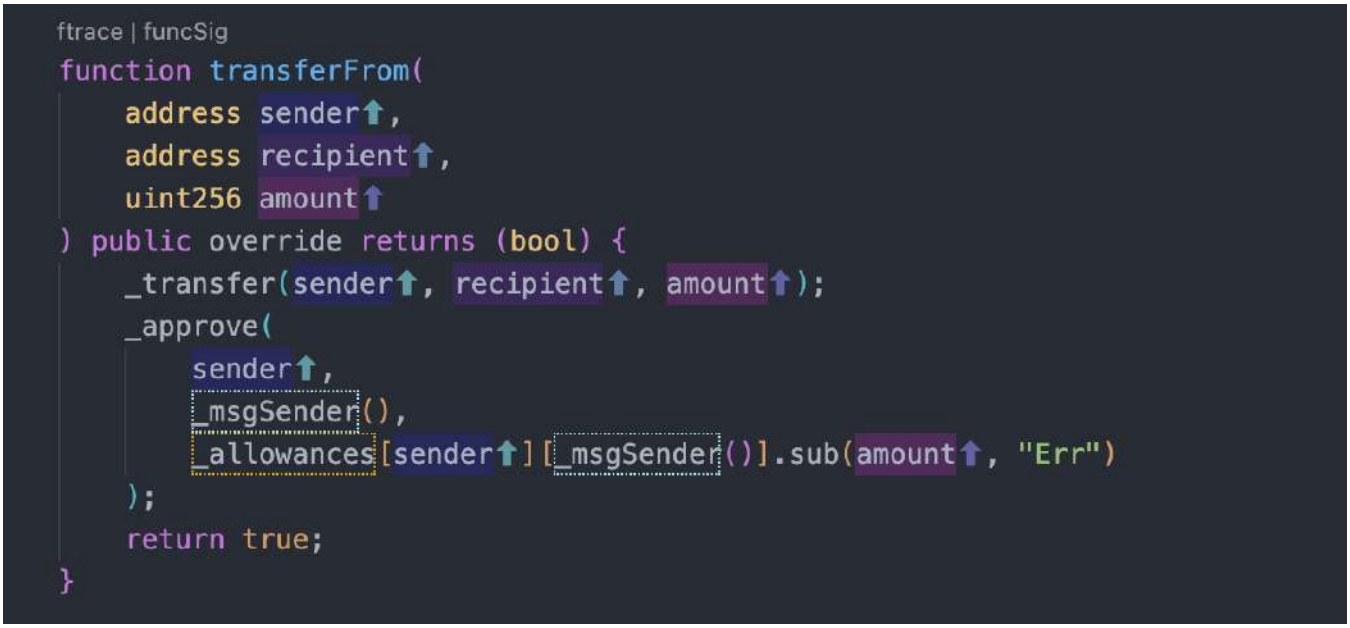


Security issue checking status

- **High severity issues: Informed and Fixed**

In transfer from function approved allowance checked and deduct after transferring tokens, because of this order this function can be manipulated with Reentrancy attack.

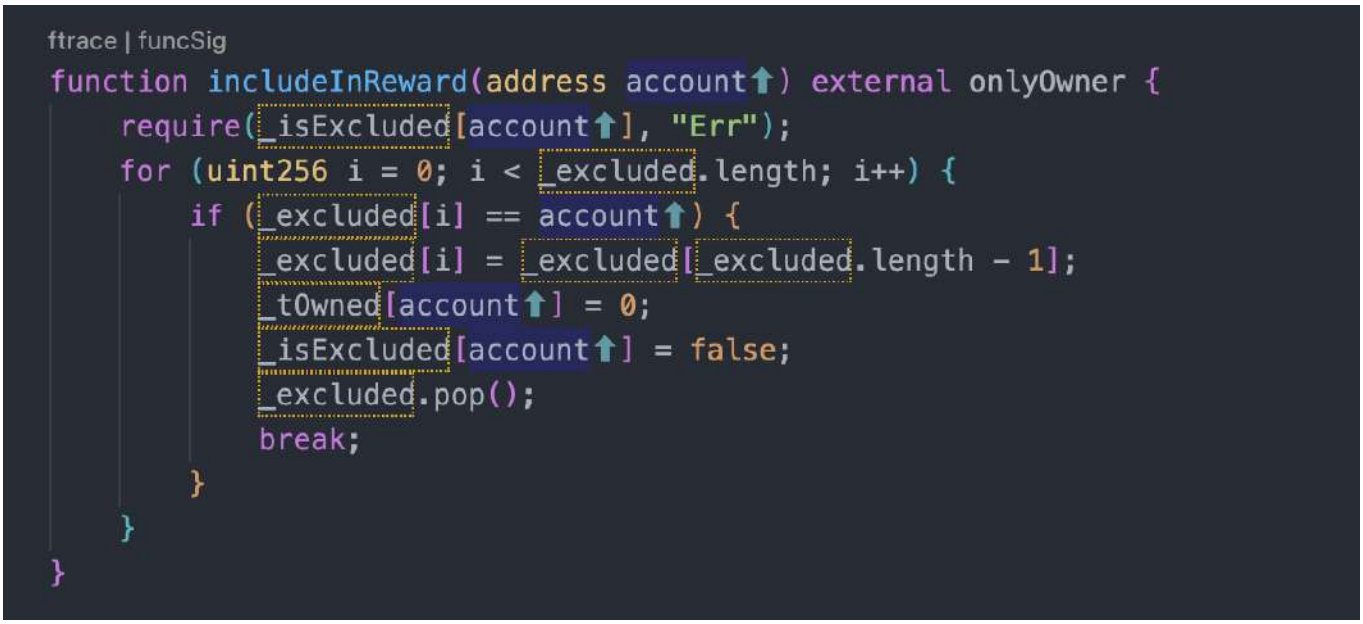
Recommendation: The transfer function should call after checking and deducting allowances.



- **Medium severity issues**
  No medium severity issues found

❖ **Low severity issues: Informed and Fixed**

If the excluded wallet length is too large, there is a possibility that this function may fail due to an out-of-gas error caused by the maximum gas limit of a block while looping through the excluded wallets.



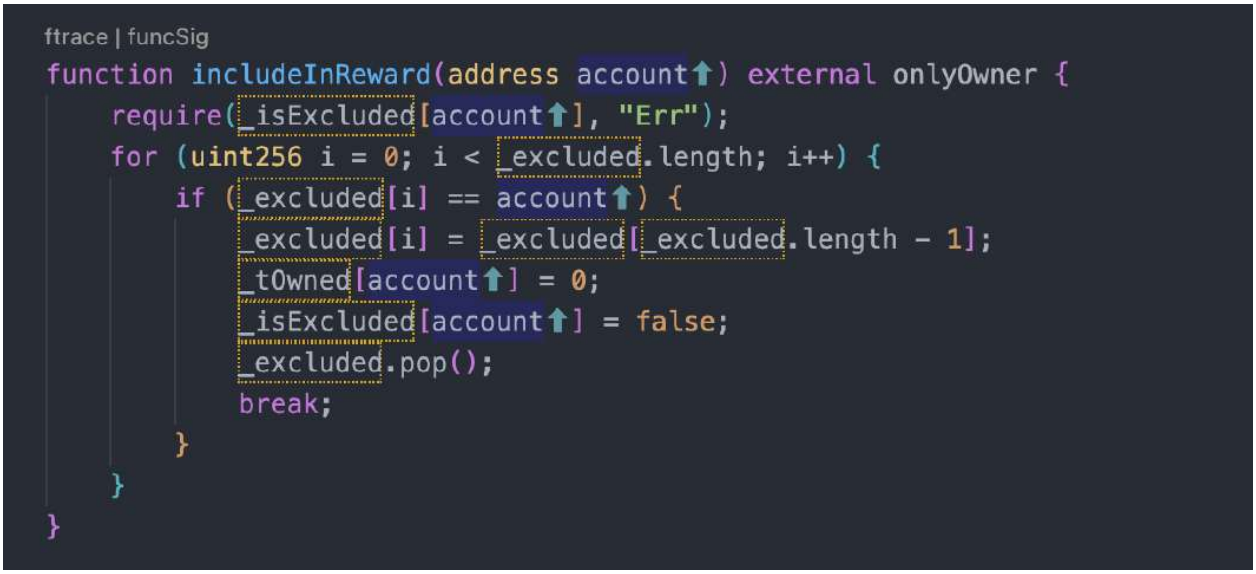
❖ **Centralization Risk**

This contract is a proxy contract and it's upgradable.

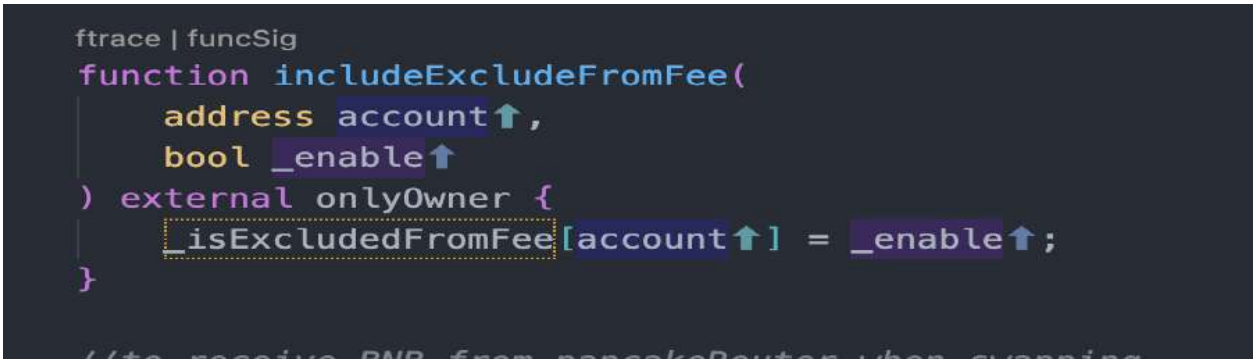
Owner privileges

- Owner can exclude wallets from reflections

- Owner can include wallets from reflections



- Owner can include/exclude wallets from transaction taxes



❖ Owner can change buy, sell, transfer taxes and max transaction amount

```
ftrace | funcSig
function changeAnyValue(uint8 _var⬆, uint256 _value⬆) external onlyOwner {
    if (_var⬆ == 1) {
        require(_value⬆ <= 110, "Err");
        selltax = _value⬆;
        emit changeValue("sell tax", _value⬆);
    } else if (_var⬆ == 2) {
        require(_value⬆ <= 110, "Err");
        buytax = _value⬆;
        emit changeValue("buy tax", _value⬆);
    } else if (_var⬆ == 3) {
        require(_value⬆ <= 110, "Err");
        transfertax = _value⬆;
        emit changeValue("transfer tax", _value⬆);
    }
```

❖ Owner can change swap percentages

```
ftrace | funcSig
function changeTaxes(
    uint256 bnbReward⬆,
    uint256 liquidity⬆,
    uint256 company⬆,
    uint256 reflection⬆,
    uint256 lottery⬆
) external onlyOwner {
    require(
        bnbReward⬆ + liquidity⬆ + company⬆ + reflection⬆ + lottery⬆ == 100,
        "Not 100"
    );
    taxes = Taxes(bnbReward⬆, liquidity⬆, company⬆, reflection⬆, lottery⬆);
    _Reflection = taxes.reflection;
    _Taxes = taxes.bnbReward.add(taxes.company).add(taxes.liquidity).add(
        taxes.lottery
    );
}
```

❖ Owner can add/remove new pair address

```
ftrace | funcSig
function updatePairAddress(
    address _pairAddress,
    bool _enable
) external onlyOwner {
    pairAddresses[_pairAddress] = _enable;
}
```

❖ Owner can add/remove pool address

```
ftrace | funcSig
function updatePoolAddress(
    address _poolAddress,
    bool _enable
) external onlyOwner {
    poolAddresses[_poolAddress] = _enable;
}
```

❖ Owner can change bonus percentages for NFT holders

```
ftrace | funcSig
function changeHHBonus(
    uint8 layer,
    uint16 _threshold,
    uint16 _bonus
) external onlyOwner {
    HHBonus[layer].threshold = _threshold;
    HHBonus[layer].bonus = _bonus;
}
```

Audit conclusion

RugFreeCoins team has performed in-depth tests, 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: **7**

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

Smart contract active ownership: **ACTIVE**

Note: The token smart contract is implemented as a proxy contract, and as such, it is designed to be upgradeable. More information regarding this aspect can be found in the audit report, which accurately reflects the state of affairs at the time of the audit.