RugFreeCoins Audit

Presale World Token
Smart Contract Security Audit

September 14 2022

Contents

Audit details

Audited project
Presale World Token

Contract Address

0x5C197A2D2c9081D30715C80bD1b57c996A14cda0

Client contact

Presale World Team

Blockchain

Binance smart chain

Project website

www.presale.world

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 set fees over 25%.

☑ The owner can't blacklist wallets.

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

Background

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

https://bscscan.com/token/0x5C197A2D2c9081D30715C80bD1b57c996A14cda0

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.

.

Roadmap

Q3 2022

- $PRESALE token launch
- CG/CMC listings
- CertiK audit for the platform and token
- Banner advertisement campaigns for both platform and token
- "Grey" marketing for trending services and exposure across the crypto space
- Increase amount of launchpad partners
- Brand alignment - fix color schemes across platform and token
- Large scale shill campaigns to promote the use of pool protection and PresaleWorld as a whole
- Recruiting for social media team
- Increase software engineer team size
- Top 10 CEX listing

Q4 and Beyond

- Continuous paid and unpaid marketing campaigns
- Expand central exchange listings limiting to the top 10
- Investigate, design and create an app for PresaleWorld

Tokenomics

4% when buying & selling

- 4% of trade goes to the marketing wallet in BNB.

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 interested in taking part with presale world utilities.
- Anyone who’s interested in taking part in the future plans of the Presale World Token.
- Anyone who’s interested in making financial transactions with any other party using Presale World Token as the currency.

Potential to grow with score points

1.	Project efficiency	9/10
2.	Project uniqueness	9/10
3	Information quality	9/10
4	Service quality	9/10
5	System quality	9/10
6	Impact on the community	9/10
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		**9.2/10**

Contract details

Token contract details for 14th of September 2022

Contract name	presale.world
Contract address	0x5C197A2D2c9081D30715C80bD1b57c996A14cda0
Token supply	100,000,000
Token ticker	PRESALE
Decimals	18
Token holders	1
Transaction count	2
Contract deployer address	0xc14aDc92d46ABC85A8A04c1eD46b5c0534c621b7
Contract’s current owner address	0xe05f374330242b2091c2d32165c3232d09a4acd8

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
Context	**Implementation**			
L	_msgSender	Internal 🔒		
L	_msgData	Internal 🔒		
Ownable	**Implementation**	**Context**		
L		Public ❗	🛑	NO❗
L	owner	Public ❗		NO❗
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❗

└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
Reentrancy Guard	**Implementation**			
└		Public ❗	🛑	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❗
IUniswapV2 Pair	**Interface**			
└	name	External ❗		NO❗
└	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❗

L	sync	External ❗	🛑	NO❗
L	initialize	External ❗	🛑	NO❗
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❗

└	getAmountsOut	External ❗		NO❗
└	getAmountsIn	External ❗		NO❗
IUniswapV2 Router02	**Interface**	**IUniswapV2 Router01**		
└	removeLiquidityETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
└	swapExactETHForTokensSupportingFeeOnTransferTokens	External ❗	💵	NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
Token Marketing	**Implementation**	**IERC20, Ownable, Reentrancy Guard**		
└		Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	totalSupply	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	currentSupply	Public ❗		NO❗
└	getNumTokensBeforeSwap	Public ❗		NO❗
└	setNumTokenSwapPerMille	External ❗	🛑	NO❗

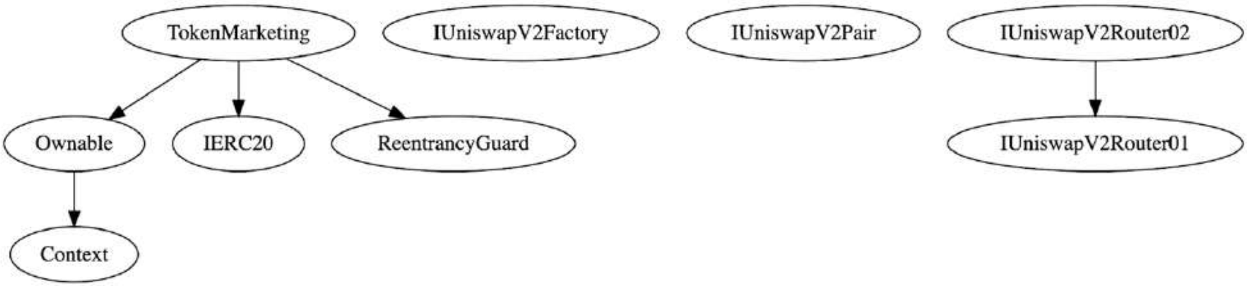
└	transfer	Public ❗	🛑	NO❗
└	allowance	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗
└	totalTaxes	Public ❗		NO❗
└	includeInFee	Public ❗	🛑	onlyOwner
└	excludeFromFee	Public ❗	🛑	onlyOwner
└	isExcludedFromFee	Public ❗		NO❗
└	setCharityAddress	External ❗	🛑	onlyOwner
└	setCharityFee	External ❗	🛑	onlyOwner
└	setMarketingAddress	External ❗	🛑	onlyOwner
└	setMarketingFee	External ❗	🛑	onlyOwner
└	removeAllFees	External ❗	🛑	onlyOwner
└	restoreAllFees	External ❗	🛑	onlyOwner
└	setSwapEnabled	Public ❗	🛑	onlyOwner
└	withdrawExcessETH	External ❗	🛑	nonReentrant onlyOwner
└		External ❗	💵	NO❗
└	_calculateCharityFee	Private 🔐		

L	_calculateMarketingFee	Private 🔐		
L	_swapTokensAndDistributeETH	Private 🔐	🛑	lockTheSwap
L	_swapTokensForEth	Private 🔐	🛑	
L	_approve	Internal 🔒	🛑	
L	_transfer	Private 🔐	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Inheritance Hierarchy

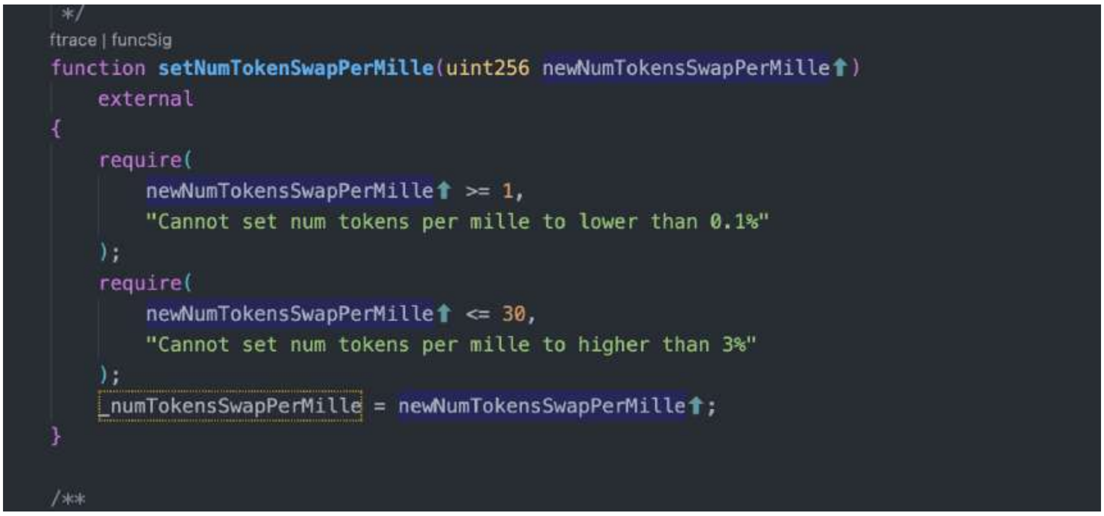


Security issue checking status

- ### High severity issues

Informed and fixed

Anyone can change the swap point by changing _numTokensSwapPerMille variable, this function should be able to call only by the owner



```
*/
ftrace | funcSig
function setNumTokenSwapPerMille(uint256 newNumTokensSwapPerMille)
    external
{
    require(
        newNumTokensSwapPerMille >= 1,
        "Cannot set num tokens per mille to lower than 0.1%"
    );
    require(
        newNumTokensSwapPerMille <= 30,
        "Cannot set num tokens per mille to higher than 3%"
    );
    _numTokensSwapPerMille = newNumTokensSwapPerMille;
}

/**
```

- ### Medium severity issues

  No medium severity issues found

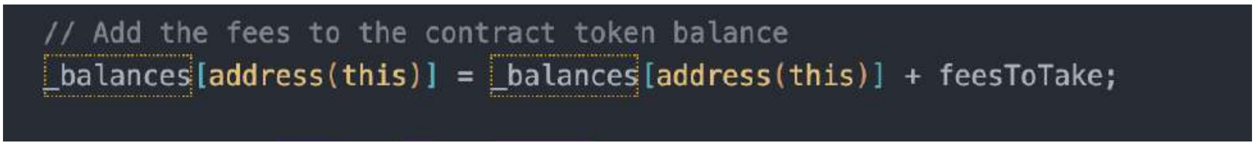
- ### Low severity issues

  No low severity issues found

- ### Informational issues

Informed and fixed

Transfer event should fire when transferring fees to the contract



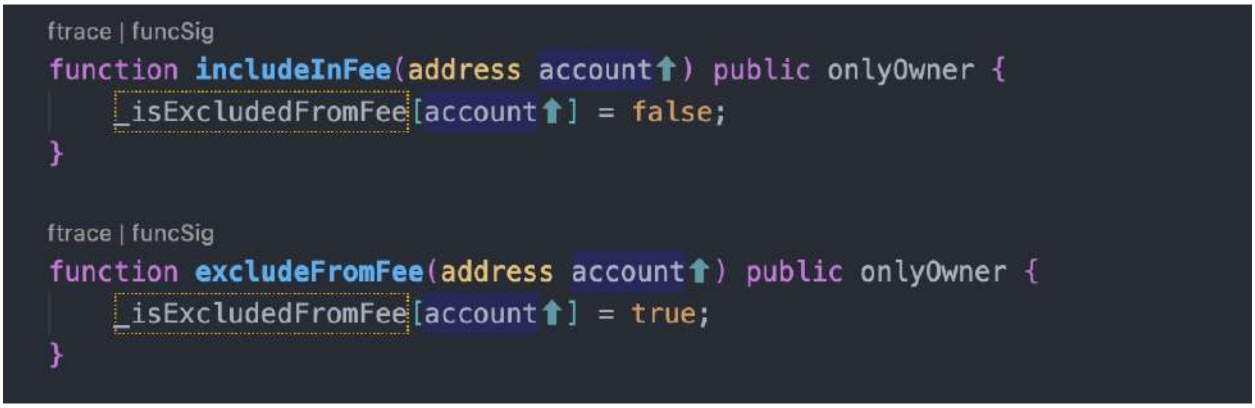
```
// Add the fees to the contract token balance
_balances[address(this)] = _balances[address(this)] + feesToTake;
```

- ### Centralization Risk

  No Centralization Risk found

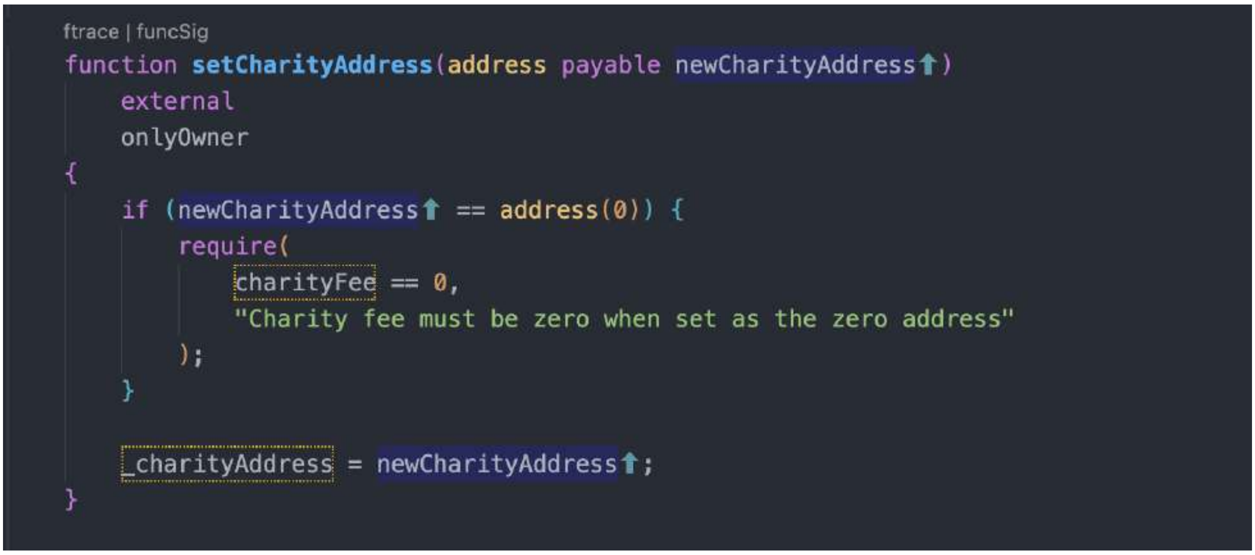
Owner privileges

- ❖ Owner can include/exclude wallets from fees



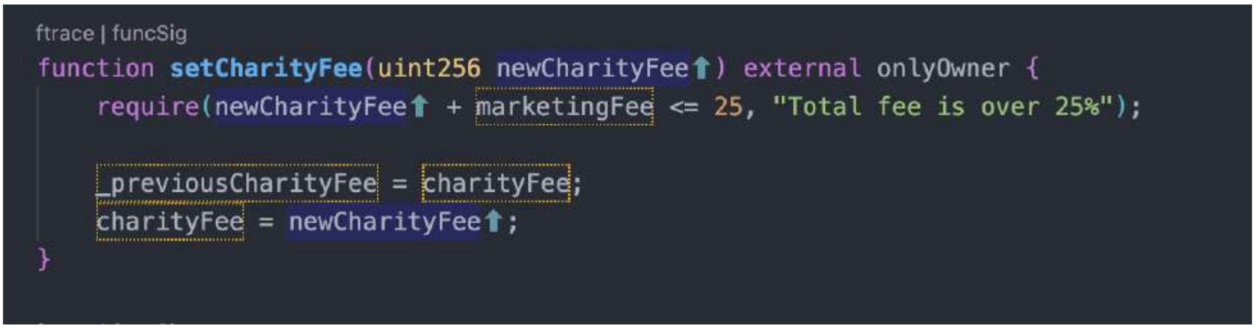
```
ftrace | funcSig
function includeInFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = false;
}

ftrace | funcSig
function excludeFromFee(address account) public onlyOwner {
    _isExcludedFromFee[account] = true;
}
```

- ❖ Owner can change charity wallet address



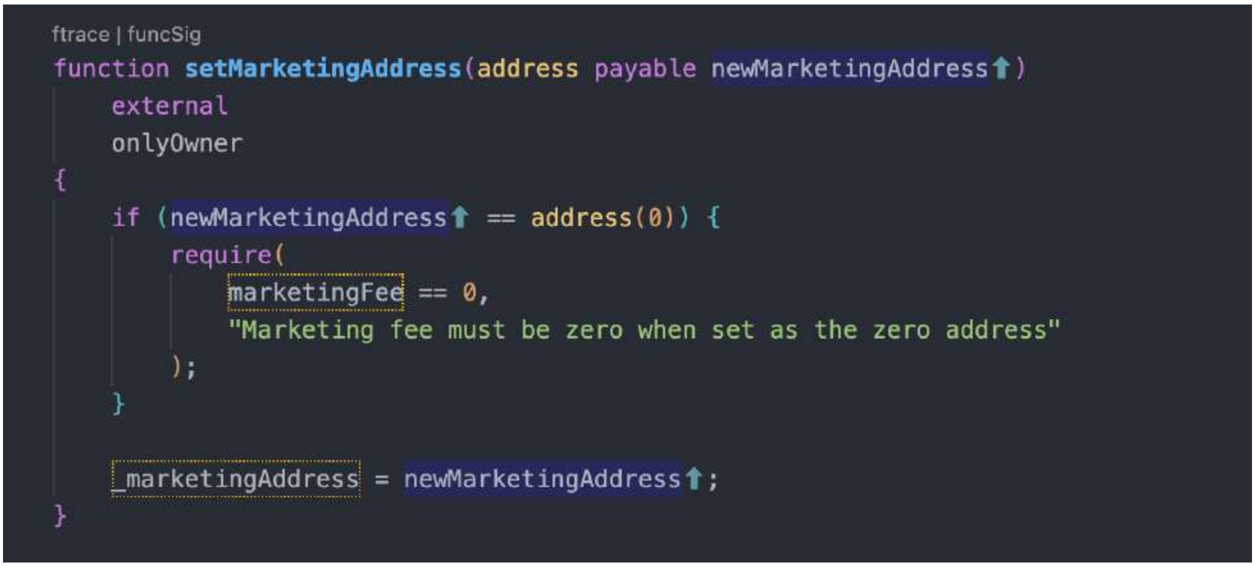
```
ftrace | funcSig
function setCharityAddress(address payable newCharityAddress)
    external
    onlyOwner
{
    if (newCharityAddress == address(0)) {
        require(
            charityFee == 0,
            "Charity fee must be zero when set as the zero address"
        );
    }

    _charityAddress = newCharityAddress;
}
```

- ❖ Owner can change charity fee, total fees maximum up to 25%



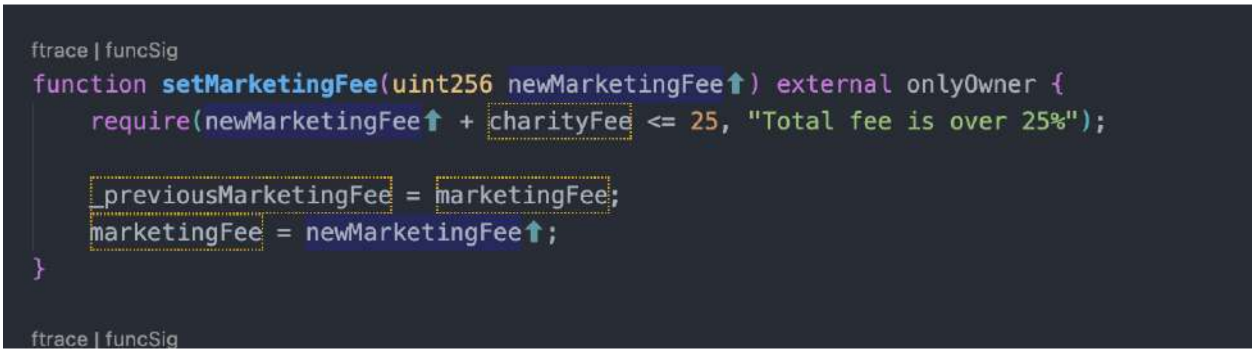
```
ftrace | funcSig
function setCharityFee(uint256 newCharityFee) external onlyOwner {
    require(newCharityFee + marketingFee <= 25, "Total fee is over 25%");

    _previousCharityFee = charityFee;
    charityFee = newCharityFee;
}
```

- Owner can change marketing wallet address



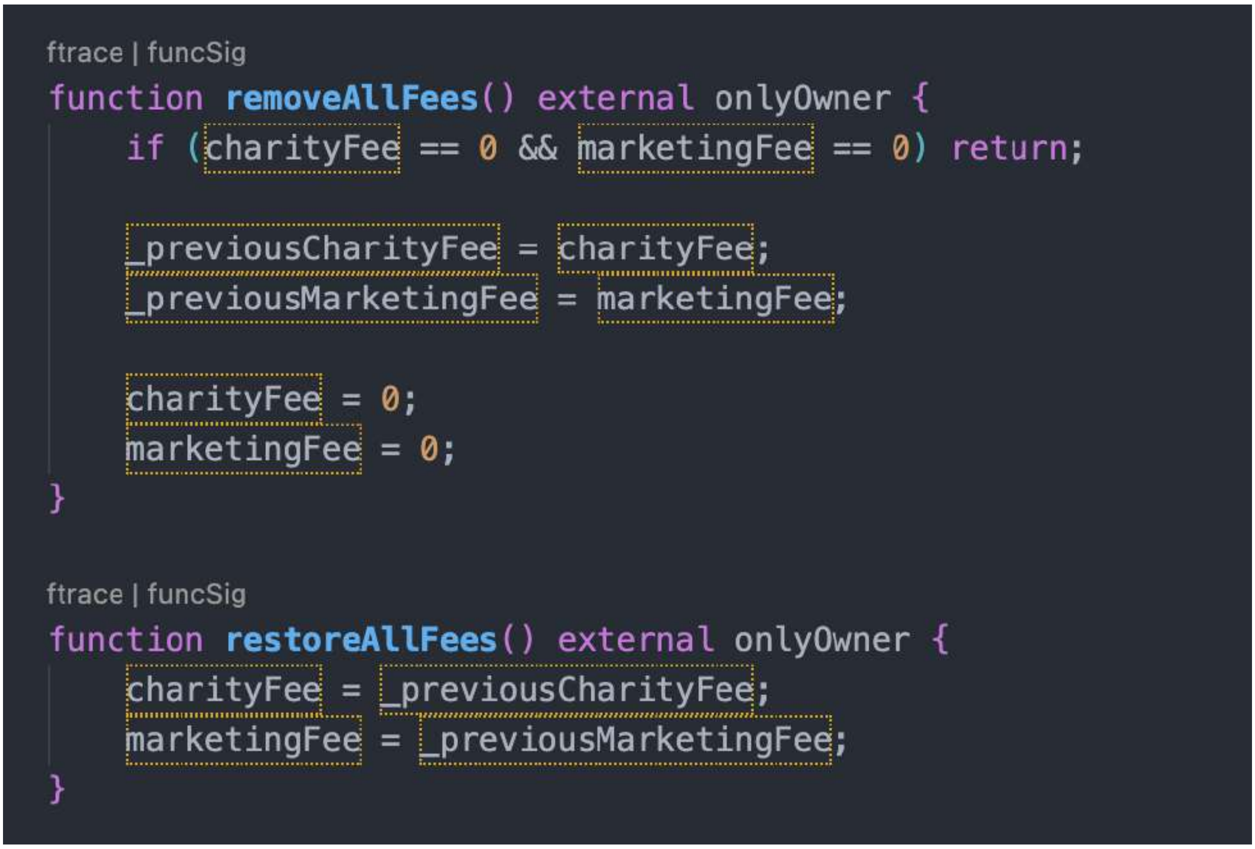
```
ftrace | funcSig
function setMarketingAddress(address payable newMarketingAddress)
    external
    onlyOwner
{
    if (newMarketingAddress == address(0)) {
        require(
            marketingFee == 0,
            "Marketing fee must be zero when set as the zero address"
        );
    }

    _marketingAddress = newMarketingAddress;
}
```

- Owner can change marketing fee, total fees maximum up to 25%



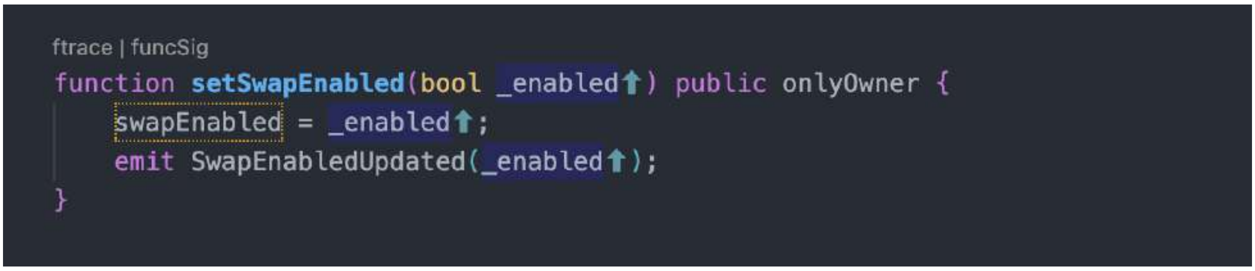
```
ftrace | funcSig
function setMarketingFee(uint256 newMarketingFee) external onlyOwner {
    require(newMarketingFee + charityFee <= 25, "Total fee is over 25%");

    _previousMarketingFee = marketingFee;
    marketingFee = newMarketingFee;
}

ftrace | funcSig
```

- Owner can remove and restore all fees



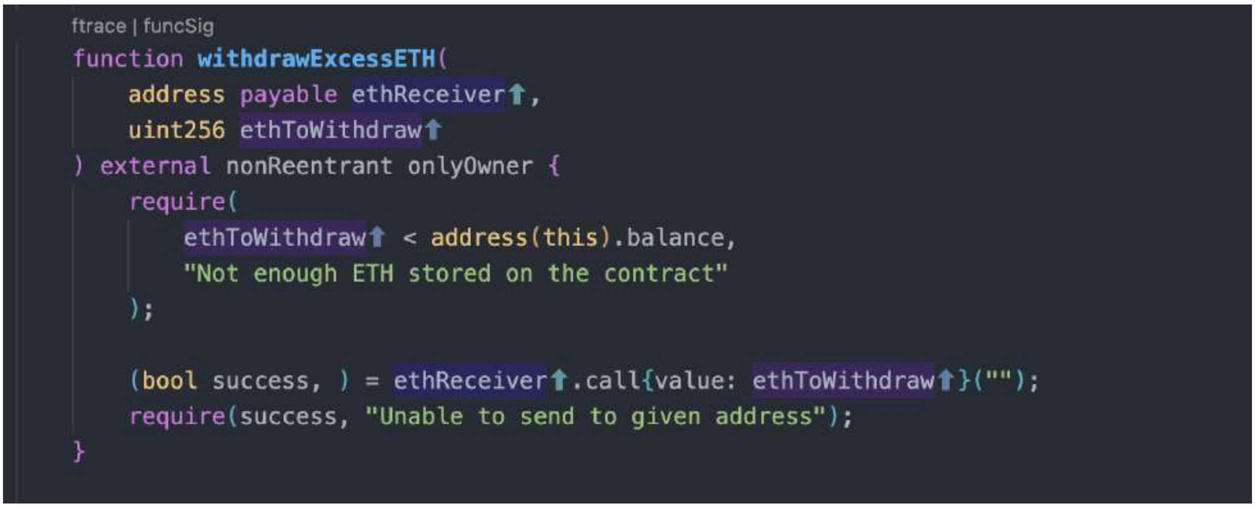
```
ftrace | funcSig
function removeAllFees() external onlyOwner {
    if (charityFee == 0 && marketingFee == 0) return;

    _previousCharityFee = charityFee;
    _previousMarketingFee = marketingFee;

    charityFee = 0;
    marketingFee = 0;
}

ftrace | funcSig
function restoreAllFees() external onlyOwner {
    charityFee = _previousCharityFee;
    marketingFee = _previousMarketingFee;
}
```

- Owner can enable/disable swap



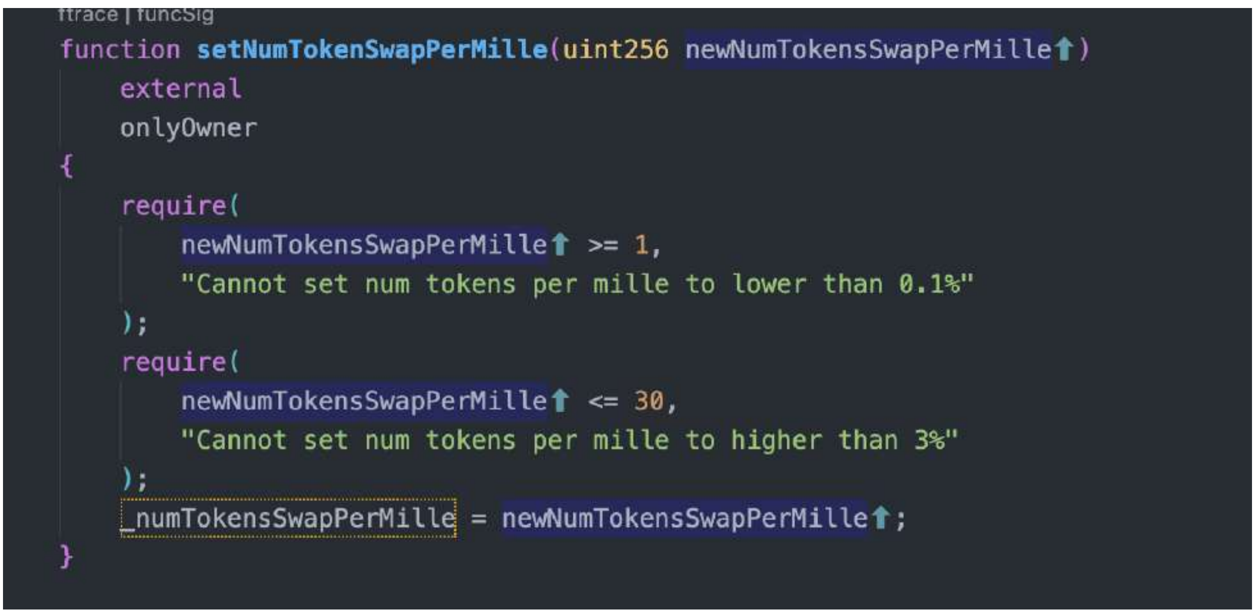
```
ftrace | funcSig
function setSwapEnabled(bool _enabled↑) public onlyOwner {
    swapEnabled = _enabled↑;
    emit SwapEnabledUpdated(_enabled↑);
}
```

- ❖ Owner can withdraw bnb from the contract



```
ftrace | funcSig
function withdrawExcessETH(
    address payable ethReceiver,
    uint256 ethToWithdraw
) external nonReentrant onlyOwner {
    require(
        ethToWithdraw < address(this).balance,
        "Not enough ETH stored on the contract"
    );

    (bool success, ) = ethReceiver.call{value: ethToWithdraw}("");
    require(success, "Unable to send to given address");
}
```

- ❖ Owner can change swap point



```
ftrace | funcSig
function setNumTokenSwapPerMille(uint256 newNumTokensSwapPerMille)
    external
    onlyOwner
{
    require(
        newNumTokensSwapPerMille >= 1,
        "Cannot set num tokens per mille to lower than 0.1%"
    );
    require(
        newNumTokensSwapPerMille <= 30,
        "Cannot set num tokens per mille to higher than 3%"
    );
    _numTokensSwapPerMille = newNumTokensSwapPerMille;
}
```

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: **9**

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

Smart contract active ownership: **YES**