RUGFREECOINS

# Blast Domains Token

RugfreeCoins Verified on February 05th, 2024

# Overview

✅ No mint function found, the owner cannot mint tokens after initial deployment.

✅ The owner can't set a max transaction limit

✅ The owner can't pause trading once it's enabled

❌ The owner must enable trade for the holders, if trading remains disabled, no one would be able to buy and sell.

✅ The owner can't change fees.

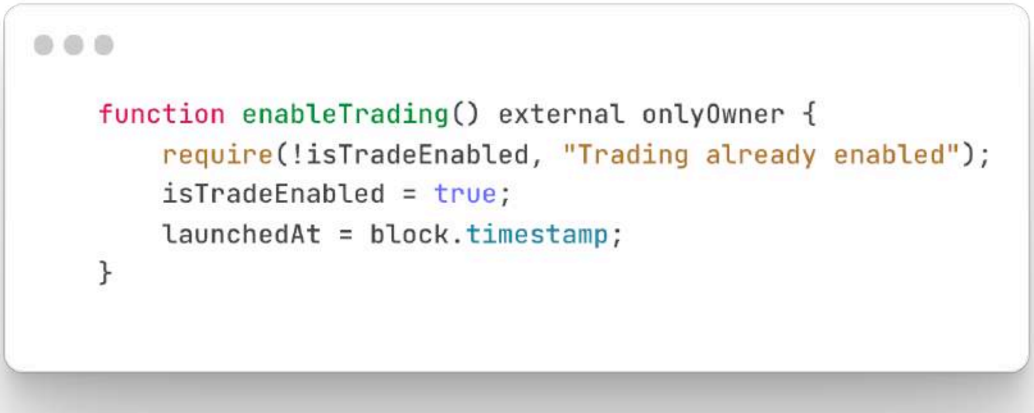
✅ The owner can't blacklist wallets.

✅ The owner can't set a max wallet limit

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

## ❗ HIGH SEVERITY ISSUES

The owner must enable trade for the holders, if trading remains disabled, no one would be able to buy and sell.



```
function enableTrading() external onlyOwner {
    require(!isTradeEnabled, "Trading already enabled");
    isTradeEnabled = true;
    launchedAt = block.timestamp;
}
```

# Contents

# Audit details

**Audited project**

Blast Domains Token

**Contract Address**

0x35404bCF27188e7252DF6b723A06969A3c04501C

**Client contact**

Blast Domains Token Team

**Blockchain**

Ethereum Mainnet

**Project website**

https://www.blastdomains.org/

# 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.

# Background

**RugfreeCoins** was commissioned by the **Blast Domains Token Team** to perform an audit of the smart contract.

**https://etherscan.io/address/0x35404bCF27188e7252DF6b723A06969A3c04501C#code**

This audit focuses on verifying 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.

# Tokenomics

### ▲ 3% tax when buying

2% of trade goes to the treasury wallet in ETH
1% of trade goes to the marketing wallet in ETH

### ▲ 4% tax when selling

2% of trade goes to the treasury wallet in ETH
2% of trade goes to the marketing wallet in ETH

# Target market and the concept

- 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 in the Blast Domains token ecosystem.
- Anyone who’s interested in taking part in the future plans of Blast Domains Token.
- Anyone who’s interested in making financial transactions with any other party Blast Domains Token as the currency.

# Potential to grow with score points

| | |
|---|---|
| ⚡ Project efficiency | 10 / 10 |
| 🌟 Project uniqueness | 10 / 10 |
| 📊 Information quality | 10 / 10 |
| 👌 Service quality | 10 / 10 |
| 💻 System quality | 10 / 10 |
| 🌍 Impact on the community | 10 / 10 |
| 💼 Impact on the business | 10 / 10 |
| 🔮 Preparing for the future | 10 / 10 |
| 🔒 Smart contract security | 9 / 10 |
| 🛠️ Smart contract functionality assessment | 10 / 10 |
| 🏆 **Total Score** | **9.9 / 10** |

# Contract details

Token contract details for 05th of February 2024

| | |
|---|---|
| Contract name | **Blast Domains** |
| Contract address | **0x35404bCF27188e7252DF6b723A06969A3c04501C** |
| Token supply | **10,000,000,000** |
| Token ticker | **BD** |
| Decimals | **18** |
| Token holders | **1** |
| Transaction count | **1** |
| Contract deployer address | **0x17D53aC59a9f1F399584cbba850a772b4f526937** |
| Contract’s current owner address | **0x17D53aC59a9f1F399584cbba850a772b4f526937** |
| Treasury wallet | **0x75756306Fdd4d6b83B0c91463ac6050D92ca4d34** |
| Marketing wallet | **0x17D53aC59a9f1F399584cbba850a772b4f526937** |

# Contract code function details

| № | Category | Item | Result |
|---|---|---|---|
| 1 | Coding conventions | ERC20 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 & centralisation | Access control of owners | HIGH |
| | | Business logics | PASS |
| | | Business implementation | 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 |
| | | | | |
| **BD** | **Implementation** | **IERC20, Ownable** | | |
| L | | Public ❗ | 🛑 | NO ❗ |
| L | | External ❗ | 💵 | NO ❗ |
| L | totalSupply | External ❗ | | NO ❗ |
| L | name | Public ❗ | | NO ❗ |
| L | symbol | Public ❗ | | NO ❗ |
| L | decimals | Public ❗ | | NO ❗ |
| L | balanceOf | Public ❗ | | NO ❗ |
| L | allowance | External ❗ | | NO ❗ |
| L | approve | Public ❗ | 🛑 | NO ❗ |
| L | _approve | Internal 🔒 | 🛑 | |
| L | approveMax | External ❗ | 🛑 | NO ❗ |
| L | transfer | External ❗ | 🛑 | NO ❗ |
| L | transferFrom | External ❗ | 🛑 | NO ❗ |
| L | _transferFrom | Internal 🔒 | 🛑 | |
| L | takeFee | Internal 🔒 | 🛑 | |

| | | | | |
|---|---|---|---|---|
| └ | _basicTransfer | Internal 🔒 | 🛑 | |
| └ | shouldTakeFee | Internal 🔒 | | |
| └ | shouldDoContractSwap | Internal 🔒 | | |
| └ | isFeeExcluded | Public ❗ | | NO ❗ |
| └ | doContractSwap | Internal 🔒 | 🛑 | swapping |
| └ | swapTokensForEth | Private 🔐 | 🛑 | |
| └ | setIsFeeExempt | External ❗ | 🛑 | onlyOwner |
| └ | setDoContractSwap | External ❗ | 🛑 | onlyOwner |
| └ | changeMarketingWallet | External ❗ | 🛑 | onlyOwner |
| └ | changeTreasuryWallet | External ❗ | 🛑 | onlyOwner |
| └ | changeSellFees | External ❗ | 🛑 | onlyOwner |
| └ | changeBuyFees | External ❗ | 🛑 | onlyOwner |
| └ | enableTrading | External ❗ | 🛑 | onlyOwner |
| └ | setAuthorizedWallets | External ❗ | 🛑 | onlyOwner |
| └ | rescueETH | External ❗ | 🛑 | onlyOwner |
| └ | toggleTransferTax | External ❗ | 🛑 | onlyOwner |
| | | | | |
| **Ownable** | **Implementation** | **Context** | | |
| └ | | Public ❗ | 🛑 | NO ❗ |
| └ | owner | Public ❗ | | NO ❗ |
| └ | _checkOwner | Internal 🔒 | | |

|  |  |  |  |  |
|---|---|---|---|---|
| └ | renounceOwnership | Public ❗ | 🛑 | onlyOwner |
| └ | transferOwnership | Public ❗ | 🛑 | onlyOwner |
| └ | _transferOwnership | Internal 🔒 | 🛑 |  |
|  |  |  |  |  |
| **IERC20** | **Interface** |  |  |  |
| └ | totalSupply | External ❗ |  | NO ❗ |
| └ | balanceOf | External ❗ |  | NO ❗ |
| └ | transfer | External ❗ | 🛑 | NO ❗ |
| └ | allowance | External ❗ |  | NO ❗ |
| └ | approve | External ❗ | 🛑 | NO ❗ |
| └ | transferFrom | External ❗ | 🛑 | NO ❗ |
|  |  |  |  |  |
| **Context** | **Implementation** |  |  |  |
| └ | _msgSender | Internal 🔒 |  |  |
| └ | _msgData | Internal 🔒 |  |  |
| └ | _contextSuffixLength | Internal 🔒 |  |  |
|  |  |  |  |  |
| **IUniswapV2 Factory** | **Interface** |  |  |  |
| └ | feeTo | External ❗ |  | NO ❗ |
| └ | feeToSetter | External ❗ |  | NO ❗ |
| └ | getPair | External ❗ |  | NO ❗ |
| └ | allPairs | External ❗ |  | NO ❗ |

| | | | | |
|---|---|---|---|---|
| L | allPairsLength | External ❗ | | NO ❗ |
| L | createPair | External ❗ | 🛑 | NO ❗ |
| L | setFeeTo | External ❗ | 🛑 | NO ❗ |
| L | setFeeToSetter | 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 ❗ |

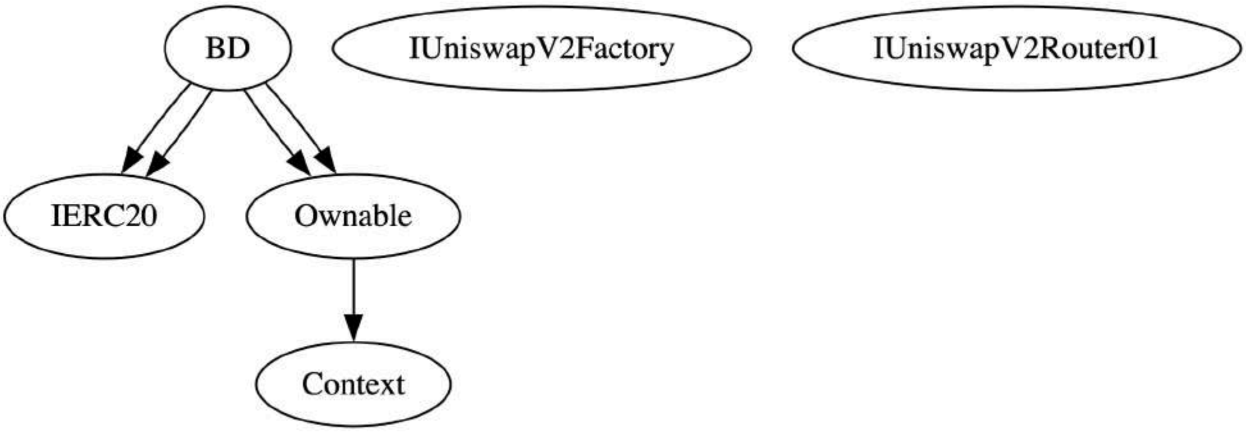
|  |  |  |  |  |
|---|---|---|---|---|
| L | quote | External ❗ |  | NO ❗ |
| L | getAmountOut | External ❗ |  | NO ❗ |
| L | getAmountIn | External ❗ |  | NO ❗ |
| L | getAmountsOut | External ❗ |  | NO ❗ |
| L | getAmountsIn | External ❗ |  | NO ❗ |
|  |  |  |  |  |
| **BD** | **Implementation** | **IERC20, Ownable** |  |  |
| L |  | Public ❗ | 🛑 | NO ❗ |
| L |  | External ❗ | 💵 | NO ❗ |
| L | totalSupply | External ❗ |  | NO ❗ |
| L | name | Public ❗ |  | NO ❗ |
| L | symbol | Public ❗ |  | NO ❗ |
| L | decimals | Public ❗ |  | NO ❗ |
| L | balanceOf | Public ❗ |  | NO ❗ |
| L | allowance | External ❗ |  | NO ❗ |
| L | approve | Public ❗ | 🛑 | NO ❗ |
| L | _approve | Internal 🔒 | 🛑 |  |
| L | approveMax | External ❗ | 🛑 | NO ❗ |
| L | transfer | External ❗ | 🛑 | NO ❗ |
| L | transferFrom | External ❗ | 🛑 | NO ❗ |
| L | _transferFrom | Internal 🔒 | 🛑 |  |
| L | takeFee | Internal 🔒 | 🛑 |  |

| | | | | |
|---|---|---|---|---|
| L | _basicTransfer | Internal 🔒 | 🛑 | |
| L | shouldTakeFee | Internal 🔒 | | |
| L | shouldDoContractSwap | Internal 🔒 | | |
| L | isFeeExcluded | Public ❗ | | NO ❗ |
| L | doContractSwap | Internal 🔒 | 🛑 | swapping |
| L | swapTokensForEth | Private 🔐 | 🛑 | |
| L | setIsFeeExempt | External ❗ | 🛑 | onlyOwner |
| L | setDoContractSwap | External ❗ | 🛑 | onlyOwner |
| L | changeMarketingWallet | External ❗ | 🛑 | onlyOwner |
| L | changeTreasuryWallet | External ❗ | 🛑 | onlyOwner |
| L | changeSellFees | External ❗ | 🛑 | onlyOwner |
| L | changeBuyFees | External ❗ | 🛑 | onlyOwner |
| L | enableTrading | External ❗ | 🛑 | onlyOwner |
| L | setAuthorizedWallets | External ❗ | 🛑 | onlyOwner |
| L | rescueETH | External ❗ | 🛑 | onlyOwner |
| L | toggleTransferTax | External ❗ | 🛑 | onlyOwner |

## Legend

| Symbol | Meaning |
|---|---|
| 🛑 | Function can modify state |
| 💵 | Function is payable |

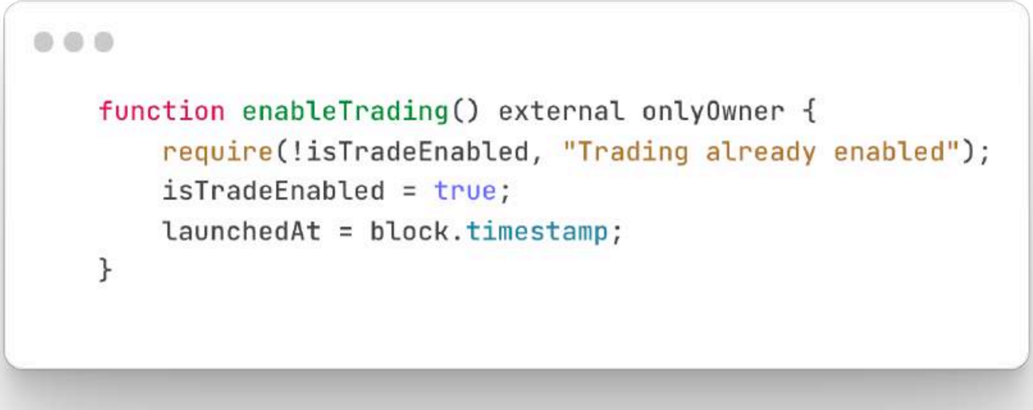
# Inheritance Hierarchy



# Security issue checking status

❖ High severity issues

The owner must enable trade for the holders, if trading remains disabled, no one would be able to buy and sell.



```
function enableTrading() external onlyOwner {
    require(!isTradeEnabled, "Trading already enabled");
    isTradeEnabled = true;
    launchedAt = block.timestamp;
}
```

❖ Medium severity issues

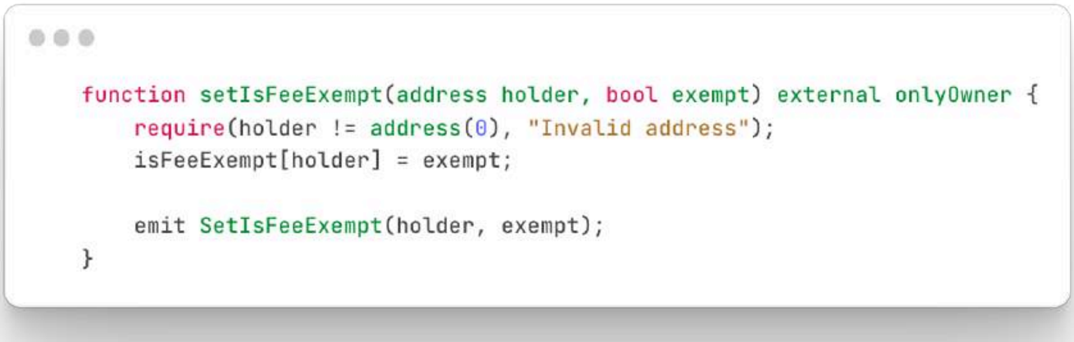
No medium severity issues found

❖ Low severity issues

No high severity issues found

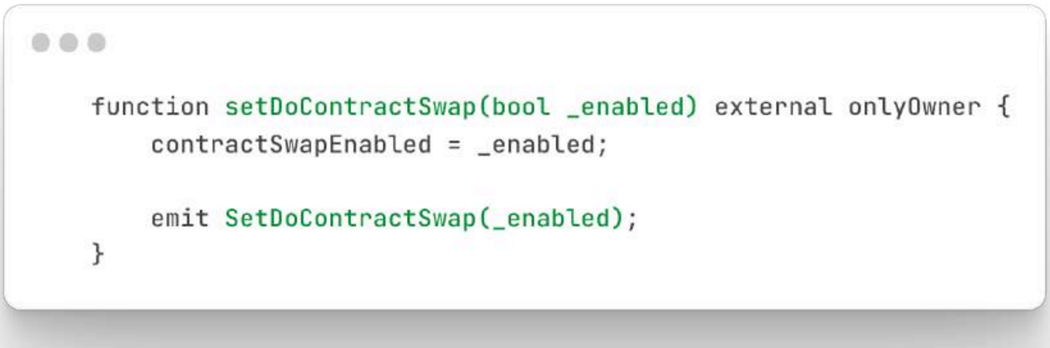
# Owner privileges

- ❖ Owner can include/exclude wallets from fees



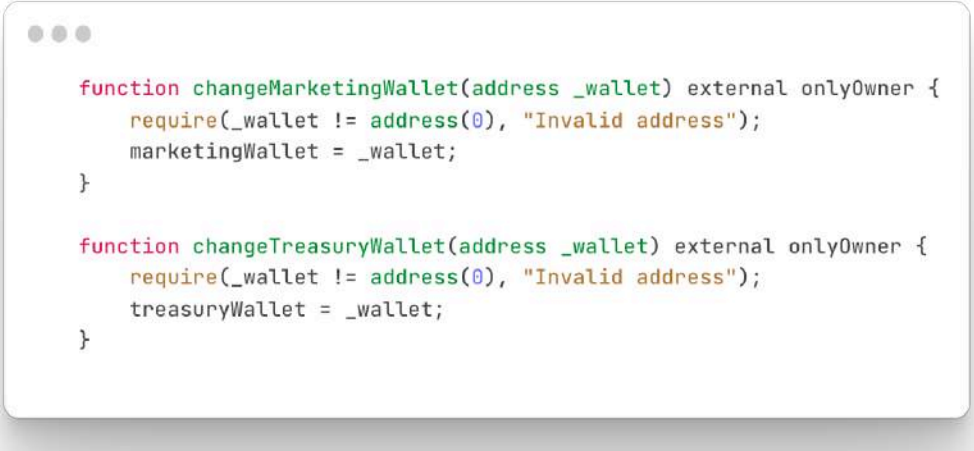
```
function setIsFeeExempt(address holder, bool exempt) external onlyOwner {
    require(holder != address(0), "Invalid address");
    isFeeExempt[holder] = exempt;

    emit SetIsFeeExempt(holder, exempt);
}
```

- ❖ Owner can enable/disable swapping



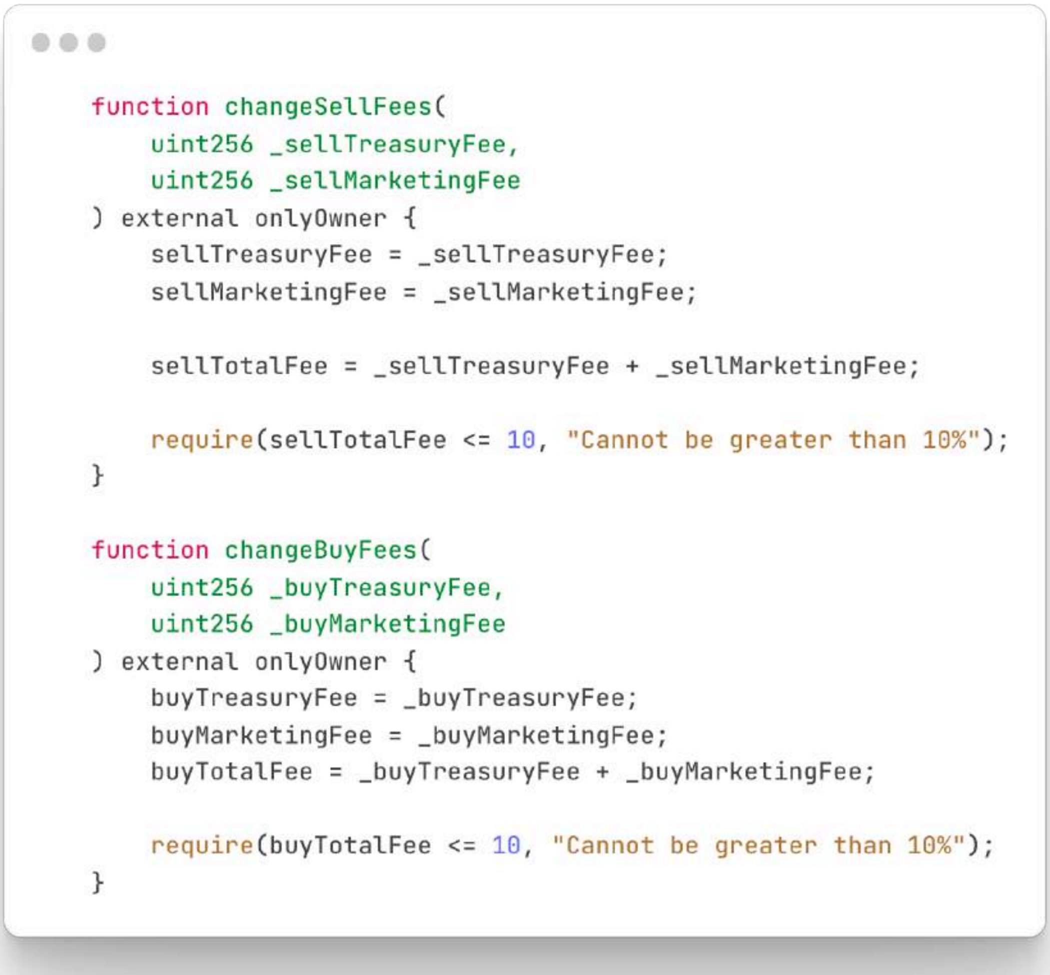
```
function setDoContractSwap(bool _enabled) external onlyOwner {
    contractSwapEnabled = _enabled;

    emit SetDoContractSwap(_enabled);
}
```

- ❖ Owner can change marketing and treasury wallet



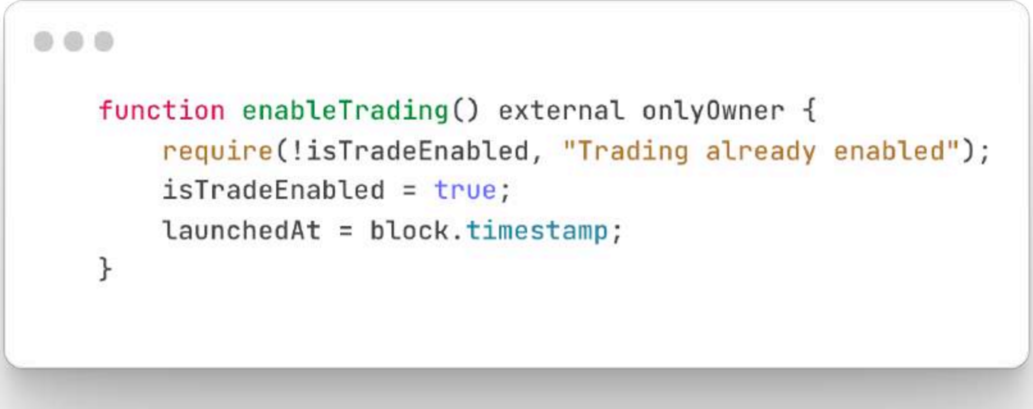
```
function changeMarketingWallet(address _wallet) external onlyOwner {
    require(_wallet != address(0), "Invalid address");
    marketingWallet = _wallet;
}

function changeTreasuryWallet(address _wallet) external onlyOwner {
    require(_wallet != address(0), "Invalid address");
    treasuryWallet = _wallet;
}
```

- Owner can change buy and sell fees each up to 10%



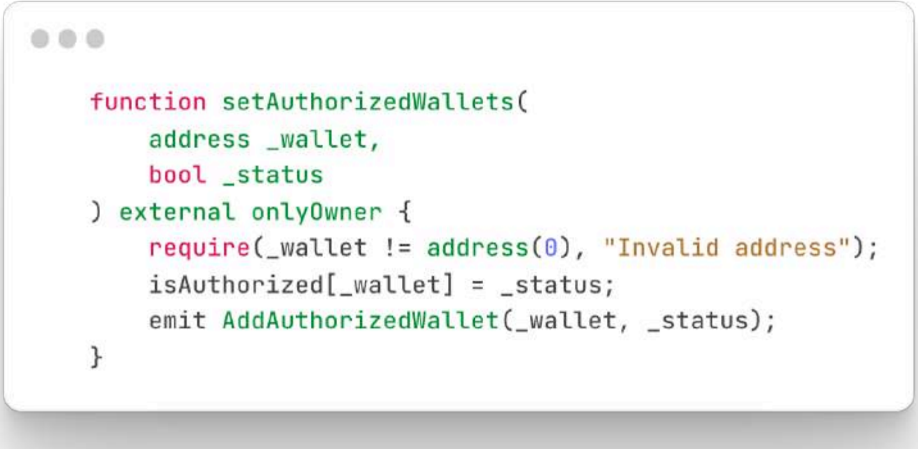
```
function changeSellFees(
    uint256 _sellTreasuryFee,
    uint256 _sellMarketingFee
) external onlyOwner {
    sellTreasuryFee = _sellTreasuryFee;
    sellMarketingFee = _sellMarketingFee;

    sellTotalFee = _sellTreasuryFee + _sellMarketingFee;

    require(sellTotalFee <= 10, "Cannot be greater than 10%");
}

function changeBuyFees(
    uint256 _buyTreasuryFee,
    uint256 _buyMarketingFee
) external onlyOwner {
    buyTreasuryFee = _buyTreasuryFee;
    buyMarketingFee = _buyMarketingFee;
    buyTotalFee = _buyTreasuryFee + _buyMarketingFee;

    require(buyTotalFee <= 10, "Cannot be greater than 10%");
}
```

- Owner can enable trading,once enabled can not disable again



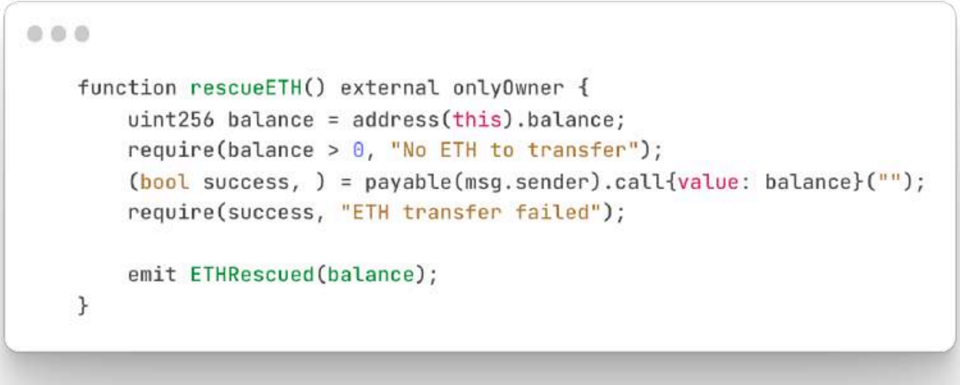
```
function enableTrading() external onlyOwner {
    require(!isTradeEnabled, "Trading already enabled");
    isTradeEnabled = true;
    launchedAt = block.timestamp;
}
```

- ❖ Owner can add/remove authorized wallets



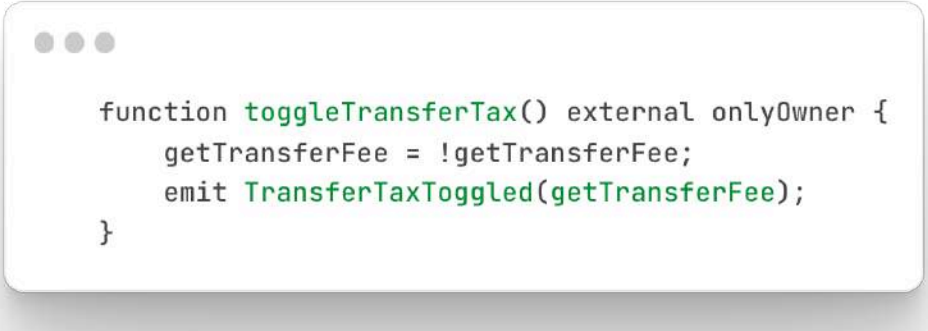
```
function setAuthorizedWallets(
    address _wallet,
    bool _status
) external onlyOwner {
    require(_wallet != address(0), "Invalid address");
    isAuthorized[_wallet] = _status;
    emit AddAuthorizedWallet(_wallet, _status);
}
```

- ❖ Owner can get ETH from the contract



```
function rescueETH() external onlyOwner {
    uint256 balance = address(this).balance;
    require(balance > 0, "No ETH to transfer");
    (bool success, ) = payable(msg.sender).call{value: balance}("");
    require(success, "ETH transfer failed");

    emit ETHRescued(balance);
}
```

- ❖ Owner can enable/disable getting tax on transfers



```
function toggleTransferTax() external onlyOwner {
    getTransferFee = !getTransferFee;
    emit TransferTaxToggled(getTransferFee);
}
```

# Audit conclusion

RugFreeCoins team has performed in-depth testing, 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 |
| Smart contract security Status: | HIGH ISSUES |
| Number of risk issues: | 01 |
| Solidity code functional issue level: | PASS |
| Number of owner privileges: | 08 |
| Centralization risk correlated to the active owner: | HIGH |
| Smart contract active ownership: | ACTIVE |