



# **Smart Contract Security Audit**

TechRate
June, 2021

## **Audit Details**



**Audited project** 

BoxerInu



Deployer address

0xC87F065B7710a277Fc02689033EB6FBcd6c320A3



**Client contacts:** 

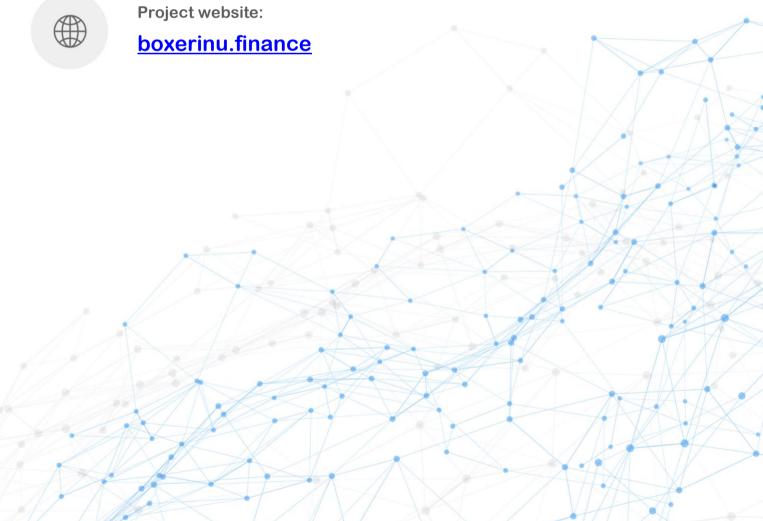
BoxerInu team



Blockchain

**Binance Smart Chain** 





## **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 below 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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**

TechRate was commissioned by BoxerInu to perform an audit of smart contracts:

https://bscscan.com/address/0xe96051a0d033b9aa57bac2cc6907af6897426154#code

#### The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

110100101001000

10111010001100000001111101100101011011

100001000110101

011001000100000

101000001

1.0

0 0 0

10001101110110011011

10001010010001100

THE RESERVE THE RESERVE THE RESERVE THE RESERVE

## **Contracts Details**

#### Token contract details for 14.06.2021

Contract name  BoxerInu  Contract address  0xE96051A0D033B9Aa57BaC2cc6907af6893  Total supply  1,000,000,000,000,000			
Total supply 1,000,000,000,000	0xE96051A0D033B9Aa57BaC2cc6907af6897426154		
	1,000,000,000,000		
Token ticker BOXER			
Decimals 9			
Token holders 1			
Transactions count 1			
Top 100 holders dominance 100.00%			
Liquidity fee 0			
Tax fee 0			
Total fees 0			
Uniswap V2 pair 0x002761bda4f7f1be46e13fa585da9475fbef0	0c41		
Contract deployer address 0xC87F065B7710a277Fc02689033EB6FBcd	6c320A3		
Contract's current owner address 0xc87f065b7710a277fc02689033eb6fbcd6c3	320a3		

### **Contract functions details**

#### + [Int] IERC20 - [Ext] totalSupply - [Ext] balanceOf - [Ext] transfer # - [Ext] allowance - [Ext] approve # - [Ext] transferFrom # + [Lib] SafeMath - [Int] add - [Int] sub - [Int] sub - [Int] mul - [Int] div - [Int] div - [Int] mod - [Int] mod + Context - [Int] \_msgSender - [Int] \_msgData + [Lib] Address - [Int] isContract - [Int] sendValue # - [Int] functionCall # - [Int] functionCall # - [Int] functionCallWithValue # - [Int] functionCallWithValue # - [Prv] functionCallWithValue # + Ownable (Context) - [Int] <Constructor> # - [Pub] owner - [Pub] renounceOwnership # - modifiers: onlyOwner - [Pub] transferOwnership # - modifiers: onlyOwner - [Pub] geUnlockTime - [Pub] lock # - modifiers: onlyOwner - [Pub] unlock # + [Int] IUniswapV2Factory - [Ext] feeTo - [Ext] feeToSetter - [Ext] getPair

- [Ext] allPairs

- [Ext] allPairsLength
- [Ext] createPair#
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

#### + [Int] IUniswapV2Pair

- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] allowance
- [Ext] approve #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] DOMAIN SEPARATOR
- [Ext] PERMIT\_TYPEHASH
- [Ext] nonces
- [Ext] permit #
- [Ext] MINIMUM\_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint #
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

#### + [Int] IUniswapV2Router01

- [Ext] factory
- [Ext] WETH
- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] removeLiquidity #
- [Ext] removeLiquidityETH #
- [Ext] removeLiquidityWithPermit #
- [Ext] removeLiquidityETHWithPermit #
- [Ext] swapExactTokensForTokens #
- [Ext] swapTokensForExactTokens #
- [Ext] swapExactETHForTokens (\$)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens (\$)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

```
+ [Int] | UniswapV2Router02 (|UniswapV2Router01)
 - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
 - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
 - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
+ BoxerInu (Context, IERC20, Ownable)
 - [Pub] <Constructor> #
 - [Pub] name
 - [Pub] symbol
 - [Pub] decimals
 - [Pub] totalSupply
 - [Pub] balanceOf
 - [Pub] transfer #
 - [Pub] allowance
 - [Pub] approve #
 - [Pub] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Pub] isExcludedFromReward
 - [Pub] totalFees
 - [Pub] totalBurn
 - [Pub] deliver #
 - [Pub] reflectionFromToken
 - [Pub] tokenFromReflection
 - [Pub] excludeFromReward #
  - modifiers: onlyOwner
 - [Ext] includeInReward #
  - modifiers: onlyOwner
 - [Ext] <Fallback> ($)
 - [Prv] _distributeFee #
 - [Prv] _getValues
 - [Prv] getTValues
 - [Prv] getRValues
 - [Prv] _getRate
 - [Prv] _getCurrentSupply
 - [Prv] takeLiquidity#
 - [Prv] calculateTaxFee
 - [Prv] calculateBurnFee
 - [Prv] calculateCharityFee
 - [Prv] calculateLiquidityFee
 - [Prv] removeAllFee #
 - [Prv] restoreAllFee #
 - [Pub] is Excluded From Fee
 - [Prv] _approve #
 - [Prv] _transfer #
 - [Prv] swapAndLiquify #
   - modifiers: lockTheSwap
 - [Prv] swapTokensForEth #
 - [Prv] addLiquidity #
 - [Prv] _tokenTransfer #
 - [Prv] _transferStandard #
 - [Prv] _transferToExcluded #
```

- [Prv] \_transferFromExcluded #

- [Prv] \_transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] enableAllFees #
  - modifiers: onlyOwner
- [Ext] disableAllFees #
  - modifiers: onlyOwner
- [Ext] setBoxerCharityWallet#
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled#
  - modifiers: onlyOwner
- (\$) = payable function
- # = non-constant function

# **Issues Checking Status**

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

### **Security Issues**

High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

# Owner privileges (In the period when the owner is not renounced)

Owner can disable and enable the fees.

```
function enableAllFees() external onlyOwner() {
    _{\mathsf{taxFee}} = 4;
    _previousTaxFee = _taxFee;
    burnFee = 1;
    _previousBurnFee = _taxFee;
    _charityFee = 2;
    _previousCharityFee = _charityFee;
    _liquidityFee = 3;
    _previousLiquidityFee = _liquidityFee;
    setSwapAndLiquifyEnabled(true);
}
ftrace | funcSig
function disableAllFees() external onlyOwner() {
    _taxFee = 0;
    _previousTaxFee = _taxFee;
    _burnFee = 0;
    _previousBurnFee = _taxFee;
    _charityFee = 0;
    _previousCharityFee = _charityFee;
    _liquidityFee = 0;
    _previousLiquidityFee = _liquidityFee;
    setSwapAndLiquifyEnabled(false);
```

• Owner can change the maximum transaction amount.

Owner can exclude from the fee.

```
function excludeFromFee(address account 1) public onlyOwner {
    _isExcludedFromFee[account 1] = true;
}
```

• Owner can change charity wallet.

```
function setBoxerCharityWallet(address newWallet1) external onlyOwner() {
   charityWallet = newWallet1;
}
```

Owner can enable and disable swapAndLiquify block.

```
function excludeFromFee(address account1) public onlyOwner {
         isExcludedFromFee[account1] = true;
}
```

 Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

```
//Locks the contract for owner for the amount of time provided
function lock(uint256 time) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = now + time;
    emit OwnershipTransferred(_owner, address(0));
}

//Unlocks the contract for owner when _lockTime is exceeds
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock");
    require(now > _lockTime , "Contract is locked until 7 days");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

### Conclusion

Smart contracts contain owner privileges! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

#### TechRate note:

Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.

