Smart Contract Security Audit V1

Insure Token Smart Contract Audit

May 25, 2023

https://saferico.com/

business@saferico.com
https://t.me/SFI_ANN

Table of Contents

Background

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.

Project Information

- **Platform**: Ethereum
- **Contract Address**: 0xfeb426010cfad88e87a285af040028163201e227
- **Code Source**: https://goerli.etherscan.io/address/0xfeb426010cfad88e87a285af040028163201e227#code

Contracts address deployed to test net (ETH)

0xInsure Token smart contracts on ETH test-net by the auditor to test every function .

https://goerli.etherscan.io/address/0xfeb426010cfad88e87a285af040028163201e227

Token Information:

Name	0xInsure
Symbol	0xI
Total supply	1,000,000,000,000
Decimals	18
Router	0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D
Liquidity Fee	1%
Dev Fee	1%
Insurance Fee	3%
Max Wallet Limit	2%
Dev wallet	0x7617CAE48D5d4e77807A463f032F72Bec93542F4
Liquidity Wallet	0x07cade9ba13098e0B681c91F461e8fbFcEf952c0
Insurance Wallet	0x3311e02fF6c6C5f3A4d73372f23ca65Ab00D47ED

Executive Summary

According to our assessment, the customer`s solidity smart contract is **Well-Secured**.

Well Secured	✓
Secured	
Poor Secured	
Insecure	

Automated checks are with remix IDE. All issues were performed by the team, which included the analysis of code functionality, manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the Project Information section and all issues found are located in the audit overview section.

Team found 0 critical, 0 high, 0 medium, 3 low, 0 very low-level issues and 0 note in all solidity files of the contract

The files:

InsureToken.sol

File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
InsureToken.sol	**c2064ce27008cc32c829e92a64bfe74f16642e81**	0xfeb426010cfad88e87a285af040028163201e227

- Contract: InsureToken
- Inherit: ERC20, Ownable
- Observation: All passed including security check
- Test Report: passed
- Score: passed
- Conclusion: passed

Function	Test Result	Type / Return Type	Score
name	✓	Read / public	**Passed**
symbol	✓	Read / public	**Passed**
decimals	✓	Read / public	**Passed**
totalSupply	✓	Read / public	**Passed**
allowance	✓	Read / public	**Passed**
balanceOf	✓	Read / public	**Passed**
decimals	✓	Read / public	**Passed**
insuranceFee	✓	Read / public	**Passed**
insuranceWallet	✓	Read / public	**Passed**
devWallet	✓	Read / public	**Passed**
devFee	✓	Read / public	**Passed**
liquidityWallet	✓	Read / public	**Passed**

liquidityFee	✓	Read / public	**Passed**
isExcluded	✓	Read / public	**Passed**
isTradingEnabled	✓	Read / public	**Passed**
limit	✓	Read / public	**Passed**
maxWalletLimit	✓	Read / public	**Passed**
transferFrom	✓	Write / public	**Passed**
transfer	✓	Write / public	**Passed**
transferOwnership	✓	Write / public	**Passed**
decreaseAllowance	✓	Write / public	**Passed**
increaseAllowance	✓	Write /public	**Passed**
renounceOwnership	✓	Write / public	**Passed**
approve	✓	Write / public	**Passed**
burn	✓	Write / public	**Passed**
claimStuckedTokens	✓	Write / public	**Passed**
enableTrading	✓	Write / public	**Passed**
excludeFromFee	✓	Write / public	**Passed**
includeInFee	✓	Write / public	**Passed**
removeMaxWalletLimit	✓	Write / public	**Passed**
updateMaxWalletPercent	✓	Write / public	**Passed**
setFeeWallets	✓	Write / public	**Passed**
setFees	✓	Write / public	**Passed**

Issues Checking Status

No.	Issue Description	Checking Status
1	Compiler warnings.	**Passed**
2	Race conditions and Reentrancy. Cross-function race conditions.	**Passed**
3	Possible delays in data delivery.	**Passed**
4	Oracle calls.	**Passed**
5	Design Logic.	**Passed**
6	Timestamp dependence.	**Passed with notes**
7	Integer Overflow and Underflow.	**Passed**
8	DoS with Revert.	**Passed**
9	DoS with block gas limit.	**Passed with notes**
10	Methods execution permissions.	**Passed**
11	Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc.	**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**

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can’t lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can’t have significant impact on execution
Note	Lowest-level vulnerabilities, code style violations and info statements can’t affect smart contract execution and can be ignored.

Audit Findings

Critical:

No Critical severity vulnerabilities were found.

High:

No High severity vulnerabilities were found.

Medium:

No Medium severity vulnerabilities were found.

Low:

#Missing Read functions

Description

In every smart contract has read and write functions, the read allows the users to read the info in the smart contract if they aren't developers, in this smart contract has 3 functions need to be public to allow users to see it and read it like router address, pair address, and factory address.

```
IUniswapV2Router02 private uniswapV2Router02;
IUniswapV2Factory private uniswapV2Factory;
address private uniswapV2Pair;
```

Remediation

Change the 3 functions from private to public to be able to read it and see it.

Status: Acknowledged

#Use of block.timestamp for comparisons

Description
The value of block.timestamp can be manipulated by the miner. And conditions with strict equality is difficult to achieve - block.timestamp.

Remediation
Avoid use of block.timestamp

Status: Acknowledged.

#Owner privileges (In the period when the owner isn't renounced)

Description

The owner can exclude / include any address from / in fees.
The owner can change the fees contract to the max = 10%.
The owner can change the max wallet percent of holding the tokens.

```
function excludeFromFee(address account) external onlyOwner {
        require(!isExcluded(account), "0xI: Account is already excluded");
        excludeList[account] = true;
    }
    function includeInFee(address account) external onlyOwner {
        require(isExcluded(account),"0XI: Account is not excluded");
        excludeList[account] = false;
    }
    function setFees(uint256 dev, uint256 insurance, uint256 liquidity) external
onlyOwner {
        devFee = dev;
        insuranceFee = insurance;
        liquidityFee = liquidity;
        require (devFee + insuranceFee + liquidityFee <= 10, "max fees is 10
percent");
    }
function updateMaxWalletPercent (uint256 newPercent) external onlyOwner {
        require (newPercent >= 1, "maxWallet limit can't go below 1 percent of the
supply");
        maxWalletLimit = (newPercent * totalSupply()) / 100;
    }
```

Remediation

Make these functions internal in next version or the team should announce the investors before doing anything to give them time if they want to do anything.

P.S: This issue is common to the majority of those smart contracts.

Status: Acknowledged.

Very Low:

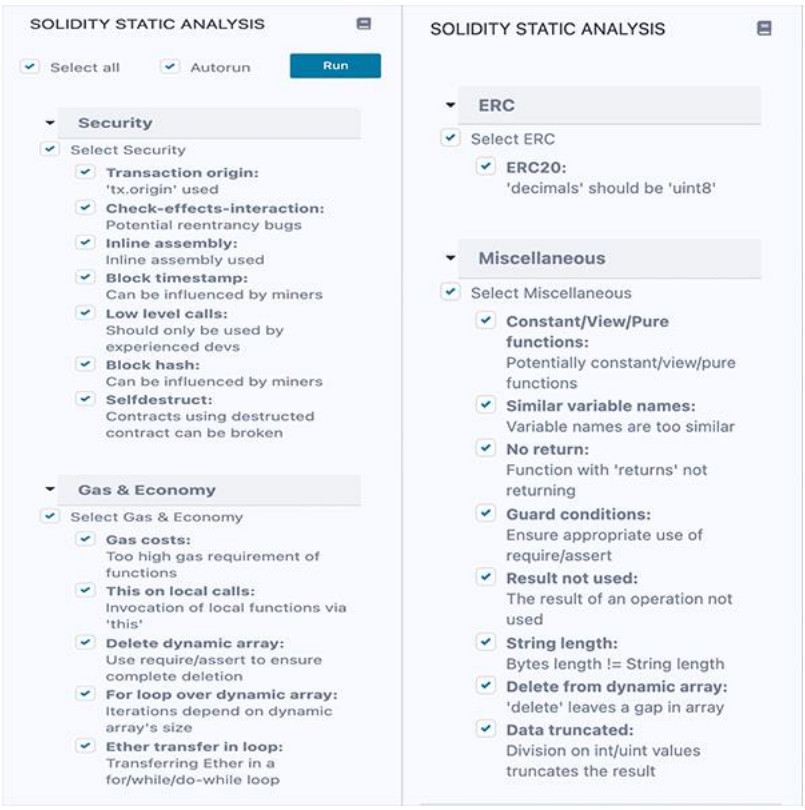
No Very Low severity vulnerabilities were found.

Notes:

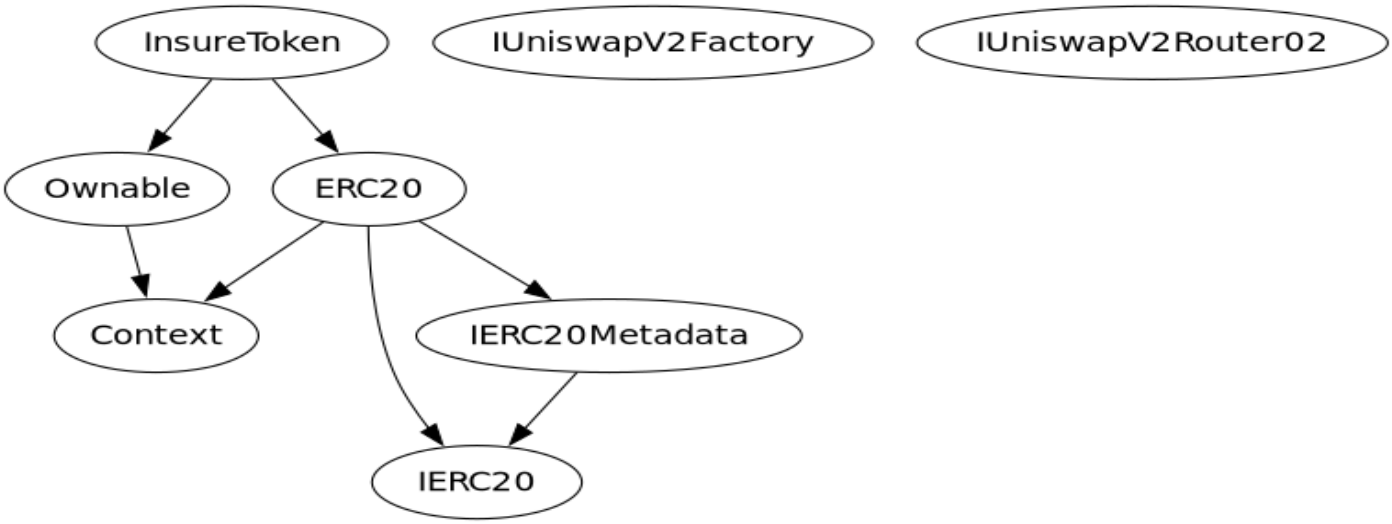
No notes were found.

Automatic Testing

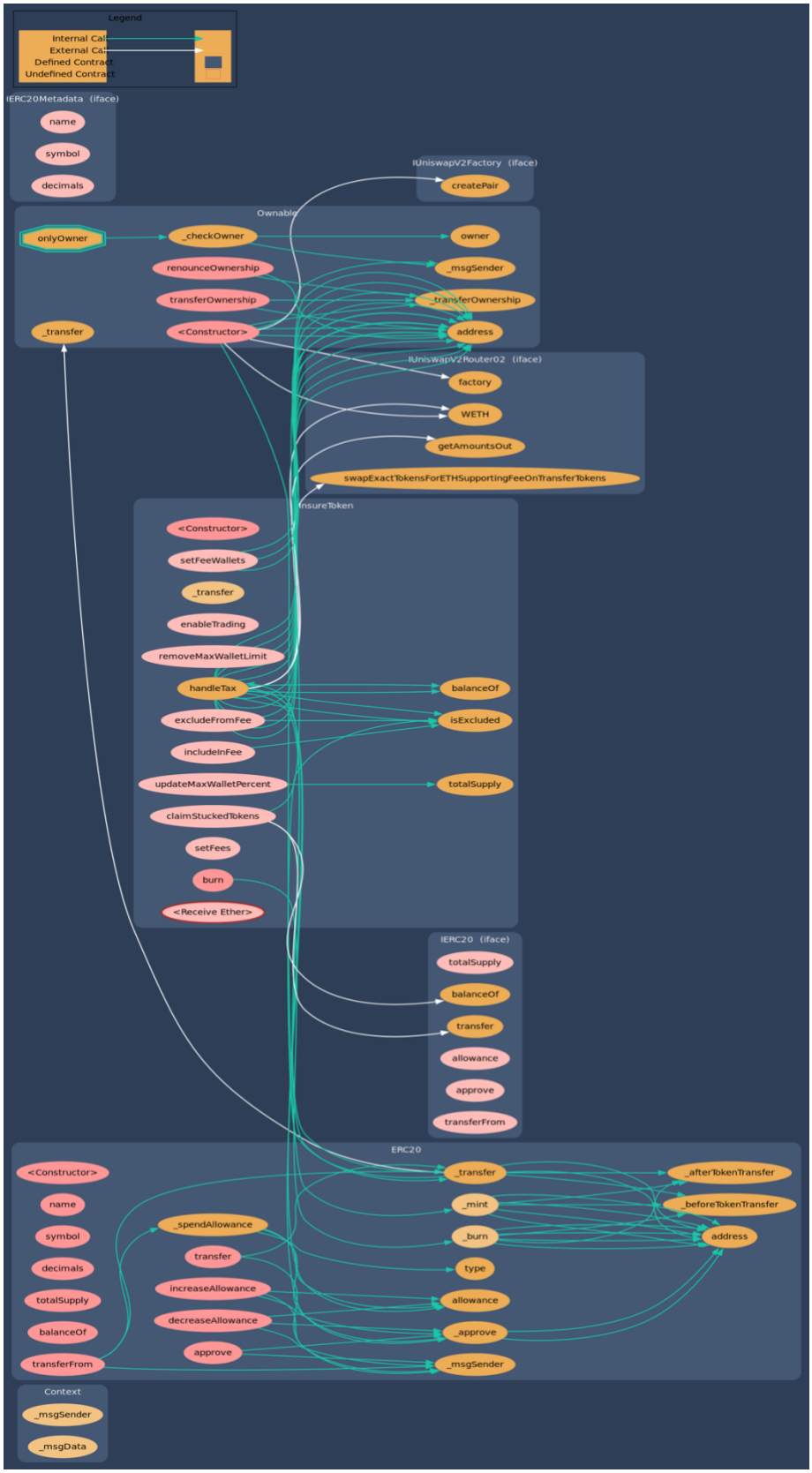
1- SOLIDITY STATIC ANALYSIS



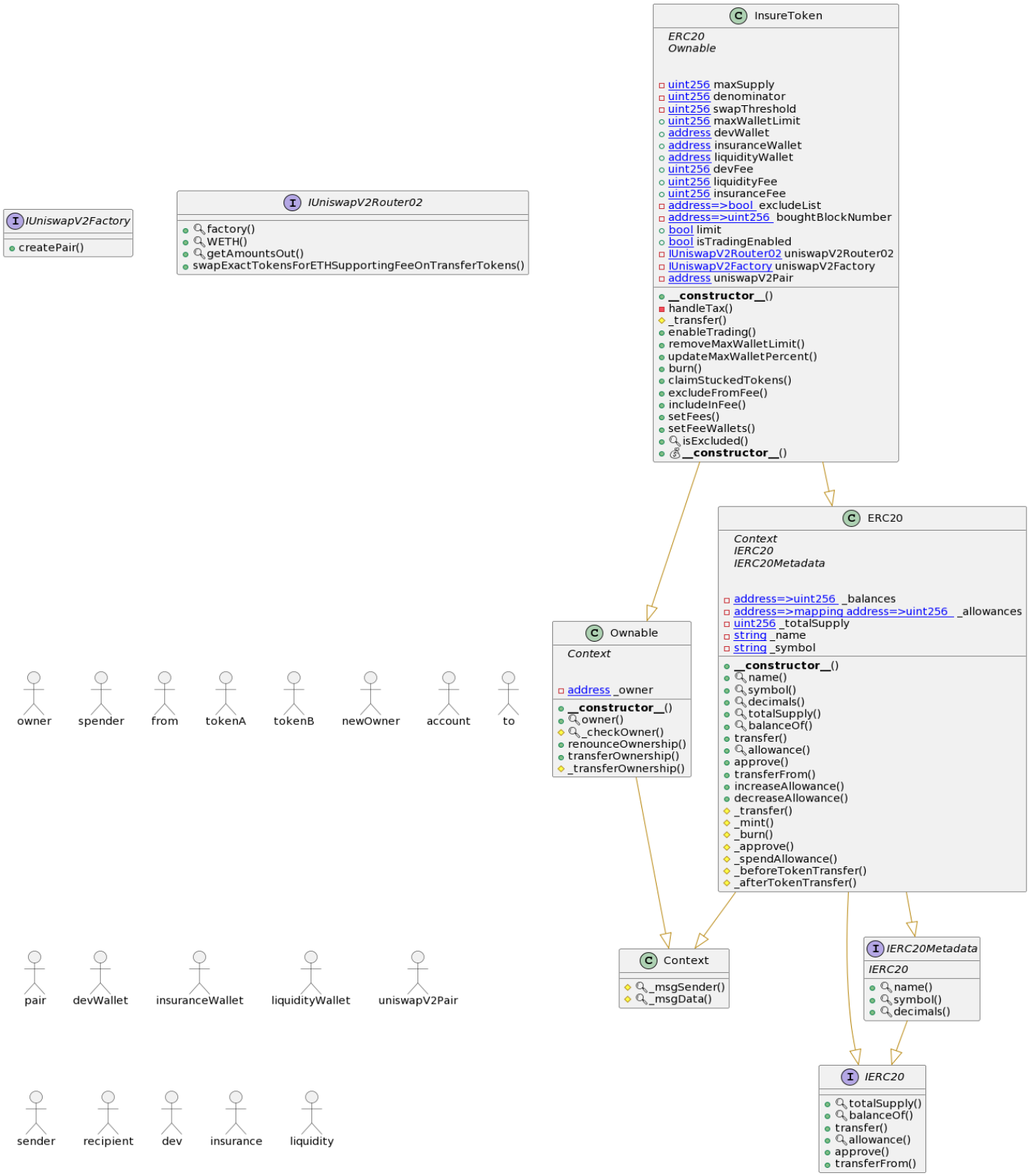
2- Inheritance graph



3- Call graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IERC20Metadata (iface)
name
symbol
decimals
IUniswapV2Factory (iface)
createPair
Ownable
onlyOwner
_checkOwner
owner
renounceOwnership
_msgSender
transferOwnership
_transferOwnership
_transfer
<Constructor>
address
IUniswapV2Router02 (iface)
factory
WETH
getAmountsOut
swapExactTokensForETHSupportingFeeOnTransferTokens
InsureToken
<Constructor>
setFeeWallets
_transfer
enableTrading
removeMaxWalletLimit
handleTax
balanceOf
excludeFromFee
isExcluded
includeInFee
updateMaxWalletPercent
totalSupply
claimStuckedTokens
setFees
burn
<Receive Ether>
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
_spendAllowance
transfer
increaseAllowance
decreaseAllowance
approve
_transfer
_mint
_burn
type
allowance
_approve
_msgSender
_afterTokenTransfer
_beforeTokenTransfer
address
Context
_msgSender
_msgData

Unified Modeling Language (UML)



Functions signature

```
Sighash   |   Function Signature
========================
39509351  =>  increaseAllowance(address,uint256)
119df25f  =>  _msgSender()
8b49d47e  =>  _msgData()
8da5cb5b  =>  owner()
53a72975  =>  _checkOwner()
715018a6  =>  renounceOwnership()
f2fde38b  =>  transferOwnership(address)
d29d44ee  =>  _transferOwnership(address)
18160ddd  =>  totalSupply()
70a08231  =>  balanceOf(address)
a9059cbb  =>  transfer(address,uint256)
dd62ed3e  =>  allowance(address,address)
095ea7b3  =>  approve(address,uint256)
23b872dd  =>  transferFrom(address,address,uint256)
06fdde03  =>  name()
95d89b41  =>  symbol()
313ce567  =>  decimals()
a457c2d7  =>  decreaseAllowance(address,uint256)
30e0789e  =>  _transfer(address,address,uint256)
4e6ec247  =>  _mint(address,uint256)
6161eb18  =>  _burn(address,uint256)
104e81ff  =>  _approve(address,address,uint256)
1532335e  =>  _spendAllowance(address,address,uint256)
cad3be83  =>  _beforeTokenTransfer(address,address,uint256)
8f811a1c  =>  _afterTokenTransfer(address,address,uint256)
c9c65396  =>  createPair(address,address)
c45a0155  =>  factory()
ad5c4648  =>  WETH()
d06ca61f  =>  getAmountsOut(uint256,address[])
791ac947  =>
swapExactTokensForETHSupportingFeeOnTransferTokens(uint256,uint256,address[],addres
s,uint256)
2dbc7632  =>  handleTax(address,address,uint256)
8a8c523c  =>  enableTrading()
98e3bc36  =>  removeMaxWalletLimit()
58068eaa  =>  updateMaxWalletPercent(uint256)
42966c68  =>  burn(uint256)
26f3819e  =>  claimStuckedTokens(IERC20)
437823ec  =>  excludeFromFee(address)
ea2f0b37  =>  includeInFee(address)
cec10c11  =>  setFees(uint256,uint256,uint256)
48d462b1  =>  setFeeWallets(address,address,address)
cba0e996  =>  isExcluded(address)
```

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/0xInsure.sol	c2064ce27008cc32c829e92a64bfe74f16642e81

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	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❗
IERC20Metadata	Interface	IERC20		
└	name	External ❗		NO❗
└	symbol	External ❗		NO❗
└	decimals	External ❗		NO❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<Constructor>	Public ❗	🛑	NO❗
└	name	Public ❗		NO❗
└	symbol	Public ❗		NO❗
└	decimals	Public ❗		NO❗
└	totalSupply	Public ❗		NO❗
└	balanceOf	Public ❗		NO❗
└	transfer	Public ❗	🛑	NO❗
└	allowance	Public ❗		NO❗
└	approve	Public ❗	🛑	NO❗
└	transferFrom	Public ❗	🛑	NO❗
└	increaseAllowance	Public ❗	🛑	NO❗
└	decreaseAllowance	Public ❗	🛑	NO❗

└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_spendAllowance	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
IUniswapV2Factory	Interface			
└	createPair	External ❗	🛑	NO❗
IUniswapV2Router02	Interface			
└	factory	External ❗		NO❗
└	WETH	External ❗		NO❗
└	getAmountsOut	External ❗		NO❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO❗
InsureToken	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	handleTax	Private 🔐	🛑	
└	_transfer	Internal 🔒	🛑	
└	enableTrading	External ❗	🛑	onlyOwner
└	removeMaxWalletLimit	External ❗	🛑	onlyOwner
└	updateMaxWalletPercent	External ❗	🛑	onlyOwner
└	burn	Public ❗	🛑	onlyOwner
└	claimStuckedTokens	External ❗	🛑	onlyOwner
└	excludeFromFee	External ❗	🛑	onlyOwner
└	includeInFee	External ❗	🛑	onlyOwner
└	setFees	External ❗	🛑	onlyOwner
└	setFeeWallets	External ❗	🛑	onlyOwner
└	isExcluded	Public ❗		NO❗
└	<Receive Ether>	External ❗	💸	NO❗

Legend

Symbol	Meaning
🛑	Function can modify state
💸	Function is payable

Conclusion

The contracts are written systematically. Team found no critical issues. So, it is good to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such an extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan Everything.

Security state of the reviewed contract is “Well Secured”.

✓ No volatile code.
✓ No high severity issues were found.

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of 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 the team on the basis of what it says or doesn't say, or how team produced it, and it is important for you to conduct your own independent investigations before making any decisions. team go into more detail on this in the below disclaimer below – please make sure to read it in full.

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