

Smart Contract Security Audit V1

Raju Token Smart Contract

27/9/2022



<https://saferico.com/>

business@saferico.com

https://t.me/SFI_ANN

—

Table of Contents

Table of Contents

Background

Project Information

Token Information

Executive Summary

File and Function Level Report

File in Scope:

Issues Checking Status

Severity Definitions

Audit Findings

Automatic testing

Testing proves

Inheritance graph

Call graph

Unified Modeling Language (UML)

Functions signature

Automatic general report

Conclusion

Disclaimer

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:** Polygon
- **Contract Address:** 0x171bef122830a763359df58291ade30db33a63dc
- **Code Source:**

<https://github.com/Saferico/Smart-Contracts-for-Projects/tree/main/%20Raju%20contracts/Raju>

Token Information

- Name: Raju
- Initial Supply: 100,000 – Max Supply: 1,000,000,000

Contracts address deployed to test net (Polygon)

Raju Token smart contracts on Polygon test-net by the auditor to test every function (Polygon Test Net)

<https://mumbai.polygonscan.com/address/0x171bef122830a763359df58291ade30db33a63dc>

<https://mumbai.polygonscan.com/address/0xd18c3d7959053669bc5f887041462f8375f3f9d9>

<https://mumbai.polygonscan.com/address/0x3c934a2e461b7e61871556540f5df5dd7aa0a475>

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, 1 high, 0 medium, 2 low, 0 very low-level issues and 1 note in all solidity files of the contract

The files:

RajuToken.sol

File and Function Level Report

File in Scope:

Contract Name	SHA 256 hash	Contract Address
RajuToken.sol	71029263929d3b2174924c7a71e88af408c0834b1b7e610ae3a87724d09baa75	0x171bef122830a763359df58291ade30db33a63dc

- Contract: RajuToken
- Inherit: Initializable
- 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
_owner	✓	Read / public	Passed
autoRebase	✓	Read / public	Passed
blackHoleFee	✓	Read / public	Passed
blackHole	✓	Read / public	Passed
blacklisted	✓	Read / public	Passed
buySellTimer	✓	Read / public	Passed

impactLimit	✓	Read / public	Passed
uniswapV2Pair	✓	Read / public	Passed
uniswapV2Router	✓	Read / public	Passed
treasuryFee	✓	Read / public	Passed
treasury	✓	Read / public	Passed
stabilizer	✓	Read / public	Passed
stabilizerFee	✓	Read / public	Passed
presaleContract	✓	Read / public	Passed
phaseStartTimes	✓	Read / public	Passed
phaseRebaseRates	✓	Read / public	Passed
frag	✓	Read / public	Passed
isDualRebase	✓	Read / public	Passed
lastLiqTime	✓	Read / public	Passed
lifeSupports	✓	Read / public	Passed
liquifierFee	✓	Read / public	Passed
liquifier	✓	Read / public	Passed
nextRebase	✓	Read / public	Passed
P2PFee	✓	Read / public	Passed
phasePeriods	✓	Read / public	Passed
approve	✓	Write / public	Passed
transferFrom	✓	Write / public	Passed
transfer	✓	Write / public	Passed
initialize	✓	Write / public	Passed
manualRebase	✓	Write / public	Passed
runInit	✓	Write /public	Passed
setAutoRebase	✓	Write / public	Passed
setBotBlacklists	✓	Write / public	Passed
setImpactLimit	✓	Write / public	Passed
setLifeSupports	✓	Write / public	Passed

setPhaseSetting	✓	Write / public	Passed
setPresale	✓	Write / public	Passed
toggleDualRebase	✓	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:

#Any one can use initialize function

Description

the smart contract inherits Initializable, which has its own risk, the initialize function any address can control it before the team runs the run init function which allows the other to Corrupt the smart contract because they will be the owner of the smart contract before run the run init function.

You can check here the auditor add the owner address to the blacklist which and corrupt the smart contract.

<https://mumbai.polygonscan.com/address/0x3c934a2e461b7e61871556540f5df5dd7aa0a475>

Remediation

Redesign the initialize function to make it on one can control it only the team.

Status: **Closed**. Fixed in version 2.

Medium:

No Medium severity vulnerabilities were found.

Low:

#Pragam version not fixed

Description

It is a good practice to lock the solidity version for a live deployment (use 0.8.16 instead of $\geq 0.8.2$). contracts should be deployed with the same compiler version and flags that they have been tested the most with. Locking the pragma helps ensure that contracts do not accidentally get deployed using, for example, the latest compiler which may have higher risks of undiscovered bugs. Contracts may also be deployed by others and the pragma indicates the compiler version intended by the original authors.

Remediation

Remove the ^ sign to lock the pragma version.

Status: **Closed**. Fixed in version 2.

#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**

Very Low:

No Very Low severity vulnerabilities were found.

Notes:

#Naming Conventions

Description

The contract follows a consistent naming convention where we are private variables with leading "_" and public variables without it. But we have missed to comply to the condition for certain variable names "__owner" which is public.

Remediation

Remove "_" from external variable names and add it to private variable names.

Status: **Closed**. Fixed in version 2.

Automatic Testing

1- Check for security

71029263929d3b2174924c7a71e88af408c0834b1b7e610ae3a87724d09baa...

File: RajuTok... | Language: solidity | Size: 24315 bytes | Date: 2022-09-25T11:22:49.102Z

Critical	High	Medium	Low	Note
0	0	0	0	0

✓

2- SOLIDITY STATIC ANALYSIS

SOLIDITY STATIC ANALYSIS

☒ Select all ☒ Autorun Run

▼ Security

☒ Select Security

- ☒ **Transaction origin:**
'tx.origin' used
- ☒ **Check-effects-interaction:**
Potential reentrancy bugs
- ☒ **Inline assembly:**
Inline assembly used
- ☒ **Block timestamp:**
Can be influenced by miners
- ☒ **Low level calls:**
Should only be used by experienced devs
- ☒ **Block hash:**
Can be influenced by miners
- ☒ **Selfdestruct:**
Contracts using destructed contract can be broken

▼ Gas & Economy

☒ Select Gas & Economy

- ☒ **Gas costs:**
Too high gas requirement of functions
- ☒ **This on local calls:**
Invocation of local functions via 'this'
- ☒ **Delete dynamic array:**
Use require/assert to ensure complete deletion
- ☒ **For loop over dynamic array:**
Iterations depend on dynamic array's size
- ☒ **Ether transfer in loop:**
Transferring Ether in a for/while/do-while loop

SOLIDITY STATIC ANALYSIS

▼ ERC

☒ Select ERC

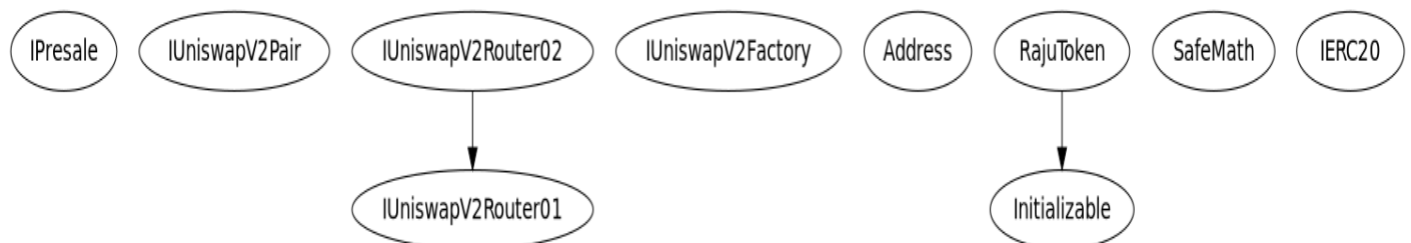
- ☒ **ERC20:**
'decimals' should be 'uint8'

▼ Miscellaneous

☒ Select Miscellaneous

- ☒ **Constant/View/Pure functions:**
Potentially constant/view/pure functions
- ☒ **Similar variable names:**
Variable names are too similar
- ☒ **No return:**
Function with 'returns' not returning
- ☒ **Guard conditions:**
Ensure appropriate use of require/assert
- ☒ **Result not used:**
The result of an operation not used
- ☒ **String length:**
Bytes length != String length
- ☒ **Delete from dynamic array:**
'delete' leaves a gap in array
- ☒ **Data truncated:**
Division on int/uint values truncates the result

3- Inheritance graph



4- SOLIDITY UNIT TESTING

SOLIDITY UNIT TESTING >

Test your smart contract in Solidity.

Select directory to load and generate test files.

Test directory:

☒ Select all

☒ tests/RajuToken_test.sol


Progress: 1 finished (of 1)

PASS


 testSuite

(tests/RajuToken_test.sol)


✓ Before all




✓ Check success




✓ Check success2



✓ Check failure



✓ Check sender and value



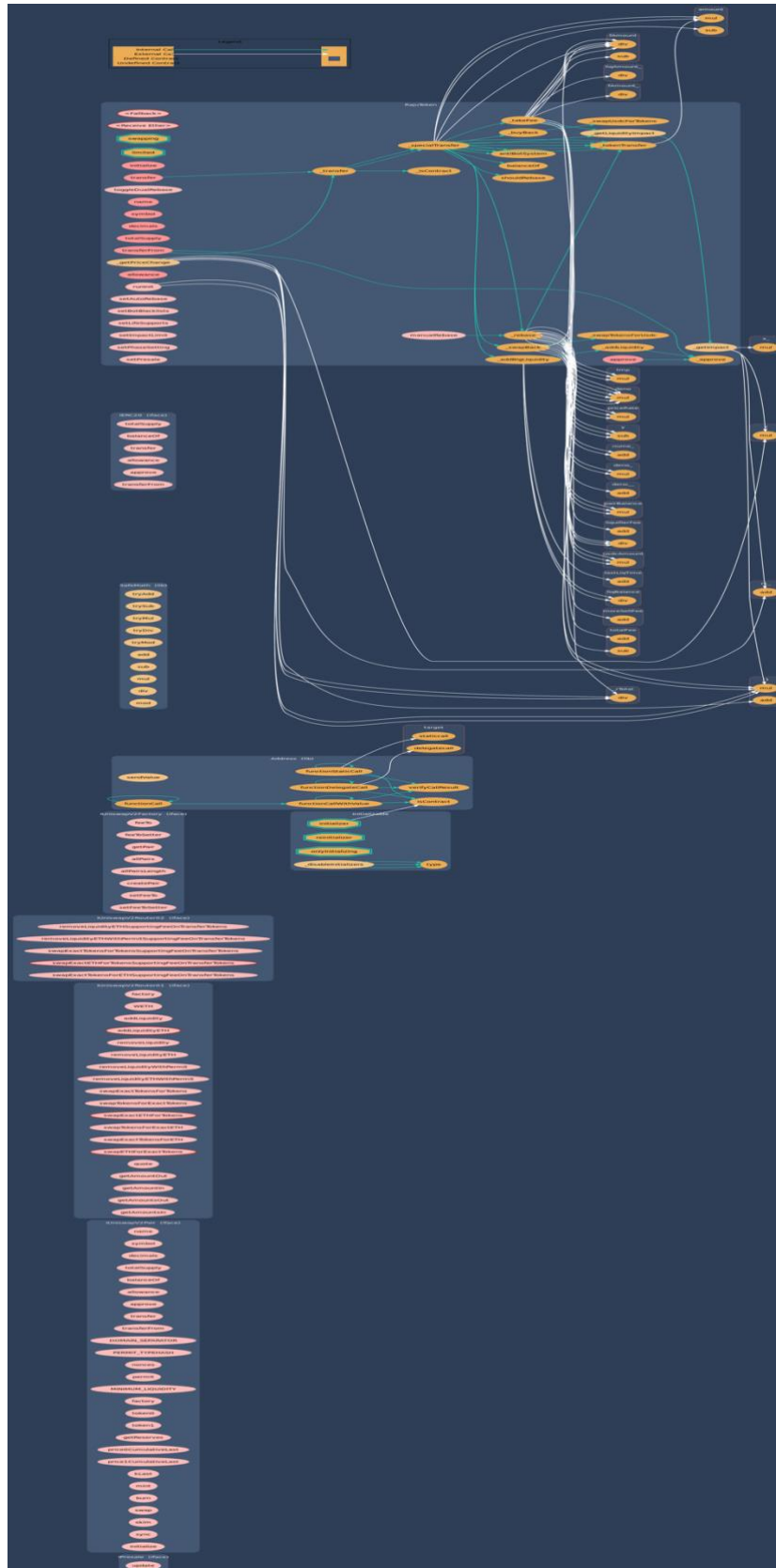
Result for tests/RajuToken_test.sol

Passed: 5

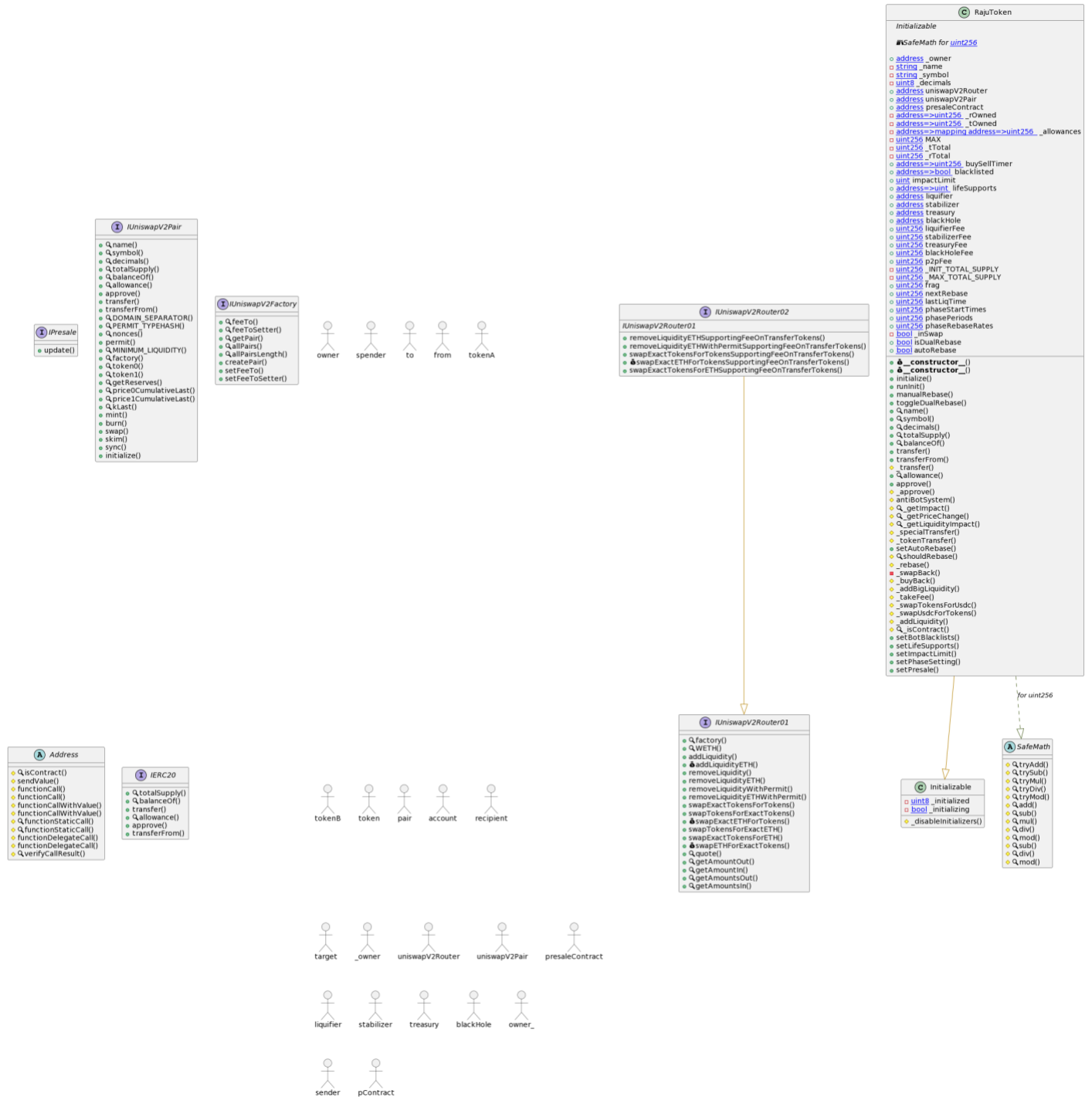
Failed: 0

Time Taken: 0.42s

5- Call graph



Unified Modeling Language (UML)



Functions signature

Sighash	Function Signature
=====	
16279055	=> isContract(address)
a2e62045	=> update()
06fdde03	=> name()
95d89b41	=> symbol()
313ce567	=> decimals()
18160ddd	=> totalSupply()
70a08231	=> balanceOf(address)
dd62ed3e	=> allowance(address,address)
095ea7b3	=> approve(address,uint256)
a9059cbb	=> transfer(address,uint256)
23b872dd	=> transferFrom(address,address,uint256)
3644e515	=> DOMAIN_SEPARATOR()
30adf81f	=> PERMIT_TYPEHASH()
7ecebe00	=> nonces(address)
d505accf	=> permit(address,address,uint256,uint256,uint8,bytes32,bytes32)
ba9a7a56	=> MINIMUM_LIQUIDITY()
c45a0155	=> factory()
0dfe1681	=> token0()
d21220a7	=> token1()
0902f1ac	=> getReserves()
5909c0d5	=> price0CumulativeLast()
5a3d5493	=> price1CumulativeLast()
7464fc3d	=> kLast()
6a627842	=> mint(address)
89afcb44	=> burn(address)
022c0d9f	=> swap(uint256,uint256,address,bytes)
bc25cf77	=> skim(address)
fff6cae9	=> sync()
485cc955	=> initialize(address,address)
ad5c4648	=> WETH()
e8e33700	=>
addLiquidity	(address,address,uint256,uint256,uint256,uint256,address,uint256)
f305d719	=> addLiquidityETH(address,uint256,uint256,uint256,address,uint256)
baa2abde	=>
removeLiquidity	(address,address,uint256,uint256,uint256,address,uint256)
02751cec	=> removeLiquidityETH(address,uint256,uint256,uint256,address,uint256)
2195995c	=>
removeLiquidityWithPermit	(address,address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes32,bytes32)
ded9382a	=>
removeLiquidityETHWithPermit	(address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes32,bytes32)
38ed1739	=> swapExactTokensForTokens(uint256,uint256,address[],address,uint256)
8803dbee	=> swapTokensForExactTokens(uint256,uint256,address[],address,uint256)
7ff36ab5	=> swapExactETHForTokens(uint256,address[],address,uint256)
4a25d94a	=> swapTokensForExactETH(uint256,uint256,address[],address,uint256)
18cbafe5	=> swapExactTokensForETH(uint256,uint256,address[],address,uint256)
fb3bdb41	=> swapETHForExactTokens(uint256,address[],address,uint256)
ad615dec	=> quote(uint256,uint256,uint256)
054d50d4	=> getAmountOut(uint256,uint256,uint256)
85f8c259	=> getAmountIn(uint256,uint256,uint256)
d06ca61f	=> getAmountsOut(uint256,address[])
1f00ca74	=> getAmountsIn(uint256,address[])
af2979eb	=>


```

removeLiquidityETHSupportingFeeOnTransferTokens (address,uint256,uint256,uint256,address,uint256)
5b0d5984 =>
removeLiquidityETHWithPermitSupportingFeeOnTransferTokens (address,uint256,uint256,uint256,address,uint256,bool,uint8,bytes32,bytes32)
5c11d795 =>
swapExactTokensForTokensSupportingFeeOnTransferTokens (uint256,uint256,address[],address,uint256)
b6f9de95 =>
swapExactETHForTokensSupportingFeeOnTransferTokens (uint256,address[],address,uint256)
791ac947 =>
swapExactTokensForETHSupportingFeeOnTransferTokens (uint256,uint256,address[],address,uint256)
017e7e58 => feeTo()
094b7415 => feeToSetter()
e6a43905 => getPair(address,address)
1e3dd18b => allPairs(uint256)
574f2ba3 => allPairsLength()
c9c65396 => createPair(address,address)
f46901ed => setFeeTo(address)
a2e74af6 => setFeeToSetter(address)
24a084df => sendValue(address,uint256)
a0b5ffb0 => functionCall(address,bytes)
241b5886 => functionCall(address,bytes,string)
2a011594 => functionCallWithValue(address,bytes,uint256)
d525ab8a => functionCallWithValue(address,bytes,uint256,string)
c21d36f3 => functionStaticCall(address,bytes)
dbc40fb9 => functionStaticCall(address,bytes,string)
ee33b7e2 => functionDelegateCall(address,bytes)
57387df0 => functionDelegateCall(address,bytes,string)
946b5793 => verifyCallResult(bool,bytes,string)
8129fc1c => initialize()
5cd8a76b => initializeV2()
4caf63ac => _disableInitializers()
884557bf => tryAdd(uint256,uint256)
a29962b1 => trySub(uint256,uint256)
6281efa4 => tryMul(uint256,uint256)
736ecb18 => tryDiv(uint256,uint256)
38dc0867 => tryMod(uint256,uint256)
771602f7 => add(uint256,uint256)
b67d77c5 => sub(uint256,uint256)
c8a4ac9c => mul(uint256,uint256)
a391c15b => div(uint256,uint256)
f43f523a => mod(uint256,uint256)
e31bdc0a => sub(uint256,uint256,string)
b745d336 => div(uint256,uint256,string)
71af23e8 => mod(uint256,uint256,string)
c4d66de8 => initialize(address)
a14e0e4e => runInit()
61a9d1b1 => manualRebase()
b952247c => toggleDualRebase()
30e0789e => _transfer(address,address,uint256)
104e81ff => _approve(address,address,uint256)
83eb049f => antiBotSystem(address)
73cec720 => _getImpact(uint256,uint256)
d68ea46c => _getPriceChange(uint256,uint256)
f16b9079 => _getLiquidityImpact(uint256,uint256)
1b90ddb9 => _specialTransfer(address,address,uint256)

```

```
f147aa74 => _tokenTransfer(address,address,uint256)
e15beb80 => setAutoRebase(bool)
63eab10a => shouldRebase()
edb65cb4 => _rebase()
065bcb0e => _swapBack(uint256)
56d5a40b => _buyBack(uint256)
b8a73b78 => _addBigLiquidity(uint256)
d7f793ab => _takeFee(address,address,uint256,uint256)
592b4fcb => _swapTokensForUsdc(uint256)
45166cdc => _swapUsdcForTokens(uint256,address)
9e8af2af => _addLiquidity(uint256,uint256)
7d48441f => _isContract(address)
091c2b42 => setBotBlacklists(address[],bool[])
dd109c43 => setLifeSupports(address[],uint256[])
f8785246 => setImpactLimit(uint256)
7e02899a => setPhaseSetting(uint256,uint256,uint256,uint256)
d5fcc7b6 => setPresale(address)
```

Automatic general report

Files Description Table

File Name	SHA-1 Hash
/Users/macbook/Desktop/smart contracts/RajuToken.sol	a0bec789428acbe6c4f62aeeb09248e85a069ad5

Contracts Description Table

Contract	Type	Bases	
L	**Function Name**	**Visibility**	**Mutability**
Modifiers			
IPresale	Interface		
L update	External !	⬤	NO!
IUniswapV2Pair	Interface		
L name	External !	NO!	
L symbol	External !	NO!	
L decimals	External !	NO!	
L totalSupply	External !	NO!	
L balanceOf	External !	NO!	
L allowance	External !	NO!	
L approve	External !	⬤	NO!
L transfer	External !	⬤	NO!
L transferFrom	External !	⬤	NO!
L DOMAIN_SEPARATOR	External !	NO!	
L PERMIT_TYPEHASH	External !	NO!	
L nonces	External !	NO!	
L permit	External !	⬤	NO!
L MINIMUM_LIQUIDITY	External !	NO!	
L factory	External !	NO!	
L token0	External !	NO!	
L token1	External !	NO!	
L getReserves	External !	NO!	
L price0CumulativeLast	External !	NO!	
L price1CumulativeLast	External !	NO!	
L kLast	External !	NO!	
L mint	External !	⬤	NO!
L burn	External !	⬤	NO!
L swap	External !	⬤	NO!
L skim	External !	⬤	NO!
L sync	External !	⬤	NO!
L initialize	External !	⬤	NO!
IUniswapV2Router01	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! |
| | | | |
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 | | |
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! |  | NO! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! |  | NO! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! |  | NO! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! |  | NO! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! |  | NO! |
| | | | |
| **IUniswapV2Factory** | 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! |
| | | | |
| **Address** | Library | | | |
| L | isContract | Internal  | | | |
| L | sendValue | Internal  |  | | | |
| L | functionCall | Internal  |  | | | |
| L | functionCall | Internal  |  | | | |
| L | functionCallWithValue | Internal  |  | | | |
| L | functionCallWithValue | Internal  |  | | | |
| L | functionStaticCall | Internal  | | | |
| L | functionStaticCall | Internal  | | | |
| L | functionDelegateCall | Internal  |  | | | |
| L | functionDelegateCall | Internal  |  | | | |
| L | verifyCallResult | Internal  | | | |
| | | | |
| **Initializable** | Implementation | | | |
| L | _disableInitializers | Internal  |  | | | |
| | | | |
| **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				
IERC20 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!	
RajuToken Implementation Initializable						
L	<Fallback>	External	!		NO!	
L	<Receive Ether>	External	!		NO!	
L	initialize	Public	!		initializer	
L	runInit	External	!		limited	
L	manualRebase	External	!		NO!	
L	toggleDualRebase	External	!		limited	
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	transferFrom	Public	!		NO!	
L	_transfer	Internal				
L	allowance	Public	!		NO!	
L	approve	Public	!		NO!	
L	_approve	Internal				
L	antiBotSystem	Internal				
L	_getImpact	Internal				
L	_getPriceChange	Internal				
L	_getLiquidityImpact	Internal				
L	_specialTransfer	Internal				
L	_tokenTransfer	Internal				
L	setAutoRebase	External	!		limited	
L	shouldRebase	Internal				
L	_rebase	Internal				
L	_swapBack	Private				
L	_buyBack	Internal				
L	_addBigLiquidity	Internal				
L	_takeFee	Internal				
L	_swapTokensForUsdc	Internal			swapping	
L	_swapUsdcForTokens	Internal			swapping	
L	_addLiquidity	Internal			swapping	
L	_isContract	Internal				
L	setBotBlacklists	External	!		limited	
L	setLifeSupports	External	!		limited	
L	setImpactLimit	External	!		limited	
L	setPhaseSetting	External	!		limited	
L	setPresale	External	!		limited	

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 mint function.
- ✓ 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.