June, 2021

Smart Contract Security Audit

Audit Details

Audited project

RichQuack

Deployer address

0x2Cb65436A0acBC46956c64E34cAE045CDBEA4b48

Client contacts:

RichQuack team

Blockchain

Binance Smart Chain

Project website:

https://www.RichQuack.com

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 RichQuack to perform an audit of smart contracts:
https://bscscan.com/address/0xd74b782e05aa25c50e7330af541d46e18f36661c#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.
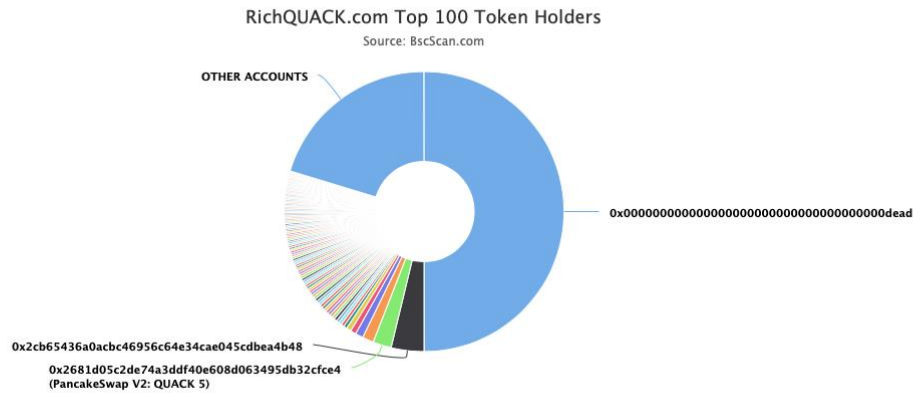
Contracts Details

Token contract details for 11.06.2021

Contract name	RichQuack
Contract address	0xD74b782E05AA25c50e7330Af541d46E18f36661C
Total supply	100,000,000,000,000,000
Token ticker	Quack
Decimals	9
Token holders	846
Transactions count	1,666
Top 100 holders dominance	79.69%
Liquidity fee	5
Tax fee	5
Total fees	1040505314565861252574011
Uniswap V2 pair	0x2681d05c2de74a3ddf40e608d063495db32cfce4
Contract deployer address	0x2Cb65436A0acBC46956c64E34cAE045CDBEA4b48
Contract's current owner address	0x2cb65436a0acbc46956c64e34cae045cdbea4b48

RichQuack Token Distribution

RichQUACK.com Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x0000000000000000000000000000000000000dead

0x2cb65436a0acbc46956c64e34cae045cdbea4b48

0x2681d05c2de74a3ddf40e608d063495db32cfce4
(PancakeSwap V2: QUACK 5)

(A total of 79,686,654,150,960,100.00 tokens held by the top 100 accounts from the total supply of 100,000,000,000,000,000.00 token)

RichQuack Contract Interaction Details

Time Series: Token Contract Overview   Wed 9, Jun 2021 - Wed 9, Jun 2021

Token Contract 0xd74b782e05aa25c50e7330af541d46e18f36661c (RichQUACK.com)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jun 8, 2021   To   Jun 9, 2021

● Transfer Amount   -●- Transfers Count   -+- Unique Receivers   -■- Unique Senders   -▲- Total Uniques

RichQuack Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000dead	50,000,000,000,000,000	50.0000%
2	0x2cb65436a0acbc46956c64e34cae045cdbea4b48	3,793,361,775,847,520.370786812	3.7934%
3	📄 PancakeSwap V2: QUACK 5	2,126,080,039,576,630.722117976	2.1261%
4	0x8bcc49d93007629991f278120bf79ac0f8a49de8	1,307,904,030,520,050.402135726	1.3079%
5	0xf83a28d52c1b8de089943e467b5c8b066a32bf3f	916,369,241,585,726.336868963	0.9164%
6	0xf43049009a86f44b0dd90cba9f6d8582cf26a0b0	637,051,743,050,154.005763038	0.6371%
7	0x1d2b6dfeca64194051a402d1ee6ba6ec8647e413	566,275,020,151,249.370507363	0.5663%
8	0x56363a815a8cb1b21bcdf8f0129c70689143df36	374,668,661,590,623.942992117	0.3747%
9	0x2090c7d3a59ae895ff64e737369da4b315817d96	353,571,984,211,269	0.3536%
10	0x64eacf35ce5fa9b7eb259cdb633803ceba1b7bb8	346,240,245,876,220	0.3462%

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]** IUniswapV2Router02 **(IUniswapV2Router01)**
  - **[Ext]** removeLiquidityETHSupportingFeeOnTransferTokens **#**
  - **[Ext]** removeLiquidityETHWithPermitSupportingFeeOnTransferTokens **#**

- **[Ext]** swapExactTokensForTokensSupportingFeeOnTransferTokens **#**
- **[Ext]** swapExactETHForTokensSupportingFeeOnTransferTokens **($)**
- **[Ext]** swapExactTokensForETHSupportingFeeOnTransferTokens **#**

+ RichQuackV2 **(Context, IERC20, Ownable)**
- **[Pub]** **<Constructor>** **#**
- **[Pub]** setRouterAddress **#**
  - modifiers: onlyOwner
- **[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]** deliver **#**
- **[Pub]** reflectionFromToken
- **[Pub]** tokenFromReflection
- **[Pub]** excludeFromReward **#**
  - modifiers: onlyOwner
- **[Ext]** includeInReward **#**
  - modifiers: onlyOwner
- **[Prv]** _transferBothExcluded **#**
- **[Pub]** excludeFromFee **#**
  - modifiers: onlyOwner
- **[Pub]** includeInFee **#**
  - modifiers: onlyOwner
- **[Ext]** setTaxFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setLiquidityFeePercent **#**
  - modifiers: onlyOwner
- **[Ext]** setMaxTxPercent **#**
  - modifiers: onlyOwner
- **[Pub]** setSwapAndLiquifyEnabled **#**
  - modifiers: onlyOwner
- **[Ext]** **<Fallback>** **($)**
- **[Prv]** _reflectFee **#**
- **[Prv]** _getValues
- **[Prv]** _getTValues
- **[Prv]** _getRValues
- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _takeLiquidity **#**
- **[Prv]** calculateTaxFee
- **[Prv]** calculateLiquidityFee
- **[Prv]** removeAllFee **#**
- **[Prv]** restoreAllFee **#**
- **[Pub]** isExcludedFromFee
- **[Prv]** _approve **#**

- **[Prv]** _transfer **#**
- **[Prv]** swapAndLiquify **#**
   - modifiers: lockTheSwap
- **[Prv]** swapTokensForEth **#**
- **[Prv]** addLiquidity **#**
- **[Prv]** _tokenTransfer **#**
- **[Prv]** _transferStandard **#**
- **[Prv]** _transferToExcluded **#**
- **[Prv]** _transferFromExcluded **#**

($) = 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 change the tax and liquidity fee.

```solidity
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {
    _taxFee = taxFee;
}

function setLiquidityFeePercent(uint256 liquidityFee) external onlyOwner() {
    _liquidityFee = liquidityFee;
}
```

- Owner can change the maximum transaction amount.

```solidity
function setMaxTxPercent(uint256 maxTxPercent) external onlyOwner() {
    _maxTxAmount = _tTotal.mul(maxTxPercent).div(
        10**2
    );
}
```

- Owner can exclude from the fee.

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

- Owner can change router address.

```solidity
function setRouterAddress(address newRouter) public onlyOwner() {
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(newRouter);
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    uniswapV2Router = _uniswapV2Router;
}
```

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

```solidity
//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 do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://team.finance/view-coin/0xD74b782E05AA25c50e7330Af541d46E18f36661C?name=RichQUACK.com&symbol=QUACK

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.