Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

March, 2022

Audit Details

Audited project

Wealth Protocol

Deployer address

0x77ef6c8e5ea1d6a5bf4d483f8b6687d92419011f

Client contacts:

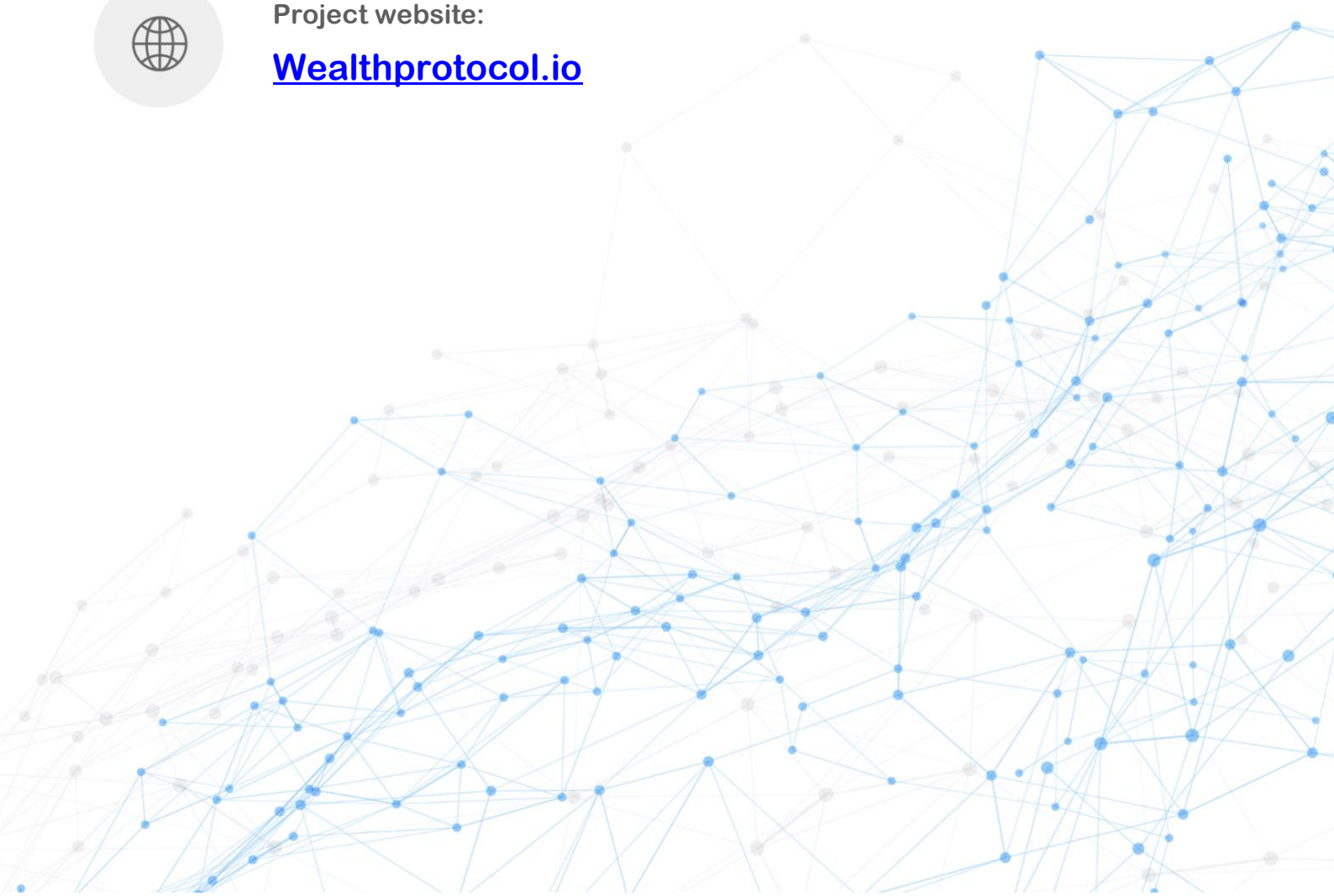
Wealth Protocol team

Blockchain

Binance Smart Chain

Project website:

Wealthprotocol.io



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 Wealth Protocol to perform an audit of smart contracts:

https://bscscan.com/address/0xB5DFCc4dE7456cF3eD67ab08F6310a0348C57850#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

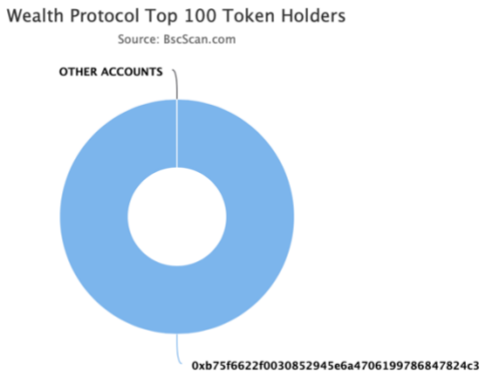
Token contract details for 03.03.2022

Contract name	Wealth Protocol
Contract address	0xB5DFCc4dE7456cF3eD67ab08F6310a0348C57850
Total supply	2,000,000,000,000
Token ticker	WEALTH
Decimals	9
Token holders	1
Transactions count	1
Top 100 holders dominance	100.00%
B/S Liquidity fee	3/3
B/S Reflection fee	0/0
B/S Marketing fee	6/6
Pancake V2 pair	0xbf0b2ec69d6741f24efbd6fe8aef566ea098dc84
Contract deployer address	0x77ef6c8e5ea1d6a5bf4d483f8b6687d92419011f
Contract's current owner address	0xb75f6622f0030852945e6a4706199786847824c3

Wealth Protocol Token Distribution

The top 100 holders collectively own 100.00% (2,000,000,000,000.00 Tokens) of Wealth Protocol

Token Total Supply: 2,000,000,000,000.00 Token | Total Token Holders: 1



(A total of 2,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 2,000,000,000,000.00 token)

Wealth Protocol Top 10 Token Holders

Rank	Address	Quantity (Token)	Percent
1.	0xb75f6622f0030852945e6a4706199786847824c3	2,000,000,000,000	100.0000%

Contract functions details

+ [Int] IPancakeRouter01
  - [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] IPancakeRouter02 (IPancakeRouter01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IPancakeFactory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Int] IPancakePair
  - [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 #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Int] verifyCallResult

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] approve #
  - [Ext] allowance

+ Ownable
  - [Int] _msgSender
  - [Int] _msgData

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
  - modifiers: onlyOwner
- [Pub] transferOwnership #
  - modifiers: onlyOwner

+ Wealth (IBEP20, Ownable)
- [Pub] <Constructor> #
- [Ext] <Fallback> ($)
- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] getOwner
- [Pub] numTokensSellToAddToLiquidityAmount
- [Pub] transfer #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #
- [Pub] getSellReflectionFee
- [Pub] getBuyReflectionFee
- [Pub] getSellLiquidityFee
- [Pub] getBuyLiquidityFee
- [Pub] getSellMarketingFee
- [Pub] getBuyMarketingFee
- [Pub] getSellBurnFee
- [Pub] getBuyBurnFee
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Pub] isExcludedFromFee
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Pub] isExcludedFromReward
- [Ext] setBuyTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setSellTaxFeePercent #
  - modifiers: onlyOwner
- [Ext] setBuyLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setSellLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setBuyMarketingFeePercent #
  - modifiers: onlyOwner
- [Ext] setSellMarketingFeePercent #
  - modifiers: onlyOwner
- [Ext] setBuyMaxTxAmount #
  - modifiers: onlyOwner

- [Ext] setSellMaxTxAmount #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] setNumTokensSellToAddToLiquidity #
  - modifiers: onlyOwner
- [Pub] transferTokens #
  - modifiers: onlyOwner
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Prv] _transfer #
- [Prv] _approve #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] calculateMarketingFee
- [Prv] calculateBurnFee
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForBNB #
- [Prv] transferOutBNB #
- [Prv] addLiquidity #
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _takeLiquidity #
- [Prv] _reflectFee #
- [Prv] _transferBurnFee #
- [Prv] initialTransfer #

($) = 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.	Low issues
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

1. Out of gas

Issue:

- The function `includeInReward()` uses the loop to find and remove addresses from the `_excluded` list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.
- The function `_getCurrentSupply` also uses the loop for evaluating total supply. It also could be aborted with `OUT_OF_GAS` exception if there will be a long excluded addresses list.

Recommendation:

Check that the excluded array length is not too big.

Notes:

- removeAllFee() function do not include _burnFee in to be zero checking.
- Do not exclude burn address from the reward, as burn fee is taking without checking address to be excluded from the reward.
- There is sending tokens to dead address instead of real burn (decreasing total supply).

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

- Owner can exclude from the fee.
- Owner can change the tax, marketing and liquidity fees.
- Owner can change the maximum transaction amounts.
- Owner can change numTokensSellToAddToLiquidity.
- Owner can call transferTokens() function (won't work, because token address not set).

Conclusion

Smart contracts contain low severity issues! 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.