

TechRate
May, 2022



SMART CONTRACTS SECURITY AUDIT REPORT



Audit Details



Audited project

PlugPRO



Deployer address

0xa5735f50899b8ec23957893816c9345b130031ca



Client contacts:

PlugPRO team



Blockchain

Binance Smart Chain



Project website:

<http://Plugpro.me>

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 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 PlugPRO to perform an audit of smart contracts:

<https://bscscan.com/address/0x2407CEd3c9fA576275A8f2871D67673e5Dea08ad#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 06.05.2022

Contract name	PlugPRO
Contract address	0x2407CEd3c9fA576275A8f2871D67673e5Dea08ad
Total supply	50,000,000,000
Token ticker	\$PP
Decimals	9
Token holders	999
Transactions count	3,787
Top 100 holders dominance	77.49%
Wallet two	0x44caa136d110bc0bd552bffd175bc7298c23e024
Team wallet	0x57dd7ba2f9b051b85ede16570746991711d5af5e
Taxes	0/20/80/4/16/10
Total LP BNB	75499635207041004910
Contract deployer address	0xa5735f50899b8ec23957893816c9345b130031ca
Owner address	0xf864c446ae918499386d2c534eab5b195ae0b7

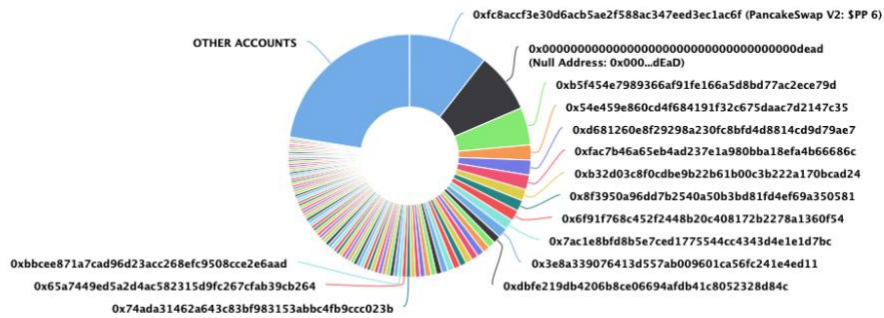
PlugPRO Token Distribution

The top 100 holders collectively own 77.49% (38,743,565,763.86 Tokens) of PlugPro

Token Total Supply: 50,000,000,000.00 Token | Total Token Holders: 999

PlugPro Top 100 Token Holders

Source: BscScan.com



(A total of 38,743,565,763.86 tokens held by the top 100 accounts from the total supply of 50,000,000,000.00 token)

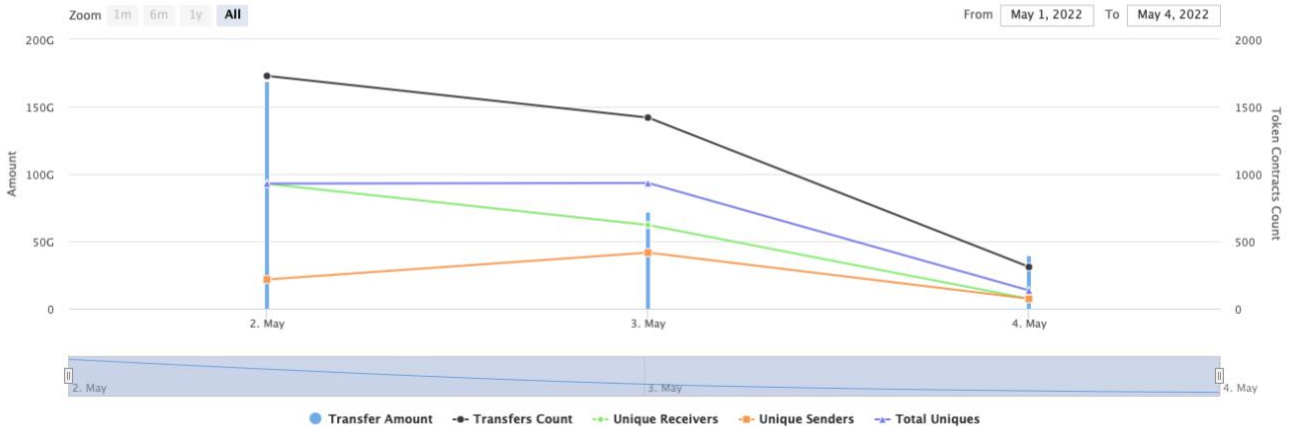
PlugPRO Contract Interaction Details

Time Series: Token Contract Overview

Mon 2, May 2022 - Wed 4, May 2022

Token Contract 0x2407CEd3c9fA576275A8f2871D67673e5Dea08ad (PlugPro)

Source: BscScan.com



1408

C6

780

76C6

5C780

29C4CAD8

C4

87C9C

31B7A384

DF1

65

PlugPRO Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: \$PP 6	5,285,846,899.958286965	10.5717%
2	Null Address: 0x000...dEaD	4,000,000,000	8.0000%
3	0xb5f454e7989366af91fe166a5d8bd77ac2ece79d	2,499,999,319	5.0000%
4	0x54e459e860cd4f684191f32c675daac7d2147c35	1,000,000,000	2.0000%
5	0xd681260e8f29298a230fc8bfd4d8814cd9d79ae7	999,999,999.312820392	2.0000%
6	0xfac7b46a65eb4ad237e1a980bba18efa4b66686c	972,485,171.472900282	1.9450%
7	0xb32d03c8f0cdbe9b22b61b00c3b222a170bcad24	758,843,265.11628918	1.5177%
8	0x8f3950a96dd7b2540a50b3bd81fd4ef69a350581	734,475,174.933911091	1.4690%
9	0x6f91f768c452f2448b20c408172b2278a1360f54	731,814,247.475369951	1.4636%
10	0x7ac1e8bfd8b5e7ced1775544cc4343d4e1e1d7bc	679,697,860.617360346	1.3594%

1408

C6

780

DF1408

65

76C6

5C780

29C4CAD8

C4

87C9C

31B2A384

DF14

65

Contract functions details

+ [Int] IBEP20

- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #

+ [Int] IPancakeERC20

- [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 #

+ [Int] IPancakeFactory

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

+ [Int] IPancakeRouter01

- [Ext] addLiquidity #
- [Ext] addLiquidityETH (\$)
- [Ext] removeLiquidity #

DF1408

65

76C6

5C780

29C4CAD8

C4

87C9C

31B7A384

DF1

65

- [Ext] removeLiquidityETH #
 - [Ext] removeLiquidityWithPermit #
 - [Ext] removeLiquidityETHWithPermit #
 - [Ext] swapExactTokensForTokens #
 - [Ext] swapTokensForExactTokens #
 - [Ext] swapExactETHForTokens (\$)
 - [Ext] swapTokensForExactETH #
 - [Ext] swapExactTokensForETH #
 - [Ext] swapETHForExactTokens (\$)
 - [Ext] factory
 - [Ext] WETH
 - [Ext] quote
 - [Ext] getamountOut
 - [Ext] getamountIn
 - [Ext] getamountsOut
 - [Ext] getamountsIn
- + [Int] IPancakeRouter02 (IPancakeRouter01)
- [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
 - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
 - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
 - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens (\$)
 - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
- + Ownable
- [Pub] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
- + [Lib] Address
- [Int] isContract
 - [Int] sendValue #
 - [Int] functionCall #
 - [Int] functionCall #
 - [Int] functionCallWithValue #
 - [Int] functionCallWithValue #
 - [Int] functionStaticCall
 - [Int] functionStaticCall
 - [Int] functionDelegateCall #
 - [Int] functionDelegateCall #
 - [Prv] _verifyCallResult

+ [Lib] EnumerableSet

- [Prv] _add #
- [Prv] _remove #
- [Prv] _contains
- [Prv] _length
- [Prv] _at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at
- [Int] add #
- [Int] remove #
- [Int] contains
- [Int] length
- [Int] at

+ PlugPro (IBEP20, Ownable)

- [Prv] _isTeam
- [Pub] <Constructor> #
- [Prv] _transfer #
- [Prv] _taxedTransfer #
- [Prv] _feelessTransfer #
- [Prv] _calculateFee
- [Pub] isExcludedFromStaking
- [Pub] _getTotalShares
- [Prv] _addToken #
- [Prv] _removeToken #
- [Prv] _newDividendsOf
- [Prv] _distributeStake #
- [Prv] claimBNB #
- [Prv] _swapContractToken #
 - modifiers: lockTheSwap
- [Prv] _swapTokenForBNB #
- [Prv] _addLiquidity #
- [Pub] getLiquidityReleaseTimeInSeconds
- [Pub] getBurnedTokens
- [Pub] getLimits
- [Pub] getTaxes
- [Pub] getAddressSellLockTimeInSeconds

- [Pub] getSellLockTimeInSeconds
- [Pub] getAddressBuyLockTimeInSeconds
- [Pub] getBuyLockTimeInSeconds
- [Pub] AddressResetSellLock #
- [Pub] AddressResetBuyLock #
- [Pub] BNBWithdraw #
- [Pub] getDividends
- [Pub] TeamWithdrawALLMarketingBNB #
 - modifiers: onlyOwner
- [Pub] TeamWithdrawXMarketingBNB #
 - modifiers: onlyOwner
- [Pub] TeamSwitchManualBNBConversion #
 - modifiers: onlyOwner
- [Pub] TeamChangeAntiWhale #
 - modifiers: onlyOwner
- [Pub] TeamChangeTeamWallet #
 - modifiers: onlyOwner
- [Pub] TeamChangeWalletTwo #
 - modifiers: onlyOwner
- [Pub] TeamDisableSellLock #
 - modifiers: onlyOwner
- [Pub] TeamDisableBuyLock #
 - modifiers: onlyOwner
- [Pub] TeamSetSellLockTime #
 - modifiers: onlyOwner
- [Pub] TeamSetBuyLockTime #
 - modifiers: onlyOwner
- [Pub] AddWalletExclusion #
 - modifiers: onlyOwner
- [Pub] TeamSetTaxes #
 - modifiers: onlyOwner
- [Pub] TeamChangeMarketingShare #
 - modifiers: onlyOwner
- [Pub] TeamCreateLPandBNB #
 - modifiers: onlyOwner
- [Pub] TeamUpdateLimits #
 - modifiers: onlyOwner
- [Pub] SetupEnableTrading #
 - modifiers: onlyOwner
- [Pub] SetupLiquidityTokenAddress #
 - modifiers: onlyOwner
- [Pub] TeamUnlockLiquidityInSeconds #
 - modifiers: onlyOwner
- [Prv] _prolongLiquidityLock #
- [Pub] TeamReleaseLiquidity #

- modifiers: onlyOwner
- [Pub] TeamRemoveLiquidity #
 - modifiers: onlyOwner
- [Pub] TeamRemoveRemainingBNB #
 - modifiers: onlyOwner
- [Ext] <Fallback> (\$)
- [Ext] <Fallback> (\$)
- [Ext] getOwner
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Prv] _approve #
- [Ext] transferFrom #
- [Ext] increaseAllowance #
- [Ext] decreaseAllowance #

(\$) = 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 `_getTotalShares()` uses the loop to find and decrease shares from the `_excludedFromStaking` list. Function will 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.

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

- Owner can withdraw marketing balance.
- Owner can disable auto call of _swapContractToken function.
- Owner can change antiWhale.
- Owner can change teamWallet and walletTwo addresses.
- Owner can disable sell/buy lock.
- Owner can exclude addresses.
- Owner can change sell/buy lock time.
- Owner can change taxes.
- Owner can change marketing share (percentage of BNB that goes to marketing).
- Owner can manually call _swapContractToken function.
- Owner can enable trading(already called).
- Owner can change liquidity token address.
- Owner can increase _liquidityUnlockTime.
- Owner can withdraw liquidity to team wallet if it is not locked.
- Owner can change balance and sell limits.
- Owner can remove liquidity.
- Owner can withdraw contract balance if it is not locked.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are 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.