TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

December, 2021

Audit Details

Audited project

Totally A Rug Pull

Deployer address

0x8b2dcefa75c9f327ed3b53451d21e026543c5404

Client contacts:

Totally A Rug Pull team

Blockchain

Binance Smart Chain

Project website:

http://www.totallyarugpull.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 Totally A Rug Pull to perform an audit of smart contracts:

https://bscscan.com/address/0x6C0A568a3fFb61957812fb3e300e4C10B708d336#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 31.12.2021

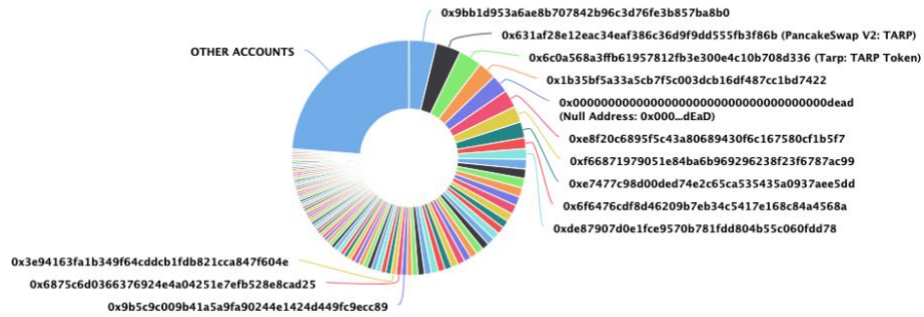|	
Contract name	**Totally A Rug Pull**
Contract address	**0x6C0A568a3fFb61957812fb3e300e4C10B708d336**
Total supply	**1,000,000,000,000**
Token ticker	**TARP**
Decimals	**9**
Token holders	**4,062**
Transactions count	**57,603**
Top 100 holders dominance	**76.24%**
liquidity	**1**
rfi	**1**
Dev address	**0x266423eba1a324305c62578483ae7413e5eba5fa**
Uniswap V2 pair	**0x631af28e12eac34eaf386c36d9f9dd555fb3f86b**
Contract deployer address	**0x8b2dcefa75c9f327ed3b53451d21e026543c5404**
Contract's current owner address	**0x8b2dcefa75c9f327ed3b53451d21e026543c5404**

Totally A Rug Pull Token Distribution

The top 100 holders collectively own 76.24% (762,386,232,200.46 Tokens) of Totally A Rug Pull | Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 4,062

Totally A Rug Pull Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x9bb1d953a6ae8b707842b96c3d76fe3b857ba8b0
0x631af28e12eac34eaf386c36d9f9dd555fb3f86b (PancakeSwap V2: TARP)
0x6c0a568a3ffb61957812fb3e300e4c10b708d336 (Tarp: TARP Token)
0x1b35bf5a33a5cb7f5c003dcb16df487cc1bd7422
0x0000000000000000000000000000000000000dead
(Null Address: 0x000...dEaD)
0xe8f20c6895f5c43a80689430f6c167580cf1b5f7
0xf66871979051e84ba6b969296238f23f6787ac99
0xe7477c98d00ded74e2c65ca535435a0937aee5dd
0x6f6476cdf8d46209b7eb34c5417e168c84a4568a
0xde87907d0e1fce9570b781fdd804b55c060fdd78

0x3e94163fa1b349f64cddcb1fdb821cca847f604e
0x6875c6d0366376924e4a04251e7efb528e8cad25
0x9b5c9c009b41a5a9fa90244e1424d449fc9ecc89

(A total of 762,386,232,200.46 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)
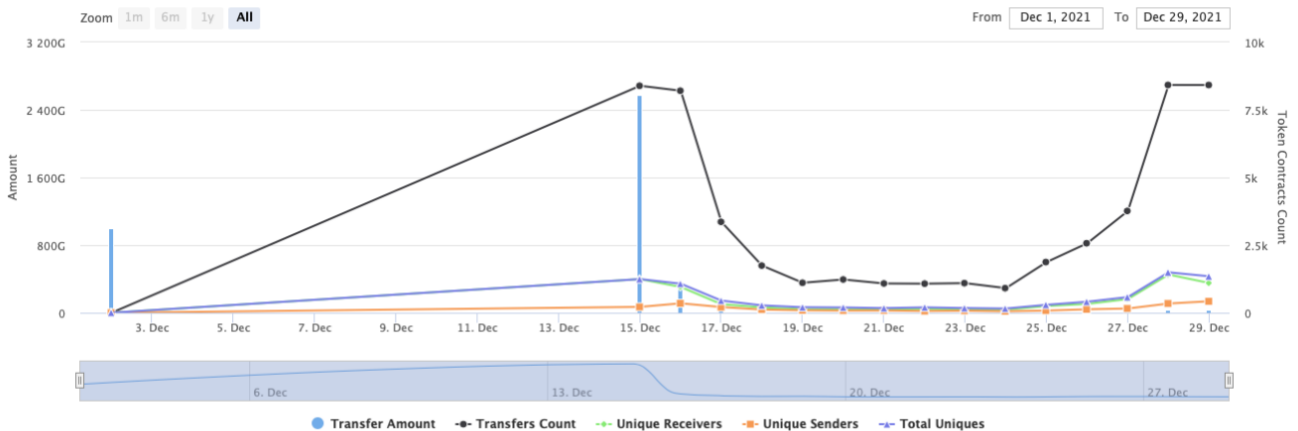
Totally A Rug Pull Contract Interaction Details

Time Series: Token Contract Overview | Thu 2, Dec 2021 - Wed 29, Dec 2021

Token Contract 0x6C0A568a3fFb61957812fb3e300e4C10B708d336 (Totally A Rug Pull)
Source: BscScan.com

Zoom 1m 6m 1y All | From Dec 1, 2021 To Dec 29, 2021

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

Totally A Rug Pull Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x9bb1d953a6ae8b707842b96c3d76fe3b857ba8b0	38,055,735,440.389346918	3.8056%
2	📄 PancakeSwap V2: TARP	34,103,093,827.071591644	3.4103%
3	📄 Tarp: TARP Token	31,500,091,406.09031273	3.1500%
4	0x1b35bf5a33a5cb7f5c003dcb16df487cc1bd7422	25,339,830,775.317209548	2.5340%
5	Null Address: 0x000...dEaD	24,975,332,200.125091459	2.4975%
6	0xe8f20c6895f5c43a80689430f6c167580cf1b5f7	24,390,745,811.638037457	2.4391%
7	0xf66871979051e84ba6b969296238f23f6787ac99	22,295,700,114.50363883	2.2296%
8	0xe7477c98d00ded74e2c65ca535435a0937aee5dd	22,147,211,647.66582536	2.2147%
9	0x6f6476cdf8d46209b7eb34c5417e168c84a4568a	14,806,496,540.852099196	1.4806%
10	0xde87907d0e1fce9570b781fdd804b55c060fdd78	14,554,076,344.368636943	1.4554%

Contract functions details

+ [Int] IERC20
- **[Ext]** totalSupply
- **[Ext]** balanceOf
- **[Ext]** transfer **#**
- **[Ext]** allowance
- **[Ext]** approve **#**
- **[Ext]** transferFrom **#**

+ Context
- [Int] _msgSender
- [Int] _msgData

+ Ownable (Context)
- **[Pub]** <Constructor> **#**
- **[Pub]** owner
- **[Pub]** renounceOwnership **#**
  - modifiers: onlyOwner
- **[Pub]** transferOwnership **#**
  - modifiers: onlyOwner
- **[Prv]** _setOwner **#**

+ [Int] IFactory
- **[Ext]** createPair **#**

+ [Int] IRouter
- **[Ext]** factory
- **[Ext]** WETH
- **[Ext]** addLiquidityETH **($)**
- **[Ext]** swapExactTokensForETHSupportingFeeOnTransferTokens **#**

+ TARP (Context, IERC20, Ownable)
- **[Pub]** <Constructor> **#**
- **[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]** reflectionFromToken
- **[Pub]** tokenFromReflection
- **[Pub]** excludeFromReward **#**
  - modifiers: onlyOwner
- **[Ext]** includeInReward **#**
  - modifiers: onlyOwner
- **[Pub]** excludeFromFee **#**

- modifiers: onlyOwner
- **[Pub]** includeInFee **#**
  - modifiers: onlyOwner
- **[Pub]** isExcludedFromFee
- **[Pub]** setTaxes **#**
  - modifiers: onlyOwner
- **[Prv]** _reflectRfi **#**
- **[Prv]** _takeLiquidity **#**
- **[Prv]** _takeDev **#**
- **[Prv]** _takeBurn **#**
- **[Prv]** _getValues
- **[Prv]** _getTValues
- **[Prv]** _getRValues
- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _approve **#**
- **[Prv]** _transfer **#**
- **[Prv]** _tokenTransfer **#**
- **[Prv]** swapAndLiquify **#**
  - modifiers: lockTheSwap
- **[Prv]** addLiquidity **#**
- **[Prv]** swapTokensForBNB **#**
- **[Ext]** updatedevWallet **#**
  - modifiers: onlyOwner
- **[Ext]** updatMaxTxAmt **#**
  - modifiers: onlyOwner
- **[Ext]** updateSwapTokensAtAmount **#**
  - modifiers: onlyOwner
- **[Ext]** updateSwapEnabled **#**
  - modifiers: onlyOwner
- **[Ext]** updateCoolDownSettings **#**
  - modifiers: onlyOwner
- **[Ext]** setAntibot **#**
  - modifiers: onlyOwner
- **[Ext]** bulkAntiBot **#**
  - modifiers: onlyOwner
- **[Ext]** updateRouterAndPair **#**
  - modifiers: onlyOwner
- **[Pub]** isBot
- **[Ext]** rescueBNB **#**
  - modifiers: onlyOwner
- **[Pub]** rescueAnyBEP20Tokens **#**
  - modifiers: onlyOwner
- **[Ext]** **<Fallback>** **($)**

($) = 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.

```solidity
function includeInReward(address account↑) external onlyOwner() {
    require(_isExcluded[account↑], "Account is not excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- 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.

```solidity
function _getCurrentSupply() private view returns(uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return (_rTotal, _tTotal);
        rSupply = rSupply-_rOwned[_excluded[i]];
        tSupply = tSupply-_tOwned[_excluded[i]];
    }
    if (rSupply < _rTotal/_tTotal) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

- The function **bulkAntiBot()** uses the loop for mark addresses as bots. It also could be aborted with **OUT_OF_GAS** exception if there will be a long addresses list.

```
function bulkAntiBot(address[] memory accounts↑, bool state↑) external onlyOwner{
    for(uint256 i = 0; i < accounts↑.length; i++){
        _isBot[accounts↑[i]] = state↑;
    }
}
```

Recommendation:
Check that the excluded array length is not too big.

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

- Owner can exclude from the fee.
- Owner can change taxes.
- Owner can change dev wallet address.
- Owner can change the maximum transaction amount.
- Owner can change swapTokensAtAmount.
- Owner can enable/disable swap.
- Owner can change cooldown settings.
- Owner can mark addresses as bots.
- Owner can change router and pair addresses.
- Owner can withdraw contract tokens and BNBs.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details provided by the team:
https://app.unicrypt.network/amm/pancake-v2/pair/0x631af28e12eac34eaf386c36d9f9dd555fb3f86b

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.