Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

November, 2021

Audit Details

Audited project

Portfolio

Deployer address

0xD18556Ba82Ff80E05eBCB4C3E8F868dcAa3Dc128

Client contacts:

Portfolio team

Blockchain

Binance Smart Chain

Project website:

https://www.portfoliotoken.net/

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 Portfolio to perform an audit of smart contracts:

https://bscscan.com/address/0x307204863f3bc29d1a874e38ace62114a8990c4e#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

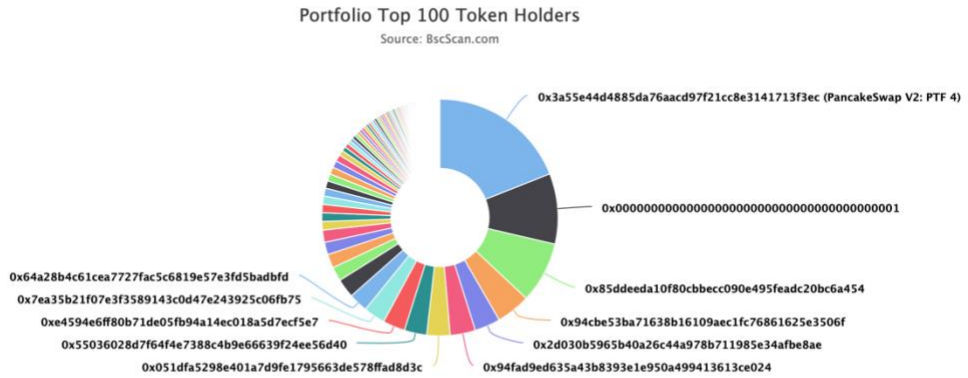
Token contract details for 22.11.2021

Contract name	Portfolio
Contract address	0x307204863f3bc29D1a874E38aCe62114a8990c4e
Total supply	775,000,000,000,000
Token ticker	PTF
Decimals	9
Token holders	1,197
Transactions count	11,171
Top 100 holders dominance	116.39%
Total fees	146,685,533,661,360.921239735
Contract deployer address	0xD18556Ba82Ff80E05eBCB4C3E8F868dcAa3Dc128
Contract's current owner address	0x3bada0E783ED10FAa7Dd42DA84A288fbb3CD4C1d

Portfolio Token Distribution

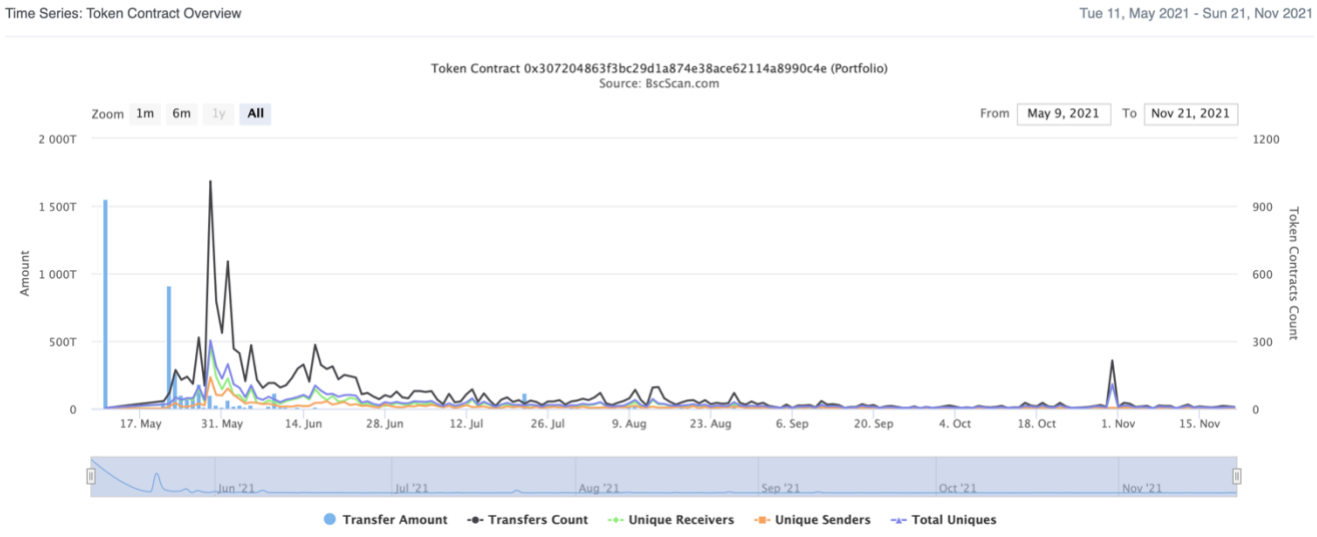
The top 100 holders collectively own 116.39% (901,998,658,488,956.00 Tokens) of Portfolio

Token Total Supply: 775,000,000,000,000.00 Token | Total Token Holders: 1,197



(A total of 901,998,658,488,956.00 tokens held by the top 100 accounts from the total supply of 775,000,000,000,000.00 token)

Portfolio Contract Interaction Details



Portfolio Top 10 Token Holders

Rank	Address	Quantity	Percentage
1	PancakeSwap V2: PTF 4	171,371,813,603,146.68752783	22.1125%
2	0x0000000000000000000000000000000000000001	86,872,217,899,929.265436795	11.2093%
3	0x85ddeeda10f80cbbecc090e495feadc20bc6a454	75,255,236,205,255.620860823	9.7104%
4	0x94cbe53ba71638b16109aec1fc76861625e3506f	42,197,278,595,881.185790726	5.4448%
5	0x2d030b5965b40a26c44a978b711985e34afbe8ae	31,688,079,407,170.295606675	4.0888%
6	0x94fad9ed635a43b8393e1e950a499413613ce024	31,149,055,678,429.752554489	4.0192%
7	0x051dfa5298e401a7d9fe1795663de578ffad8d3c	28,645,367,451,044.116788882	3.6962%
8	0x55036028d7f64f4e7388c4b9e66639f24ee56d40	27,765,287,118,667.592334008	3.5826%
9	0xe4594e6ff80b71de05fb94a14ec018a5d7ecf5e7	27,397,207,615,244.979582728	3.5351%
10	0x7ea35b21f07e3f3589143c0d47e243925c06fb75	26,672,558,695,635.158274982	3.4416%

Contract functions details

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

+ [Int] IBEP20
  - [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

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

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

+ Portfolio (Context, IBEP20, 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] isExcluded
- [Pub] isCharity
- [Pub] totalFees
- [Pub] totalBurn
- [Pub] totalCharity
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Ext] setAsCharityAccount #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _standardTransferContent #
- [Prv] _transferToExcluded #
- [Prv] _excludedFromTransferContent #
- [Prv] _transferFromExcluded #
- [Prv] _excludedToTransferContent #
- [Prv] _transferBothExcluded #
- [Prv] _bothTransferContent #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTBasics
- [Prv] getTTransferAmount
- [Prv] _getRBasics
- [Prv] _getRTransferAmount
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _sendToCharity #
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Prv] _getTaxFee
- [Ext] TAXFEE #
  - modifiers: onlyOwner
- [Ext] BURNFEE #
  - modifiers: onlyOwner
- [Ext] CHARITYFEE #
  - modifiers: onlyOwner
- [Prv] _getMaxTxAmount

($) = 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.	High issue
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

1. Reward fee

Issue:

- Charity fee is subtracted from `_rTotal` value in `_reflectFee()` function. Also, exactly this fee amount goes to charity address.

```
function _reflectFee(uint256 rFee, uint256 rBurn, uint256 rCharity, uint256 tFee, uint256 tBurn, uint256 tCharity) private {
    _rTotal = _rTotal.sub(rFee).sub(rBurn).sub(rCharity);
    _tFeeTotal = _tFeeTotal.add(tFee);
    _tBurnTotal = _tBurnTotal.add(tBurn);
    _tCharityTotal = _tCharityTotal.add(tCharity);
    _tTotal = _tTotal.sub(tBurn);
}
```

Recommendation:

Please recheck logic of charity fee and keep only one way of taking it – would it be reflecting or it would go to charity address. Otherwise, reflection rate would be wrong.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

2. Out of gas

Issue:

- The function `includeAccount()` 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.

```
function includeAccount(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already 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.

```
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.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

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

- Owner can include in and exclude from reward.

```
function excludeAccount(address account) external onlyOwner() {
    require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'We can not exclude Uniswap router.');
    require(!_isExcluded[account], "Account is already excluded");
    if(_rOwned[account] > 0) {
        _tOwned[account] = tokenFromReflection(_rOwned[account]);
    }
    _isExcluded[account] = true;
    _excluded.push(account);
}

function includeAccount(address account) external onlyOwner() {
    require(_isExcluded[account], "Account is already 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;
        }
    }
}
```

- Owner can set charity addresses.

```
function setAsCharityAccount(address account) external onlyOwner() {
    require(account != 0x7a250d5630B4cF539739dF2C5dAcb4c659F2488D, 'The Uniswap router can not be the charity account.');
    require(!_isCharity[account], "Account is already charity account");
    _isCharity[account] = true;
    _charity.push(account);
}
```

- Owner can change tax, burn and charity fees.

```
function TAXFEE(uint256 taxFee) external onlyOwner() {
    _TAX_FEE = taxFee;
}

function BURNFEE(uint256 burnFee) external onlyOwner() {
    _BURN_FEE = burnFee;
}

function CHARITYFEE(uint256 charityFee) external onlyOwner() {
    _CHARITY_FEE = charityFee;
}
```

Conclusion

Smart contracts contain high severity issues and owner privileges!
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.