Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

May, 2021

Audit Details

Audited project

Weedz Token

Deployer address

0x71c87346fd1C86BE81FB461443f102cF67b08bFC

Client contacts:

Weedz Token team

Blockchain

Binance Smart Chain

Project website:

https://weedz.space/

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 Weedz Token to perform an audit of smart contracts:
https://bscscan.com/address/0x6e14ea10a4c6cb9731b720137416dff88fc4df40#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

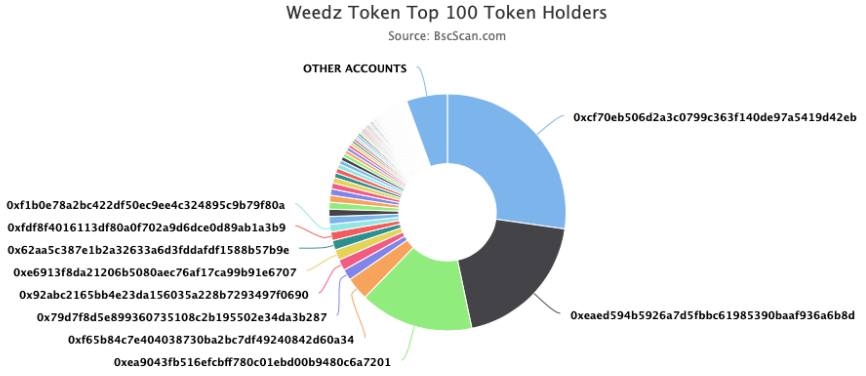
Token contract details for 30.05.2021

Contract name	Weedz Token
Contract address	0x6e14EA10A4c6cB9731b720137416dff88fC4df40
Total supply	390690700756112110583709
Token ticker	weedz
Decimals	9
Token holders	577
Transactions count	6,328
Top 100 holders dominance	94.41%
Liquidity fee	2
Tax fee	4
Total tax fees	39079065658517185888569
Uniswap V2 pair	0xcf70eb506d2a3c0799c363f140de97a5419d42eb
Contract deployer address	0x71c87346fd1C86BE81FB461443f102cF67b08bFC
Contract's current owner address	0x0000000000000000000000000000000000000000

Weedz Token Token Distribution

The top 100 holders collectively own 94.41% (368,862,516,047,871.00 Tokens) of Weedz Token

Token Total Supply: 390,690,700,756,112.11 Token | Total Token Holders: 577

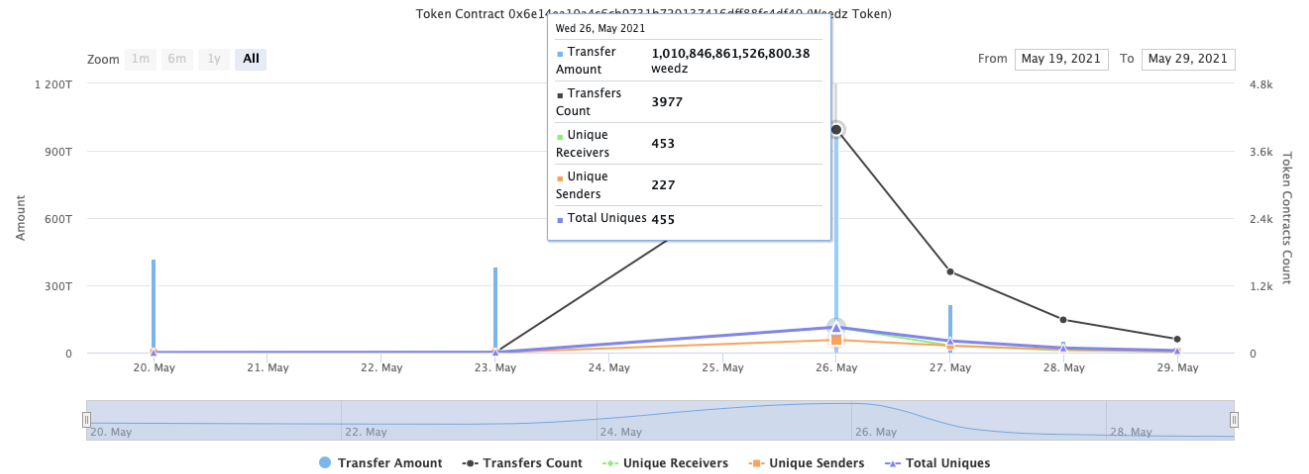


(A total of 368,862,516,047,871.00 tokens held by the top 100 accounts from the total supply of 390,690,700,756,112.11 token)

Weedz Token Contract Interaction Details

Time Series: Token Contract Overview

Thu 20, May 2021 - Sat 29, May 2021



Weedz Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xcf70eb506d2a3c0799c363f140de97a5419d42eb	106,449,731,837,328.290475975	27.2465%
2	0xeaed594b5926a7d5fbbc61985390baaf936a6b8d	76,026,741,665,490	19.4596%
3	0xea9043fb516efcbff780c01ebd00b9480c6a7201	60,792,243,915,579.086663466	15.5602%
4	0xf65b84c7e404038730ba2bc7df49240842d60a34	12,290,065,730,869.447308757	3.1457%
5	0x79d7f8d5e899360735108c2b195502e34da3b287	5,898,482,781,610.027040478	1.5098%
6	0x92abc2165bb4e23da156035a228b7293497f0690	5,836,243,302,215.903613659	1.4938%
7	0xe6913f8da21206b5080aec76af17ca99b91e6707	5,664,240,585,914.854187207	1.4498%
8	0x62aa5c387e1b2a32633a6d3fddafdf1588b57b9e	5,073,571,001,389.130587284	1.2986%
9	0xfdf8f4016113df80a0f702a9d6dce0d89ab1a3b9	4,562,423,250,735.079927759	1.1678%
10	0xf1b0e78a2bc422df50ec9ee4c324895c9b79f80a	4,198,691,171,570.313703053	1.0747%

Weedz Token LP Token Holders

Rank	Address	Quantity	Percentage
1	0xc765bddb93b0d1c1a88282ba0fa6b2d00e3e0c83	2,958.527595473194161456	88.8377%
2	0x6e14ea10a4c6cb9731b720137416dff88fc4df40	329.735661256675406646	9.9012%
3	0xaa3d85ad9d128dfecb55424085754f6dfa643eb1	29.884117125991860216	0.8974%
4	0x07d80ae6f36a5e08dca74ce884a24d39db9934ed	12.115760010425940241	0.3638%
5	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

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

+ [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
  - [Int] ceil

+ [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

+ [Int] IUniswapV2Factory
  - [Ext] createPair #

+ [Int] IUniswapV2Pair
  - [Ext] sync #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
```

```
+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)

+  RewardWallet
  - [Pub] <Constructor> #

+  Balancer
  - [Pub] <Constructor> #

+  WeedzToken (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Int] find2Percent
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcluded
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Ext] excludeAccount #
    - modifiers: onlyOwner
  - [Ext] includeAccount #
    - modifiers: onlyOwner
  - [Prv] _approve #
  - [Prv] _transfer #
  - [Prv] collectFee #
  - [Prv] _getReflectionRate
  - [Prv] swapAndLiquify #
    - modifiers: lockTheSwap
  - [Prv] swapTokensForEth #
  - [Prv] addLiquidity #
  - [Ext] setPair #
    - modifiers: onlyOwner
  - [Ext] setTaxless #
    - modifiers: onlyOwner
  - [Ext] setSwapAndLiquifyEnabled #
    - modifiers: onlyOwner
  - [Ext] setFeeActive #
    - modifiers: onlyOwner
  - [Ext] setTaxFee #
    - modifiers: onlyOwner
  - [Ext] setBurnFee #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFee #
```

  - modifiers: onlyOwner
- [Ext] setCommunity #
  - modifiers: onlyOwner
- [Ext] setMaxTxAmount #
  - modifiers: onlyOwner
- [Ext] setMinTokensBeforeSwap #
  - 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 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], "ERC20: Account is already included");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tokenBalance[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- The function _getReflectionRate() 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 _getReflectionRate() private view returns (uint256) {
    uint256 reflectionSupply = _reflectionTotal;
    uint256 tokenSupply = _tokenTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _reflectionBalance[_excluded[i]] > reflectionSupply ||
            _tokenBalance[_excluded[i]] > tokenSupply
        ) return _reflectionTotal.div(_tokenTotal);
        reflectionSupply = reflectionSupply.sub(
            _reflectionBalance[_excluded[i]]
        );
        tokenSupply = tokenSupply.sub(_tokenBalance[_excluded[i]]);
    }
    if (reflectionSupply < _reflectionTotal.div(_tokenTotal))
        return _reflectionTotal.div(_tokenTotal);
    return reflectionSupply.div(tokenSupply);
}
```

Recommendation:

Check that the excluded array length is not too big.

2. Wrong reflection from token calculations

Issue:

- **Missing parentheses when calculating target value.**

```
tokenAmount
        .sub(tokenAmount.mul(_taxFee).div(10**(_feeDecimal + 2)))
        .mul(_getReflectionRate());
```

```
function reflectionFromToken(uint256 tokenAmount, bool deductTransferFee)
    public
    view
    returns (uint256)
{
    require(tokenAmount <= _tokenTotal, "Amount must be less than supply");
    if (!deductTransferFee) {
        return tokenAmount.mul(_getReflectionRate());
    } else {
        return
            tokenAmount
                .sub(tokenAmount.mul(_taxFee).div(10**_feeDecimal + 2))
                .mul(_getReflectionRate());
    }
}
```

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

- **Owner can change the tax, burn and liquidity fee.**

```
ftrace | funcSig
function setTaxFee(uint256 fee) external onlyOwner {
    _taxFee = fee;
}

ftrace | funcSig
function setBurnFee(uint256 fee) external onlyOwner {
    _burnFee = fee;
}

ftrace | funcSig
function setLiquidityFee(uint256 fee) external onlyOwner {
    _liquidityFee = fee;
}
```

- **Owner can change the maximum transaction amount.**

```
ftrace | funcSig
function setMaxTxAmount(uint256 amount) external onlyOwner {
    maxTxAmount = amount;
}
```

- Owner can change uniswapV2Pair.

```
ftrace | funcSig
function setPair(address pair) external onlyOwner {
    uniswapV2Pair = pair;
}
```

- Owner can exclude from the taxes.

```
ftrace | funcSig
function setTaxless(address account, bool value) external onlyOwner {
    isTaxless[account] = value;
}
```

- Owner can disable and enable fees.

```
ftrace | funcSig
function setFeeActive(bool value) external onlyOwner {
    isFeeActive = value;
}
```

- Owner can change community fee.

```
ftrace | funcSig
function setCommunity(uint256 amount) external onlyOwner {
    communityFee = amount;
}
```

- Owner can change minimum amount of tokens needed to swap.

```
ftrace | funcSig
function setMinTokensBeforeSwap(uint256 amount) external onlyOwner {
    minTokensBeforeSwap = amount;
}
```

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/0xcF70Eb506d2A3c0799c363F140DE97A5419d42EB

Ownership renounce provided by the team:
https://bscscan.com/tx/0x0da4292eed51b06a0e222055f91bace5f9e910e18e6dfb7e88464b6484bc3196#eventlog

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.