TECH RATE

SMART CONTRACTS SECURITY

AUDIT REPORT

Audit Details

Audited project

WEB3 Game

Deployer address

0x78eeee6c07ea6d4f672f60d42a53af932a0e721a

Client contacts:

WEB3 Game team

Blockchain

Binance Smart Chain

Project website:

https://web3game.tech

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 WEB3 Game to perform an audit of smart contracts:
https://bscscan.com/address/0x09d96101dB62FfAc32f798CB9A61e501337b79C6#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 19.04.2022

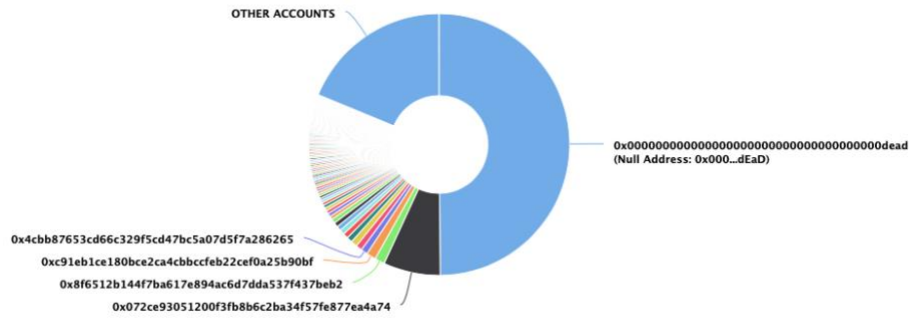|	
Contract name	WEB3 Game
Contract address	0x09d96101dB62FfAc32f798CB9A61e501337b79C6
Total supply	10,000,000,000,000
Token ticker	WEB3
Decimals	9
Token holders	10,851
Transactions count	24,162
Top 100 holders dominance	81.22%
Total fees	173440430486244848280
Uniswap V2 pair	0x0000000000000000000000000000000000000000
Contract deployer address	0x78eeee6c07ea6d4f672f60d42a53af932a0e721a
Owner address	0x78eeee6c07ea6d4f672f60d42a53af932a0e721a

WEB3 Game Token Distribution

The top 100 holders collectively own 81.22% (8,122,130,201,325.86 Tokens) of WEB3 Game   Token Total Supply: 10,000,000,000,000.00 Token | Total Token Holders: 10,853

WEB3 Game Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x0000000000000000000000000000000000000dead
(Null Address: 0x000...dEaD)

0x4cbb87653cd66c329f5cd47bc5a07d5f7a286265
0xc91eb1ce180bce2ca4cbbccfeb22cef0a25b90bf
0x8f6512b144f7ba617e894ac6d7dda537f437beb2
0x072ce93051200f3fb8b6c2ba34f57fe877ea4a74

(A total of 8,122,130,201,325.86 tokens held by the top 100 accounts from the total supply of 10,000,000,000,000.00 token)

WEB3 Game Contract Interaction Details

Time Series: Token Contract Overview   Wed 13, Apr 2022 - Mon 18, Apr 2022

Token Contract 0x09d96101dB62FfAc32f798CB9A61e501337b79C6 (WEB3 Game)
Source: BscScan.com

Zoom 1m 6m 1y **All**   From Apr 12, 2022 To Apr 18, 2022

● Transfer Amount   ●∙ Transfers Count   +∙ Unique Receivers   ▬∙ Unique Senders   ▵∙ Total Uniques

WEB3 Game Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0x000...dEaD	4,985,551,657,966.468159215	49.8555%
2	0x072ce93051200f3fb8b6c2ba34f57fe877ea4a74	705,569,565,787.283659576	7.0557%
3	0x8f6512b144f7ba617e894ac6d7dda537f437beb2	123,198,512,640.831960631	1.2320%
4	0xc91eb1ce180bce2ca4cbbccfeb22cef0a25b90bf	116,605,891,287.513832292	1.1661%
5	0x4cbb87653cd66c329f5cd47bc5a07d5f7a286265	83,492,780,156.501823817	0.8349%
6	0x1094f6e1127b5dc869dc9809f672d975f59e68dd	78,444,244,179.0695081	0.7844%
7	0xd0101051681604743c0ee71e963b4122e87f64e1	77,450,241,069.169933985	0.7745%
8	0x9a397dbd961b9b736afd98eae69bc019e38e07e7	68,010,101,338.157032337	0.6801%
9	0x1733b96f2693d2eb6684c82d0e4c91c2d4747bbe	65,852,043,409.824650711	0.6585%
10	Web3 Games: Deployer	60,555,406,594.456029356	0.6056%

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

+ [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

+ WEB3 (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] isExcluded
- [Pub] totalFees
- [Ext] setMaxTxPercent #
  - modifiers: onlyOwner
- [Pub] reflect #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Ext] excludeAccount #
  - modifiers: onlyOwner
- [Ext] includeAccount #
  - modifiers: onlyOwner
- [Ext] addToWhitelist #
  - modifiers: onlyOwner
- [Ext] removeFromWhitelist #
  - modifiers: onlyOwner
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #
- [Prv] _transferBothExcluded #
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Ext] setUniswapPair #
  - modifiers: onlyOwner

($) = 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.**	Low issues
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.
- 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.
- The function removeFromWhitelist() also uses the loop to iterate through the whitelist. It also could be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:
Check that the arrays' length is not too big.

2. Rounding error

Issue:

- At some calculation with division, it is goes first. In Solidity we don't have floating points, but instead we get rounding errors.

Recommendation:
Do division after multiplication.

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

- Owner can change the maximum transaction amount.
- Owner can whitelist addresses.
- Owner can change uniswapPair.

TECH
RATE

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 provided by the team:
https://app.unicrypt.network/amm/pancake-v2/pair/0x072ce93051200f3fb8b6c2ba34f57fe877ea4a74

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.