Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

October, 2021

Audit Details

Audited project

WEX

Deployer address

0x5207843600db13e69397e48eb104e1f4444ce71a
0x6e557bba2370b2f9ba2b06e8aa9d3019cc40deb9

Client contacts:

WEX team

Blockchain

Binance Smart Chain

Project website:

Not provided

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 WEX to perform an audit of smart contracts:

- MasterChef: https://bscscan.com/address/0xa8a8b895d95dbd2791799476b35d9caeb9c36a13
- Token: https://bscscan.com/address/0x09bb6042a19bb3a6981e9a47ec0f006dbd28a8d1
- Referral: https://bscscan.com/address/0x2ef40994bea0724f6416cb5250d2bbae35509caf
- Profile: https://bscscan.com/address/0xa99956a6420c1d0cba7f1463b4d31911ae1b25a9
- NFT: https://bscscan.com/token/0xd7286bfe8b97922f81bda4a49e959903d882eb82
- NFT Factory: https://bscscan.com/address/0x6d6bb29ae359b0989a7c0a03f0e4af50a655304f

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

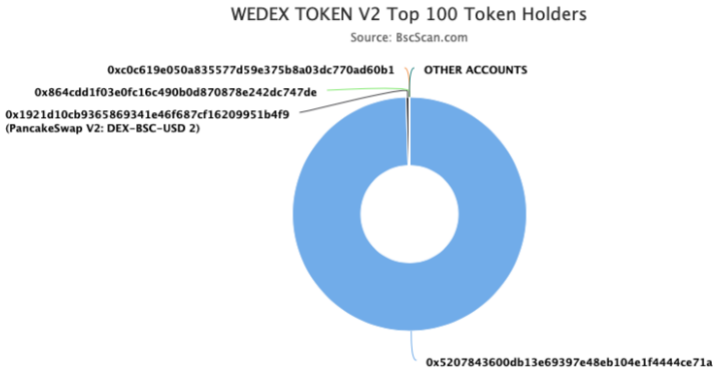
WEDEX TOKEN V2 contract details for 26.10.2021

Contract name	Wedex
Contract address	0x09BB6042A19BB3A6981e9a47EC0f006dBd28a8d1
Total supply	650,000
Token ticker	DEX
Decimals	18
Token holders	7
Transactions count	18
Top 100 holders dominance	100.00%
Contract deployer address	0x5207843600db13e69397e48eb104e1f4444ce71a
Contract’s current owner address	0x5207843600db13e69397e48eb104e1f4444ce71a

WEX Token Distribution

The top 100 holders collectively own 100.00% (650,000.00 Tokens) of WEDEX TOKEN V2

Token Total Supply: 650,000.00 Token | Total Token Holders: 7

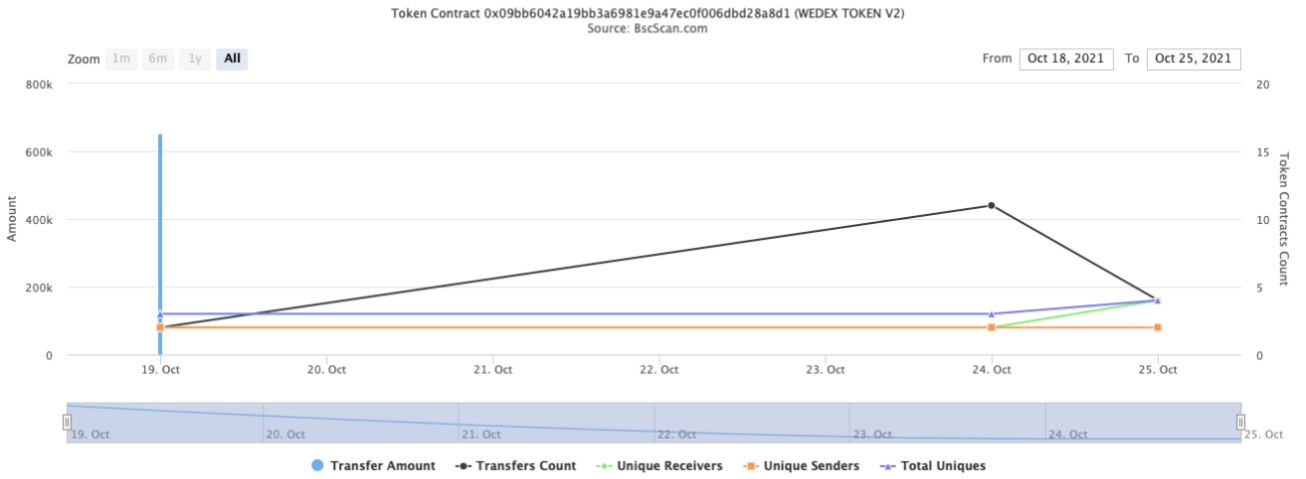


(A total of 650,000.00 tokens held by the top 100 accounts from the total supply of 650,000.00 token)

WEX Contract Interaction Details

Time Series: Token Contract Overview

Tue 19, Oct 2021 - Mon 25, Oct 2021



WEX Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x5207843600db13e69397e48eb104e1f4444ce71a	646,990.0059895088215391	99.5369%
2	PancakeSwap V2: DEX-BSC-USD 2	2,716.606378770149839119	0.4179%
3	0x864cdd1f03e0fc16c490b0d870878e242dc747de	170.486636911917742761	0.0262%
4	0xc0c619e050a835577d59e375b8a03dc770ad60b1	70.145683908271741111	0.0108%
5	0x889f48e569546df6d7d16c697e411856941a09ec	49.029667936850311124	0.0075%
6	0xfbe0961ded05ac9080ad81b1e747a18cf3e5f951	2.728474522495623276	0.0004%
7	0xa8eed8b3be35b9ad25f2c9fc628acf48abd08255	0.997168441493203509	0.0002%

Contracts Details

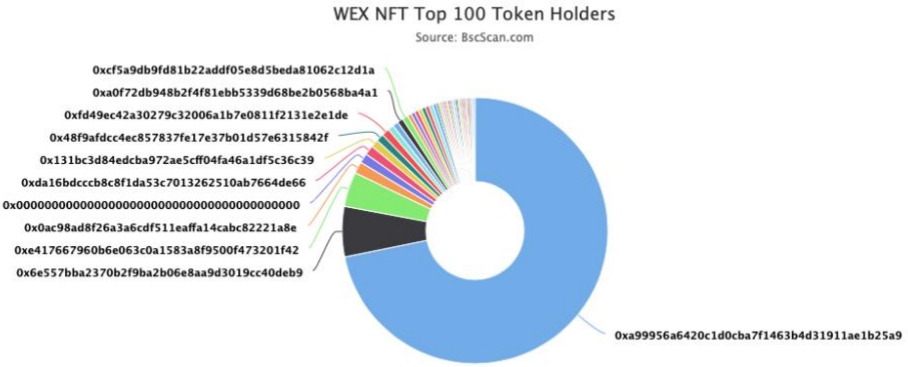
WexNFT contract details for 26.10.2021

Contract name	WexNFT
Contract address	0xd7286bfe8b97922f81bda4a49e959903d882eb82
Total supply	421
Token ticker	WNT
Base URI	ipfs://
Token holders	41
Transactions count	806
Top 100 holders dominance	101.19%
Contract deployer address	0x6e557bba2370b2f9ba2b06e8aa9d3019cc40deb9
Contract’s current owner address	0x6d6bb29ae359b0989a7c0a03f0e4af50a655304f

WEX Token Distribution

The top 100 holders collectively own 101.19% (426.00 Tokens) of WEX NFT

Token Total Supply: 421.00 Token | Total Token Holders: 41



(A total of 426.00 tokens held by the top 100 accounts from the total supply of 421.00 token)

WEX Contract Interaction Details

Time Series: Address Token (BEP-20) Transfers

Fri 30, Jul 2021 - Fri 30, Jul 2021

Pro-Tip: Click on the chart data points to view more

WEX Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xa99956a6420c1d0cba7f1463b4d31911ae1b25a9	306	72.6841%
2	0x6e557bba2370b2f9ba2b06e8aa9d3019cc40deb9	26	6.1758%
3	0xe417667960b6e063c0a1583a8f9500f473201f42	18	4.2755%
4	0x0ac98ad8f26a3a6cdf511eaffa14cabc82221a8e	6	1.4252%
5	0x0000000000000000000000000000000000000000	5	1.1876%
6	0xda16bdcccb8c8f1da53c7013262510ab7664de66	5	1.1876%
7	0x131bc3d84edcba972ae5cff04fa46a1df5c36c39	4	0.9501%
8	0x48f9afdcc4ec857837fe17e37b01d57e6315842f	4	0.9501%
9	0xfd49ec42a30279c32006a1b7e0811f2131e2e1de	4	0.9501%
10	0x2ce30d25ef5290bca64d6cff2470d7935c234579	3	0.7126%

NFTFactoryV6 functions details

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

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

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

+ [Lib] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ [Lib] Counters
  - [Int] current
  - [Int] increment #
  - [Int] decrement #

+ [Int] IERC165
  - [Ext] supportsInterface

+ [Int] IERC721 (IERC165)
  - [Ext] balanceOf
  - [Ext] ownerOf
  - [Ext] safeTransferFrom #
  - [Ext] transferFrom #
  - [Ext] approve #
  - [Ext] getApproved
  - [Ext] setApprovalForAll #
  - [Ext] isApprovedForAll
  - [Ext] safeTransferFrom #

+ [Int] IERC721Metadata (IERC721)
  - [Ext] name
  - [Ext] symbol
  - [Ext] tokenURI

+ [Int] IERC721Enumerable (IERC721)
  - [Ext] totalSupply
  - [Ext] tokenOfOwnerByIndex
  - [Ext] tokenByIndex

+ [Int] IERC721Receiver
  - [Ext] onERC721Received #

+ ERC165 (IERC165)
  - [Int] <Constructor> #
  - [Pub] supportsInterface
  - [Int] _registerInterface #

+ [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

+ [Lib] EnumerableMap
  - [Prv] _set #
  - [Prv] _remove #
  - [Prv] _contains
  - [Prv] _length
  - [Prv] _at
  - [Prv] _get
  - [Prv] _get
  - [Int] set #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
  - [Int] get
  - [Int] get

+ [Lib] Strings
  - [Int] toString

+ ERC721 (Context, ERC165, IERC721, IERC721Metadata, IERC721Enumerable)
  - [Pub] <Constructor> #
  - [Pub] balanceOf
  - [Pub] ownerOf
  - [Pub] name
  - [Pub] symbol
  - [Pub] tokenURI
  - [Pub] baseURI
  - [Pub] tokenOfOwnerByIndex
  - [Pub] totalSupply
  - [Pub] tokenByIndex
  - [Pub] approve #
  - [Pub] getApproved
  - [Pub] setApprovalForAll #
  - [Pub] isApprovedForAll
  - [Pub] transferFrom #
  - [Pub] safeTransferFrom #
  - [Pub] safeTransferFrom #
  - [Int] _safeTransfer #
  - [Int] _exists
  - [Int] _isApprovedOrOwner
  - [Int] _safeMint #
  - [Int] _safeMint #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _transfer #
  - [Int] _setTokenURI #
  - [Int] _setBaseURI #
  - [Prv] _checkOnERC721Received #
  - [Prv] _approve #
  - [Int] _beforeTokenTransfer #

+ PancakeBunnies (ERC721, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC721
  - [Ext] getBunnyId
  - [Ext] getBunnyName
  - [Ext] getBunnyNameOfTokenId
  - [Ext] mint #
    - modifiers: onlyOwner
  - [Ext] setBunnyName #
    - modifiers: onlyOwner
  - [Ext] burn #
    - modifiers: onlyOwner

+ [Int] IWedexReferral
  - [Ext] recordReferral #
  - [Ext] recordReferralCommission #
  - [Ext] getReferrer
  - [Ext] addTotalFund #
  - [Ext] reduceTotalFund #
  - [Ext] getReferrerPercentage

+ NFTFactoryV5 (Ownable)
  - [Pub] <Constructor> #
  - [Ext] mintNFT #
  - [Int] payRefCommision #
  - [Int] safeWedexTransfer #
  - [Pub] setWedexReferral #
    - modifiers: onlyOwner
  - [Ext] changeOwnershipNFTContract #
    - modifiers: onlyOwner
  - [Ext] claimFee #
    - modifiers: onlyOwner
  - [Ext] updateRefferalSystem #
    - modifiers: onlyOwner
  - [Ext] setBunny #
    - modifiers: onlyOwner
  - [Ext] burnBunny #
  - [Ext] setBunnyPrice #
    - modifiers: onlyOwner
  - [Ext] setStartBlockNumber #
    - modifiers: onlyOwner
  - [Ext] setEndBlockNumber #
    - modifiers: onlyOwner

+ NFTFactoryV6 (Ownable)
  - [Pub] <Constructor> #
  - [Ext] mintNFT #
  - [Pub] totalCommission
  - [Int] payRefCommision #
  - [Int] payBonusCommission #
  - [Int] safeWedexTransfer #
  - [Pub] setWedexReferral #
    - modifiers: onlyOwner
  - [Ext] changeOwnershipNFTContract #

    - modifiers: onlyOwner
  - [Ext] claimFee #
    - modifiers: onlyOwner
  - [Ext] updateRefferalSystem #
    - modifiers: onlyOwner
  - [Ext] setBunny #
    - modifiers: onlyOwner
  - [Ext] burnBunny #
  - [Ext] setBunnyPrice #
    - modifiers: onlyOwner
  - [Ext] setStartBlockNumber #
    - modifiers: onlyOwner
  - [Pub] setCaketoken #
    - modifiers: onlyOwner
  - [Ext] setEndBlockNumber #
    - modifiers: onlyOwner

($) = payable function
= non-constant function

WexNFT functions details

+ Context
  - [Int] _msgSender
  - [Int] _msgData
+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod
+ [Lib] Counters
  - [Int] current
  - [Int] increment #
  - [Int] decrement #
+ [Int] IERC165
  - [Ext] supportsInterface
+ [Int] IERC721 (IERC165)
  - [Ext] balanceOf
  - [Ext] ownerOf
  - [Ext] safeTransferFrom #
  - [Ext] transferFrom #
  - [Ext] approve #
  - [Ext] getApproved

  - [Ext] setApprovalForAll #
  - [Ext] isApprovedForAll
  - [Ext] safeTransferFrom #
+ [Int] IERC721Metadata (IERC721)
  - [Ext] name
  - [Ext] symbol
  - [Ext] tokenURI
+ [Int] IERC721Enumerable (IERC721)
  - [Ext] totalSupply
  - [Ext] tokenOfOwnerByIndex
  - [Ext] tokenByIndex
+ [Int] IERC721Receiver
  - [Ext] onERC721Received #
+ ERC165 (IERC165)
  - [Int] <Constructor> #
  - [Pub] supportsInterface
  - [Int] _registerInterface #
+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [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
+ [Lib] EnumerableMap
  - [Prv] _set #
  - [Prv] _remove #
  - [Prv] _contains
  - [Prv] _length
  - [Prv] _at
  - [Prv] _get

  - [Prv] _get
  - [Int] set #
  - [Int] remove #
  - [Int] contains
  - [Int] length
  - [Int] at
  - [Int] get
  - [Int] get
+ [Lib] Strings
  - [Int] toString
+ ERC721 (Context, ERC165, IERC721, IERC721Metadata, IERC721Enumerable)
  - [Pub] <Constructor> #
  - [Pub] balanceOf
  - [Pub] ownerOf
  - [Pub] name
  - [Pub] symbol
  - [Pub] tokenURI
  - [Pub] baseURI
  - [Pub] tokenOfOwnerByIndex
  - [Pub] totalSupply
  - [Pub] tokenByIndex
  - [Pub] approve #
  - [Pub] getApproved
  - [Pub] setApprovalForAll #
  - [Pub] isApprovedForAll
  - [Pub] transferFrom #
  - [Pub] safeTransferFrom #
  - [Pub] safeTransferFrom #
  - [Int] _safeTransfer #
  - [Int] _exists
  - [Int] _isApprovedOrOwner
  - [Int] _safeMint #
  - [Int] _safeMint #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _transfer #
  - [Int] _setTokenURI #
  - [Int] _setBaseURI #
  - [Prv] _checkOnERC721Received #
  - [Prv] _approve #
  - [Int] _beforeTokenTransfer #
+ WexNFT (ERC721, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC721
  - [Ext] getBunnyId
  - [Ext] getBunnyName
  - [Ext] getBunnyNameOfTokenId
  - [Ext] mint #
    - modifiers: onlyOwner
  - [Ext] setBunnyName #
    - modifiers: onlyOwner
  - [Ext] burn #
    - modifiers: onlyOwner
($) = payable function
= non-constant function

PancakeProfile functions details

+ [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

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

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

+ AccessControl (Context)
  - [Pub] hasRole
  - [Pub] getRoleMemberCount
  - [Pub] getRoleMember
  - [Pub] getRoleAdmin
  - [Pub] grantRole #
  - [Pub] revokeRole #
  - [Pub] renounceRole #
  - [Int] _setupRole #
  - [Int] _setRoleAdmin #
  - [Prv] _grantRole #
  - [Prv] _revokeRole #

+ [Lib] SafeMath
  - [Int] add

  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Lib] Counters
  - [Int] current
  - [Int] increment #
  - [Int] decrement #

+ [Int] IERC165
  - [Ext] supportsInterface

+ [Int] IERC721 (IERC165)
  - [Ext] balanceOf
  - [Ext] ownerOf
  - [Ext] safeTransferFrom #
  - [Ext] transferFrom #
  - [Ext] approve #
  - [Ext] getApproved
  - [Ext] setApprovalForAll #
  - [Ext] isApprovedForAll
  - [Ext] safeTransferFrom #

+ [Int] IERC721Receiver
  - [Ext] onERC721Received #

+ ERC721Holder (IERC721Receiver)
  - [Pub] onERC721Received #

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ PancakeProfile (AccessControl, ERC721Holder)
  - [Pub] <Constructor> #

- [Ext] createProfile #
- [Ext] pauseProfile #
- [Ext] updateProfile #
- [Ext] reactivateProfile #
- [Ext] addNftAddress #
  - modifiers: onlyOwner
- [Ext] claimFee #
  - modifiers: onlyOwner
- [Ext] updateNumberCake #
  - modifiers: onlyOwner
- [Ext] updateCakeToken #
  - modifiers: onlyOwner
- [Ext] getUserProfile
- [Ext] getUserStatus

($) = payable function
= non-constant function

WEXReferral functions details

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

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

+ [Lib] SafeMath
  - [Int] sqrt
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul

  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [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] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ [Int] IWedexReferral
  - [Ext] recordReferral #
  - [Ext] recordReferralCommission #
  - [Ext] getReferrer
  - [Ext] addTotalFund #
  - [Ext] reduceTotalFund #
  - [Ext] getTeam
  - [Ext] totalFund

+ [Int] IWexProfile
  - [Ext] getUserStatus

+ WEXReferral (IWedexReferral, Ownable)
  - [Pub] <Constructor> #
  - [Pub] noLoop #
  - [Pub] recordReferral #
    - modifiers: onlyOperator
  - [Pub] recordReferralCommission #
    - modifiers: onlyOperator
  - [Pub] addTotalFund #
    - modifiers: onlyOperator
  - [Pub] reduceTotalFund #
    - modifiers: onlyOperator
  - [Pub] setMaxloop #
    - modifiers: onlyOperator
  - [Ext] addBlacklist #
    - modifiers: onlyOwner
  - [Ext] removeReferrer #

- modifiers: onlyOwner
- [Pub] getReferrer
- [Pub] isVip
- [Ext] setTotalFund #
  - modifiers: onlyOperator
- [Pub] getTeam
- [Pub] setWexProfile #
  - modifiers: onlyOwner
- [Pub] setVipRequirement #
  - modifiers: onlyOwner
- [Ext] updateMigration #
- [Pub] migration #
  - modifiers: onlyOperator
- [Ext] updateOperator #
  - modifiers: onlyOwner
- [Ext] drainBEP20Token #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

WEDEX TOKEN V2 functions details

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

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

+ [Lib] SafeMath
  - [Int] sqrt
  - [Int] tryAdd
  - [Int] trySub

  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [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] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ ReentrancyGuard
  - [Int] <Constructor> #

+ BEP20 (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] getOwner
  - [Pub] name
  - [Pub] decimals
  - [Pub] symbol
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #

  - [Int] _approve #
  - [Int] _burnFrom #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

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

+ [Int] IUniswapV2Pair
  - [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 #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #

- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Factory
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #
- [Ext] setFeeToSetter #

+ Wedex (BEP20)
- [Pub] <Constructor> #
  - modifiers: BEP20
- [Pub] mint #
  - modifiers: onlyMinter
- [Int] _transfer #
  - modifiers: antiWhale
- [Prv] isContract
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap,transferTaxFree
- [Prv] swapTokensForEth #
- [Ext] setBusdAddress #
  - modifiers: onlyOwner
- [Ext] setBlacklist #
  - modifiers: onlyOwner
- [Ext] setWhitelist #
  - modifiers: onlyOwner
- [Ext] setExpectedPrice #
  - modifiers: onlyOwner
- [Ext] setAllowanceDiff #
  - modifiers: onlyOwner
- [Pub] getWexPrice
- [Pub] maxTransferAmount
- [Pub] isExcludedFromAntiWhale
- [Pub] presaleLocked
- [Ext] <Fallback> ($)
- [Pub] updateTransferTaxRate #
  - modifiers: onlyOperator
- [Pub] updateBurnRate #
  - modifiers: onlyOperator
- [Pub] updateMaxTransferAmountRate #
  - modifiers: onlyOperator
- [Pub] updateMinAmountToLiquify #
  - modifiers: onlyOperator
- [Pub] setExcludedFromAntiWhale #
  - modifiers: onlyOperator
- [Pub] updateSwapAndLiquifyEnabled #
  - modifiers: onlyOperator
- [Pub] updateWedexSwapRouter #
  - modifiers: onlyOperator

- [Pub] recoverLostBNB #
  - modifiers: onlyOperator
- [Pub] recoverLostTokensExceptOurTokens #
  - modifiers: onlyOperator
- [Pub] activateTrading #
  - modifiers: onlyOperator
- [Pub] operator
- [Pub] transferOperator #
  - modifiers: onlyOperator
- [Pub] setMinter #
  - modifiers: onlyOwner
- [Ext] delegates
- [Ext] delegate #
- [Ext] delegateBySig #
- [Ext] getCurrentVotes
- [Ext] getPriorVotes
- [Int] _delegate #
- [Int] _moveDelegates #
- [Int] _writeCheckpoint #
- [Int] safe32
- [Int] getChainId

($) = payable function
= non-constant function

WedexChef functions details

+ [Int] IWedexReferral
  - [Ext] recordReferral #
  - [Ext] recordReferralCommission #
  - [Ext] getReferrer
  - [Ext] addTotalFund #
  - [Ext] reduceTotalFund #
  - [Ext] getTeam
  - [Ext] totalFund

+ [Int] IWexProfile
  - [Ext] getUserStatus

+ WEXReferral (IWedexReferral, Ownable)
  - [Pub] <Constructor> #
  - [Pub] noLoop #
  - [Pub] recordReferral #
    - modifiers: onlyOperator
  - [Pub] recordReferralCommission #
    - modifiers: onlyOperator
  - [Pub] addTotalFund #
    - modifiers: onlyOperator
  - [Pub] reduceTotalFund #
    - modifiers: onlyOperator
  - [Pub] setMaxloop #
    - modifiers: onlyOperator
  - [Ext] addBlacklist #

    - modifiers: onlyOwner
  - [Ext] removeReferrer #
    - modifiers: onlyOwner
  - [Pub] getReferrer
  - [Pub] isVip
  - [Ext] setTotalFund #
    - modifiers: onlyOperator
  - [Pub] getTeam
  - [Pub] setWexProfile #
    - modifiers: onlyOwner
  - [Pub] setVipRequirement #
    - modifiers: onlyOwner
  - [Ext] updateMigration #
  - [Pub] migration #
    - modifiers: onlyOperator
  - [Ext] updateOperator #
    - modifiers: onlyOwner
  - [Ext] drainBEP20Token #
    - modifiers: onlyOwner

+ ReentrancyGuard
  - [Int] <Constructor> #

+ BEP20 (Context, IBEP20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] getOwner
  - [Pub] name
  - [Pub] decimals
  - [Pub] symbol
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _burnFrom #

+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #

- [Ext] swapTokensForExactTokens #
- [Ext] swapExactETHForTokens ($)
- [Ext] swapTokensForExactETH #
- [Ext] swapExactTokensForETH #
- [Ext] swapETHForExactTokens ($)
- [Ext] quote
- [Ext] getAmountOut
- [Ext] getAmountIn
- [Ext] getAmountsOut
- [Ext] getAmountsIn

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

+ [Int] IUniswapV2Pair
- [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 #
- [Ext] MINIMUM_LIQUIDITY
- [Ext] factory
- [Ext] token0
- [Ext] token1
- [Ext] getReserves
- [Ext] price0CumulativeLast
- [Ext] price1CumulativeLast
- [Ext] kLast
- [Ext] mint #
- [Ext] burn #
- [Ext] swap #
- [Ext] skim #
- [Ext] sync #
- [Ext] initialize #

+ [Int] IUniswapV2Factory
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair #
- [Ext] setFeeTo #

- [Ext] setFeeToSetter #

+ Wedex (BEP20)
  - [Pub] <Constructor> #
    - modifiers: BEP20
  - [Pub] mint #
    - modifiers: onlyMinter
  - [Int] _transfer #
    - modifiers: antiWhale
  - [Prv] isContract
  - [Prv] swapAndLiquify #
    - modifiers: lockTheSwap,transferTaxFree
  - [Prv] swapTokensForEth #
  - [Ext] setBusdAddress #
    - modifiers: onlyOwner
  - [Ext] setBlacklist #
    - modifiers: onlyOwner
  - [Ext] setWhitelist #
    - modifiers: onlyOwner
  - [Ext] setExpectedPrice #
    - modifiers: onlyOwner
  - [Ext] setAllowanceDiff #
    - modifiers: onlyOwner
  - [Pub] getWexPrice
  - [Pub] maxTransferAmount
  - [Pub] isExcludedFromAntiWhale
  - [Pub] presaleLocked
  - [Ext] <Fallback> ($)
  - [Pub] updateTransferTaxRate #
    - modifiers: onlyOperator
  - [Pub] updateBurnRate #
    - modifiers: onlyOperator
  - [Pub] updateMaxTransferAmountRate #
    - modifiers: onlyOperator
  - [Pub] updateMinAmountToLiquify #
    - modifiers: onlyOperator
  - [Pub] setExcludedFromAntiWhale #
    - modifiers: onlyOperator
  - [Pub] updateSwapAndLiquifyEnabled #
    - modifiers: onlyOperator
  - [Pub] updateWedexSwapRouter #
    - modifiers: onlyOperator
  - [Pub] recoverLostBNB #
    - modifiers: onlyOperator
  - [Pub] recoverLostTokensExceptOurTokens #
    - modifiers: onlyOperator
  - [Pub] activateTrading #
    - modifiers: onlyOperator
  - [Pub] operator
  - [Pub] transferOperator #
    - modifiers: onlyOperator
  - [Pub] setMinter #
    - modifiers: onlyOwner
  - [Ext] delegates
  - [Ext] delegate #

  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

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

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

+ [Lib] SafeMath
  - [Int] sqrt
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [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] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ [Int] IMigratorChef
  - [Ext] migrate #

+ WedexChef (Ownable, ReentrancyGuard)
  - [Pub] <Constructor> #
  - [Ext] poolLength
  - [Pub] add #
    - modifiers: onlyOwner
  - [Pub] set #
    - modifiers: onlyOwner
  - [Pub] getMultiplier
  - [Pub] getWexPrice
  - [Pub] getLPPrice
  - [Ext] pendingWedex
  - [Pub] canHarvest
  - [Pub] massUpdatePools #
  - [Pub] updatePool #
  - [Pub] getLeader
  - [Pub] getUpperVip
  - [Pub] deposit #
    - modifiers: nonReentrant
  - [Pub] setNewChefAddress #
    - modifiers: onlyOwner
  - [Pub] setIsMigrating #
    - modifiers: onlyOwner
  - [Int] payDirectCommission #
  - [Pub] withdraw #
    - modifiers: nonReentrant
  - [Pub] withdrawInvestment #
    - modifiers: nonReentrant
  - [Pub] getFreeInvestmentAmount
  - [Pub] emergencyWithdraw #
    - modifiers: nonReentrant
  - [Int] payOrLockupPendingWedex #
  - [Int] safeWedexTransfer #
  - [Pub] setReferDepth #
    - modifiers: onlyOwner
  - [Pub] setReferralCommissionTier #
    - modifiers: onlyOwner
  - [Pub] setWexLpAddress #

    - modifiers: onlyOwner
  - [Pub] setDevAddress #
  - [Pub] setFeeAddress #
  - [Ext] setPancakeRouterV2 #
    - modifiers: onlyOwner
  - [Ext] setBusdAddress #
    - modifiers: onlyOwner
  - [Pub] setWedexReferral #
    - modifiers: onlyOwner
  - [Pub] setEmergencyWithdrawEnable #
    - modifiers: onlyOwner
  - [Prv] getReferralCommissionRate
  - [Int] payReferralCommission #

($) = 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.	Low issues
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 high severity issues found.

Low Severity Issues

1. Block gas limit

Issue:

`add(uint256 _allocPoint, ...)`, `set(uint256 _pid, ...)` could invoke `massUpdatePools()` function, that can fail due to block gas limit if the pool size is too big.

Issue:

`Migration()` function that can fail due to block gas limit if the referrer's array size is too big.

2. `add` function issue

Issue:

If some LP token is added to the contract twice using function add, then the total amount of reward in function `updatePool` will be incorrect.

Recommendation:

Add the mapping from address to bool and check that same address will not be added twice.

Notes:

- There is sending tokens to the dead address in overridden _transfer functions, instead of burning them in token contract.
- WedexChef has transfer and deposit fee.
- burnBunny function has only external access modifier.

Owner privileges:

- WEXReferral:
  - Owner can add/remove addresses in blacklist.
  - Owner can remove referrers.
  - Owner can change wexProfile.
  - Owner can change vipRequirement.
  - Owner can change operator of the contract.
  - Owner can drain tokens that are sent to the referral contract which is useful for withdrawing tokens sent by mistake to the contract.
  - Owner can change the operator of the referral contract.
  - Operator can migrate.
  - Operator can change referral commission rate.
  - Operator can add/remove total funds.
  - Operator can change maximumLoop.
  - Operator can change total funds.
- WexNFT:
  - Owner can mint any amount of token.
  - Owner can burn.
  - Owner can change bunnyNames.
- WedexChef:
  - Owner can change newChefAddress.
  - Owner can enable/disable isMigrating value.
  - Owner can change referDepth and referralCommissionTier.
  - Owner can change wexLPAddress and pancakeRouterV2.
  - Owner can change busdAddress and wedexReferral.
  - Owner can enable/disable emergencyLockingWithdrawEnable value.
- Wedex:
  - Owner and Minter can mint any amounts of tokens.
  - Owner can blacklists/whitelist addresses.
  - Owner can change busdAddress.
  - Owner can change expectedPrice and alowanceDiff values.
  - Owner can add/remove minters.
- PancakeProfile:
  - Owner can add NFT addresses.
  - Owner can withdraw cake token.
  - Owner can change cake number to register, update and reactivate.
  - Owner can change cake token address.
- NFTFactoryV6:
  - Owner can change wedexReferral contract.
  - Owner can change ownership of pancakeBunnies.
  - Owner can withdraw cake token.
  - Owner can change tierCommisionrate and referDepth.
  - Owner can change and burn Bunny’s.
  - Owner can change bunny price.
  - Owner can change start and end block numbers.
  - Owner can change cake token address.

Conclusion

Smart contracts contain low severity issues and owner privileges. 10% of rewards also adds to devAddress. The further transfers and operations with the funds raise are not related to this particular contract.

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.