TechRate

AUDIT COMPANY

# Smart Contract Security Audit

TechRate

July, 2021

# Audit Details

Audited project

**HONEYPAD**

Deployer address

**0x13d5573a0936f72d20152ba779281247669188c7**

Client contacts:

**HONEYPAD team**

Blockchain

**Binance Smart Chain**

Project website:

[https://honeypad.io](https://honeypad.io)

# 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 HONEYPAD to perform an audit of smart contracts:**

https://bscscan.com/address/0xdb607c61aaa2a954bf1f9d117953f12d6c319e15#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.

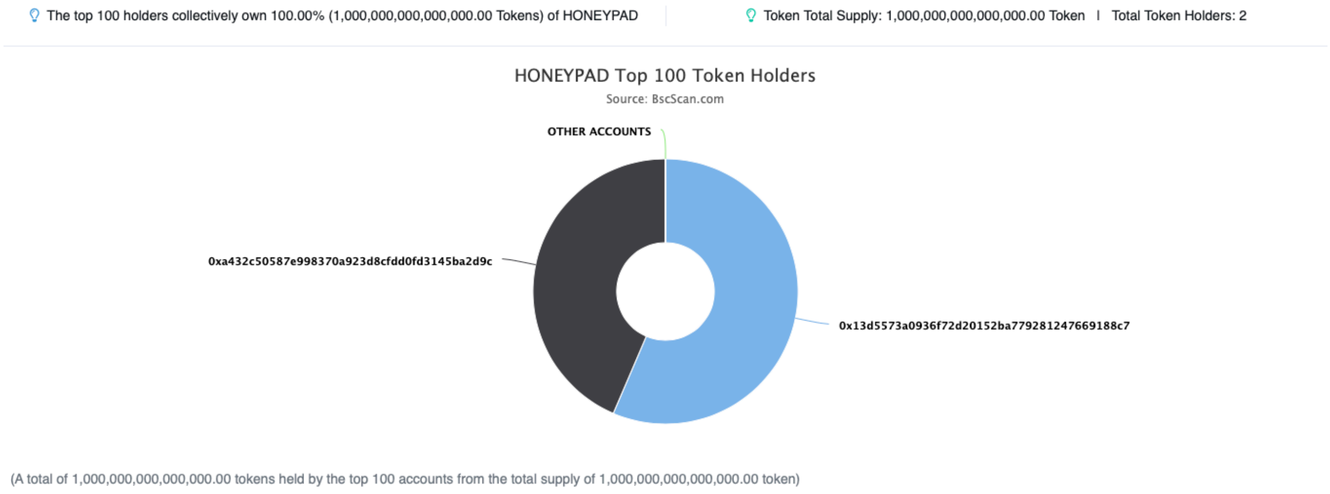
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

# Contracts Details

## Token contract details for 27.08.2021

| | |
|---|---|
| Contract name | HoneyPad |
| Contract address | 0xdb607c61Aaa2a954Bf1f9d117953F12d6c319E15 |
| Total supply | 1,000,000,000,000,000 |
| Token ticker | $HONEY |
| Decimals | 9 |
| Token holders | 2 |
| Transactions count | 8 |
| Top 100 holders dominance | 100.00% |
| Marketing fee | 5 |
| Dividend fee | 5 |
| BuyBack fee | 5 |
| Buyback wallet | 0x9392c6fbe6a7be44f491d597217cea634c916ff6 |
| Dividend tracker | 0x2c65debf3c7671cb79340bddb0893fbb0d5accd7 |
| Pancake pair | 0x60b06d471113d3e64ff10be62ddcceedd1895d61 |
| Contract deployer address | 0x13d5573a0936f72d20152ba779281247669188c7 |
| Contract's current owner address | 0x13d5573a0936f72d20152ba779281247669188c7 |

# HONEYPAD Token Distribution



The top 100 holders collectively own 100.00% (1,000,000,000,000,000.00 Tokens) of HONEYPAD

Token Total Supply: 1,000,000,000,000,000.00 Token | Total Token Holders: 2

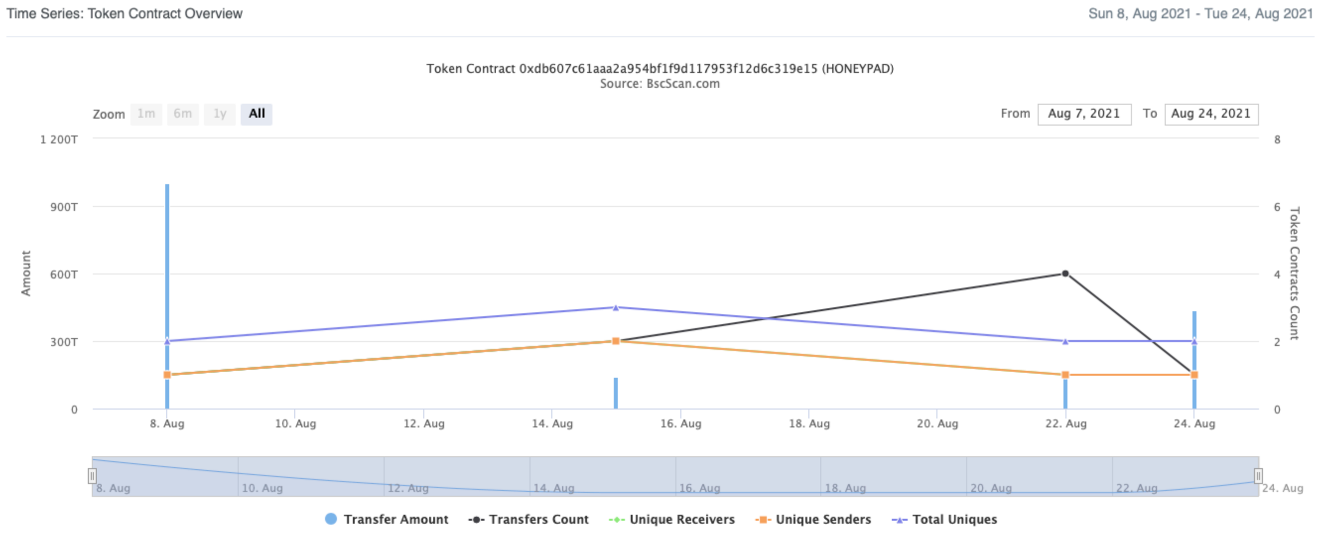
HONEYPAD Top 100 Token Holders

Source: BscScan.com

OTHER ACCOUNTS
0xa432c50587e998370a923d8cfdd0fd3145ba2d9c
0x13d5573a0936f72d20152ba779281247669188c7

(A total of 1,000,000,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000,000.00 token)

# HONEYPAD Contract Interaction Details



Time Series: Token Contract Overview

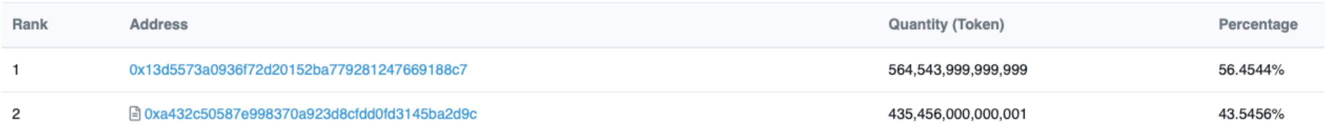
Sun 8, Aug 2021 - Tue 24, Aug 2021

Token Contract 0xdb607c61aaa2a954bf1f9d117953f12d6c319e15 (HONEYPAD)

Source: BscScan.com

From: Aug 7, 2021 To: Aug 24, 2021

# HONEYPAD Top 10 Token Holders



| Rank | Address | Quantity (Token) | Percentage |
|---|---|---|---|
| 1 | 0x13d5573a0936f72d20152ba779281247669188c7 | 564,543,999,999,999 | 56.4544% |
| 2 | 🗎 0xa432c50587e998370a923d8cfdd0fd3145ba2d9c | 435,456,000,000,001 | 43.5456% |

# Contract functions details

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

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

 + [Int] IERC20Metadata (IERC20)
   - [Ext] name
   - [Ext] symbol
   - [Ext] decimals

 +  ERC20 (Context, IERC20, IERC20Metadata)
   - [Pub] <Constructor> #
   - [Pub] name
   - [Pub] symbol
   - [Pub] decimals
   - [Pub] totalSupply
   - [Pub] balanceOf
   - [Pub] transfer #
   - [Pub] allowance
   - [Pub] approve #
   - [Pub] transferFrom #
   - [Pub] increaseAllowance #
   - [Pub] decreaseAllowance #
   - [Int] _transfer #
   - [Int] _mint #
   - [Int] _burn #
   - [Int] _approve #
   - [Int] _beforeTokenTransfer #
   - [Int] _afterTokenTransfer #

 + [Lib] SafeMathUint
   - [Int] toInt256Safe

 + [Lib] SafeMathInt
   - [Int] mul
   - [Int] div
   - [Int] sub
   - [Int] add
   - [Int] toUint256Safe

 + [Lib] SafeMath
   - [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] IterableMapping
  - [Pub] get
  - [Pub] getIndexOfKey
  - [Pub] getKeyAtIndex
  - [Pub] size
  - [Pub] set #
  - [Pub] remove #

+ [Int] DividendPayingTokenOptionalInterface
  - [Ext] withdrawableDividendOf
  - [Ext] withdrawnDividendOf
  - [Ext] accumulativeDividendOf

+ [Int] DividendPayingTokenInterface
  - [Ext] dividendOf
  - [Ext] distributeDividends ($)
  - [Ext] withdrawDividend #

+ DividendPayingToken (ERC20, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface)
  - [Pub] <Constructor> #
    - modifiers: ERC20
  - [Ext] <Fallback> ($)
  - [Pub] distributeDividends ($)
  - [Pub] withdrawDividend #
  - [Int] _withdrawDividendOfUser #
  - [Pub] dividendOf
  - [Pub] withdrawableDividendOf
  - [Pub] withdrawnDividendOf
  - [Pub] accumulativeDividendOf
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _setBalance #

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

+ [Int] IPancakeFactory

```
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
  - [Ext] setFeeToSetter #

+ [Int] IPancakePair
  - [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] IPancakeRouter01
  - [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] IPancakeRouter02 (IPancakeRouter01)
    - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
    - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
    - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
    - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
    - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

 +  HoneyPad (ERC20, Ownable)
    - [Pub] <Constructor> #
       - modifiers: ERC20
    - [Pub] updatePancakeRouter #
       - modifiers: onlyOwner
    - [Ext] <Fallback> ($)
    - [Pub] excludeFromAllLimits #
       - modifiers: onlyOwner
    - [Ext] setSwapTokensAtAmount #
       - modifiers: onlyOwner
    - [Ext] setMaxTxAmount #
       - modifiers: onlyOwner
    - [Ext] setMaxHoldingAmount #
       - modifiers: onlyOwner
    - [Ext] setRestrictionPeriod #
       - modifiers: onlyOwner
    - [Pub] getAccountPeriodSellVolume #
    - [Prv] removeAccSells #
    - [Pub] getAccountSells
    - [Ext] setBuyFees #
       - modifiers: onlyOwner
    - [Ext] setSellFees #
       - modifiers: onlyOwner
    - [Ext] setWallets #
       - modifiers: onlyOwner
    - [Ext] setCanTransferBeforeTradingIsEnabled #
       - modifiers: onlyOwner
    - [Ext] excludeFromDividends #
       - modifiers: onlyOwner
    - [Ext] isExcludedFromDividends
    - [Pub] updateDividendTracker #
       - modifiers: onlyOwner
    - [Pub] excludeFromFees #
       - modifiers: onlyOwner
    - [Pub] excludeFromPeriodLimit #
       - modifiers: onlyOwner
    - [Pub] excludeFromMaxTxLimit #
       - modifiers: onlyOwner
    - [Pub] excludeMultipleAccountsFromFees #
       - modifiers: onlyOwner
    - [Pub] updateGasForProcessing #
       - modifiers: onlyOwner
    - [Ext] updateClaimWait #
       - modifiers: onlyOwner
```

  - [Ext] updateMinimumTokenBalanceForDividends #
    - modifiers: onlyOwner
  - [Ext] getClaimWait
  - [Ext] getTotalDividendsDistributed
  - [Pub] isExcludedFromFees
  - [Pub] isExcludedFromMaxTxLimit
  - [Pub] isExcludedFromMaxHoldLimit
  - [Pub] isExcludedFromPeriodLimit
  - [Pub] withdrawableDividendOf
  - [Pub] dividendTokenBalanceOf
  - [Ext] getAccountDividendsInfo
  - [Ext] getAccountDividendsInfoAtIndex
  - [Ext] processDividendTracker #
  - [Ext] claim #
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfDividendTokenHolders
  - [Ext] setSwapIsEnabled #
    - modifiers: onlyOwner
  - [Ext] setTradingIsEnabled #
    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Prv] swapTokensForEth #
  - [Prv] swapAndDistributeBNB #
  - [Pub] withdrawStuckTokens #
    - modifiers: onlyOwner

+  HoneyPadDividendTracker (DividendPayingToken, Ownable)
  - [Pub] <Constructor> #
    - modifiers: DividendPayingToken
  - [Int] _transfer
  - [Pub] withdrawDividend
  - [Ext] excludeFromDividends #
    - modifiers: onlyOwner
  - [Ext] updateClaimWait #
    - modifiers: onlyOwner
  - [Ext] updateMinimumTokenBalanceForDividends #
    - modifiers: onlyOwner
  - [Ext] getLastProcessedIndex
  - [Ext] getNumberOfTokenHolders
  - [Pub] getAccount
  - [Pub] getAccountAtIndex
  - [Prv] canAutoClaim
  - [Ext] setBalance #
    - modifiers: onlyOwner
  - [Pub] process #
  - [Pub] processAccount #
    - 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. | 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 excludeMultipleAccountsFromFees() uses the loop to exclude multiple accounts from fees. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- The functions removeAccSells() and getAccountPeriodSellVolume() uses the loop to iterate through sell's history. Functions will be aborted with OUT_OF_GAS exception if there will be a long sells list.

**Recommendation**:

Be careful about array length.

## Notes:

- Dividend tracker may be changed. So that logic of setBalance and other functions could be another and not audited.
- In _withdrawDividendOfUser function gas value is constant, and could not be changed if needed.
- There is double checking from address to be excluded from period limit in transfer function.

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

- Owner can change router address.
- Owner can exclude from all limits.
- Owner can change swapTokensAtAmount value.
- Owner can change maxTransactionAmount and maxHoldingAmount values.
- Owner can change restriction period.
- Owner can change buy and sell fees.
- Owner can change buyback and marketing wallet addresses.
- Owner can add in canTransferBeforeTradingIsEnabled exclusion.
- Owner can exclude from dividends.
- Owner can change dividend tracker.
- Owner can exclude from fees, maxTX and period limit.
- Owner can change gas for processing.
- Owner can update claimWait value.
- Owner can change minimum balance for dividends.
- Owner can enable swap and trading.
- Owner can withdraw ERC20 tokens.

# 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 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.*