Smart Contract Security Audit

Audit details:

Audited project:	Polybull Finance
Deployer address	0x268162b846D623Cac4C756AE1D383cbf17c2558e
Blockchain:	Matic
Project website:	https://polybull.finance

May, 2021
TechRate

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 Polybull Finance to perform an audit of smart contracts:

- *https://explorer-mainnet.maticvigil.com/address/0x138B9C072879219CD6Ef2D6d9E0D179B3396F07b/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0xd3fbFBB1233576d295EA7e948b349079F89a920b/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0x478E8DE0E2b9ab00C1D1E0461EA00096183b1803/contracts*
- *https://explorer-mainnet.maticvigil.com/address/0x664E854F5429C03AEFa81961Dd0bdB6dE7B99Ab1/contracts*

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 16.05.2021.

Contract name:	Polybull Finance
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x138B9C072879219CD6Ef2D6d9E0D179B3396F07b
Total supply:	1000000000000000000
Token ticker:	BULL
Decimals:	18
Token holders:	44
Transactions count:	413
Contract deployer address:	0x268162b846D623Cac4C756AE1D383cbf17c2558e
Contract’s current owner address:	0x664E854F5429C03AEFa81961Dd0bdB6dE7B99Ab1

Polybull Finance top 10 token holders

0xFFF72f6C640C347726FF2b318E4dccD6B28862B2
0.540027836448895442 BULL 54.0028%

0xA9adda56845662af63A16a02AFe2512E0bABE4F0
0.091832103528190999 BULL 9.1832%

0xd59551a032C70C47AB202Eb834500a07C1d31d98
0.074102804344577711 BULL 7.4103%

0x5Ab85C90BEE2cBa351277b879834E30ABaed95Cb
0.039307811250965001 BULL 3.9308%

0x8dcC92e697F4a0cD0e2dbC497f4e0978D61369Fc
0.03153439751358393 BULL 3.1534%

0x3271572717D2Fe117eDeBd32B730b5f2028aE01c
0.025267342052354671 BULL 2.5267%

0x0000000000000000000000000000000000000dEaD
0.023278049333367833 BULL 2.3278%

0x664E854F5429C03AEFa81961Dd0bdB6dE7B99Ab1
0.021298404280937318 BULL 2.1298%

0x58b80FF10946cFdA425c81F8619c6C1615A517B5
0.018789594910414591 BULL 1.8790%

0xC22e3559c1460B6A845bE5fb6945d176503Fb708
0.018128345558891817 BULL 1.8128%

MasterChef contract details for 16.05.2021.

Contract name:	MasterChef
Compiler version:	v0.6.12+commit.27d51765
Contract address:	0x664E854F5429C03AEFa81961Dd0bdB6dE7B99Ab1
Deployer address:	0x268162b846D623Cac4C756AE1D383cbf17c2558e
Fee address:	0x268162b846D623Cac4C756AE1D383cbf17c2558e
Dev address:	0x268162b846D623Cac4C756AE1D383cbf17c2558e
BULL contract address:	0x138B9C072879219CD6Ef2D6d9E0D179B3396F07b
BULL per block:	1000000000000000000
Contract owner address:	0x268162b846D623Cac4C756AE1D383cbf17c2558e
Pool length:	11
Start block:	14608888
Total alloc point:	28000
Bonus multiplier:	1

MasterChef functions outline

+ [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

+ [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
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ [Lib] SafeBEP20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #

  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ [Int] IBullReferral
  - [Ext] recordReferral #
  - [Ext] getReferrer

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

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

+ BullToken (BEP20)
  - [Pub] mint #

    - modifiers: onlyOwner
  - [Int] _transfer #
  - [Ext] delegates
  - [Ext] delegate #
  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

+ MasterChef (Ownable, ReentrancyGuard)
  - [Pub] <Constructor> #
  - [Ext] poolLength
  - [Pub] add #
    - modifiers: onlyOwner
  - [Pub] set #
    - modifiers: onlyOwner
  - [Pub] getMultiplier
  - [Ext] pendingBull
  - [Pub] massUpdatePools #
  - [Pub] updatePool #
  - [Pub] deposit #
    - modifiers: nonReentrant
  - [Pub] withdraw #
    - modifiers: nonReentrant
  - [Pub] emergencyWithdraw #
    - modifiers: nonReentrant
  - [Int] safeBullTransfer #
  - [Pub] setDevAddress #
  - [Pub] setFeeAddress #
  - [Pub] updateEmissionRate #
  - [Pub] setBullReferral #
    - modifiers: onlyOwner
  - [Pub] setReferralCommissionRate #
    - modifiers: onlyOwner
  - [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.	Medium 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

1. Wrong burning

Issue:

There is sending tokens to the dead address in overridden _transfer functions, instead of burning them in the token contract.

Recommendation:

There should be a burn instead of sending to the dead address.

Low Severity Issues

1. Block gas limit

Issue:

The `updateEmissionRate` function can fail due to the block gas limit if the pool 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 the same address will not be added twice.

Owner privileges

Transfer onwership of BullToken to Masterchef
https://explorer-mainnet.maticvigil.com/tx/0x26e81e14e27f06d044b7a92e931c05386df75693cf84558f893da96712367731/internal-transactions

Transfer ownership of MasterChef to Timelock
https://explorer-mainnet.maticvigil.com/tx/0x06fa1010169c59a9bbf1981c31c7b3041791f19a50b41fec622bff6b392e0d08/internal-transactions

- ❏ Owner can change the bull referral contract.
- ❏ Owner can change the referral commission rate.
- ❏ Owner can change the deposit fee and pool details.

- ❏ Owner can drain tokens that are sent to the referral contract which is useful for withdrawing tokens sent by mistake to the contract.

Conclusion

Smart contracts do not contain high severity issues!

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.