HackSafe

Smart Contract Security Audit Report

BASE REWARD TOKEN

February 2023

Security Status

★★★★☆

www.hacksafe.io

Audit Details

Audited project
BASE REWARD TOKEN

Deployer address
0xd7655a7584910be99dc20a8b2975591e9fdc0d90

Client contacts
BASE REWARD TOKEN Team

Blockchain
Binance smart chain

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) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by BASE REWARD TOKEN to perform an audit of smart contracts:

- https://bscscan.com/token/0x0d499B25Bce7Aa72bb6c50E434E2Ed26fE1e785D#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 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.

Contract Details

Token contract details for 04.02.2023

Token Type	: DEFI
Contract name	: BaseRewardToken
Contract address	: 0x0d499B25Bce7Aa72bb6c50E434E2Ed26fE1e785D
Total supply	: 12,000,000
Token ticker	: BRT
Decimals	: 18
Token Holders	: 3,936
Transactions count	: 59,481
Compiler version	: v0.6.12+commit.27d51765
Contract deployer address	: 0xd7655a7584910be99dc20a8b2975591e9fdc0d90
Owner address	: 0x000000000000000000000000000000000000dead

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **“Secure”.** This token contract does not contain owner control as ownership has been renounce, which do make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here 

We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 2 low.

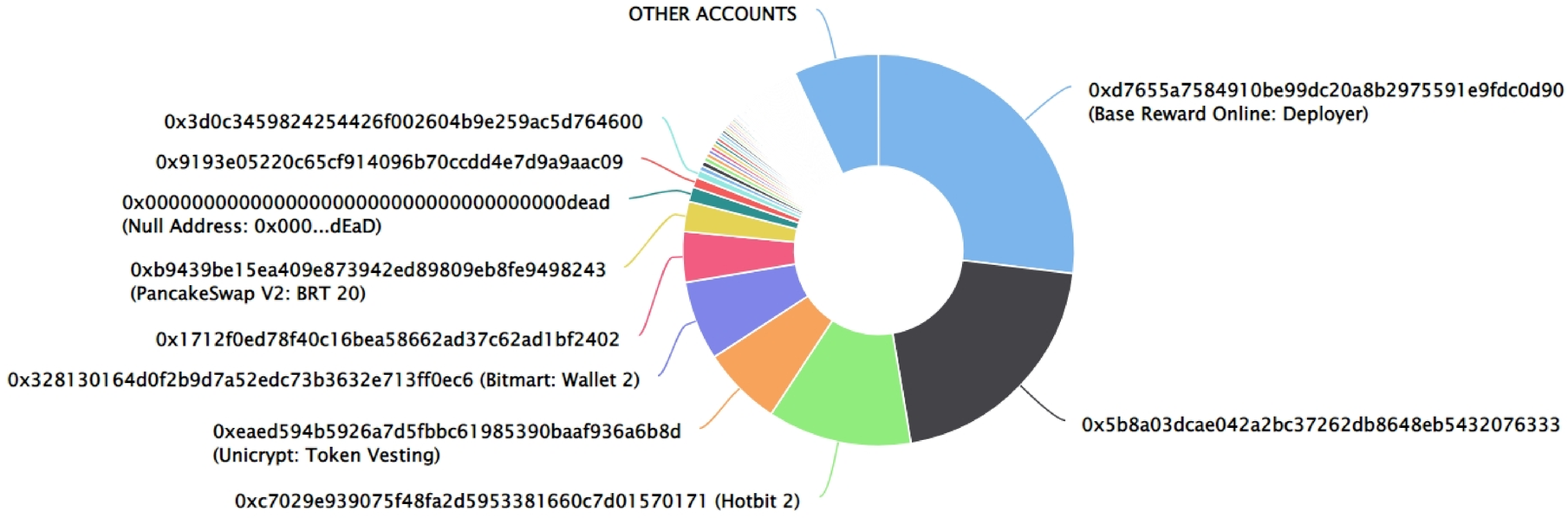
BASE REWARD TOKEN Distribution

The top 100 holders collectively own 92.98%
(11,157,320.07 Tokens) of BASE REWARD TOKEN

Token Total Supply: 12,000,000.00 Token | Total Token Holders: 3,936

BASE REWARD TOKEN Top 100 Token Holders

Source: BscScan.com



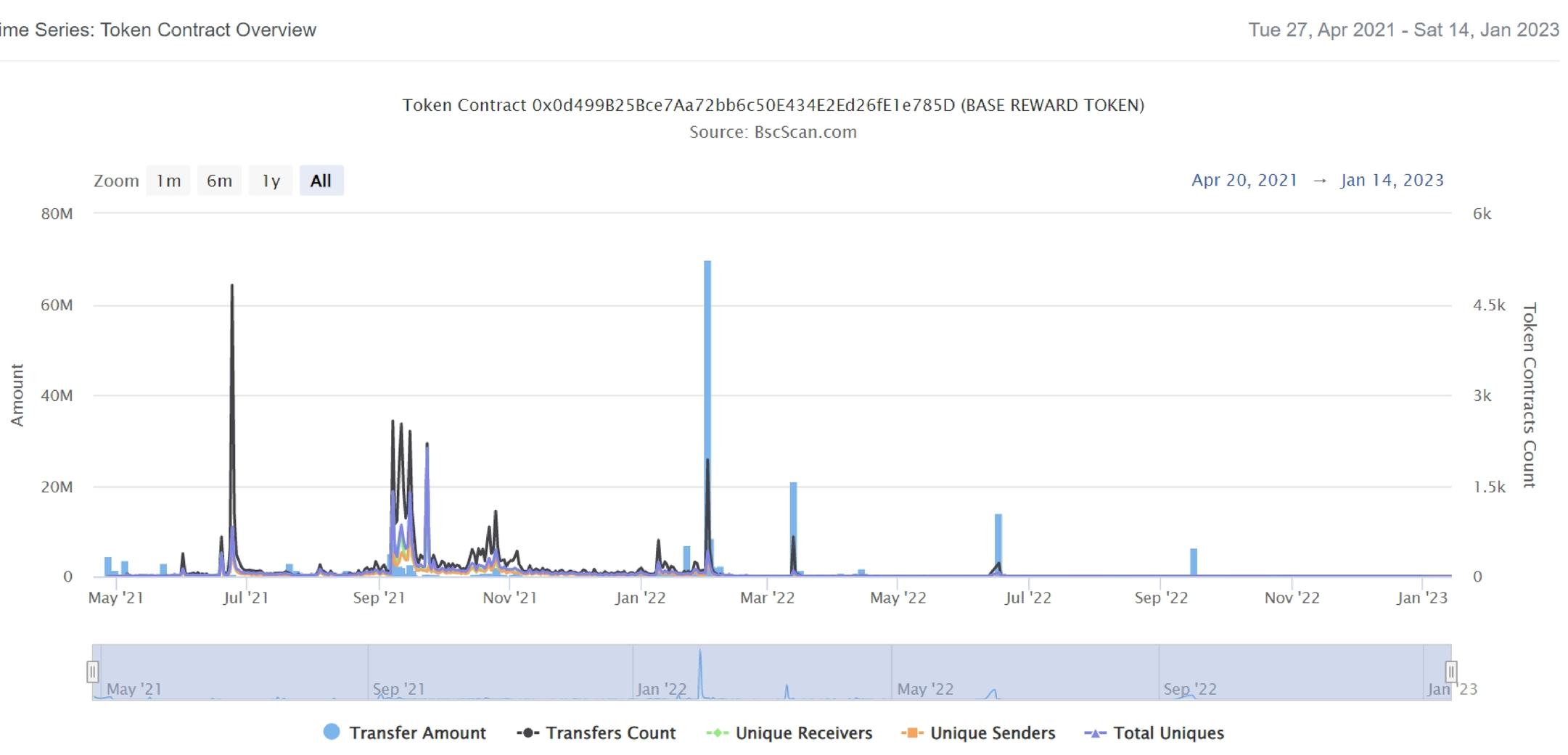
BASE REWARD TOKEN Top 20 Token Holders

(A total of 11,157,320.07 tokens held by the top 100 accounts from the total supply of 12,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Base Reward Online: Deployer	3,228,245.220008650959295881	26.9020%
2	0x5b8a03dcae042a2bc37262db8648eb5432076333	2,454,775.678527702634055736	20.4565%
3	Hotbit 2	1,426,373.882474038521011172	11.8864%
4	Unicrypt: Token Vesting	792,000	6.6000%
5	Bitmart: Wallet 2	782,263.014393631905830064	6.5189%
6	0x1712f0ed78f40c16bea58662ad37c62ad1bf2402	500,000	4.1667%
7	PancakeSwap V2: BRT 20	297,567.199906315395814967	2.4797%
8	Null Address: 0x000...dEaD	145,650.529435243781061743	1.2138%
9	0x9193e05220c65cf914096b70ccdd4e7d9a9aac09	101,147.650714840268862932	0.8429%
10	0x3d0c3459824254426f002604b9e259ac5d764600	74,179.668906933093322926	0.6182%
11	0x00bd3d0244a1fb5a690dba95b3945af37ddc324e	50,815.1	0.4235%
12	0x9bfc409b715e7d8d53f9e00d3c783a32151cd461	49,000	0.4083%
13	0x29127a5f27eff4f7ec1c0d20e5c0fbbc20be76ce	46,839.065214577360742029	0.3903%
14	0x628e5ef174af2d00f9237fbd58cfbed1d23f5695	42,284.016825059911290405	0.3524%
15	0xea763a7a06e397047dd71ba227f3a089809e6abd	38,979.155532333350891085	0.3248%
16	0x060a33a0df3953b31b887d9efdcf4d9f5b05daa9	37,788.942886984948876739	0.3149%
17	0x987a9965dd6b69416868410c749952ed13fb40d9	36,672.869301599758181773	0.3056%
18	0x4882740a7b6b55bfdc61fa0cb519d5b9b204c333	35,072.120858931847106462	0.2923%
19	0x2f7bc652f22ced241f2ce84839aa4e7aa28de60d	34,260.754153190907363148	0.2855%
20	0xeb0e37be2afda44a729142ddbb203e3b0b767180	30,836.242001809621394121	0.2570%

BASE REWARD TOKEN Distribution

BASE REWARD TOKEN Contract Overview



Contract functions details

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

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

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

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

+[Int] IBEP20
    -[Ext] totalSupply
    -[Ext] balanceOf
    -[Ext] transfer #
    -[Ext] allowance
    -[Ext] approve #
    -[Ext] transferFrom #

+BEP20 (Context, IBEP20)
    -[Pub] <Constructor>#

Contract functions details

-[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] _setupDecimals #
-[Int] _beforeTokenTransfer #

+BEP20Capped (BEP20)
    -[Pub] <Constructor>#
    -[Pub] cap
    -[Int] _beforeTokenTransfer #

+BaseRewardToken (BEP20Capped, Ownable)
    -[Pub] <Constructor>#
      - modifiers: BEP20,BEP20Capped
    -[Ext] <Fallback >($)
    -[Pub] mint #
      - modifiers: onlyOwner
    -[Pub] burn #
      - modifiers: onlyOwner

($) = payable function
= non-constant function

Issues Checking Status

No.	Title	Status
1.	Compiler error	Passed
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Low issue
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Low issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.
- **High Severity Issues**
  No high severity issue found.
- **Medium Severity Issues**
  No medium severity issue found.
- **Low Severity Issues**
  Two low severity issue found.

1. Old compiler version

- **Description**
  Contract has been deployed using too old solidity version.
- **Recommendation**
  It is advisable to deploy contract using any of the latest version of solidity

2. Abuse of authority (Not an issue while owner is renounced)

- **Issue:**
  The function burn() can be called only by the owner of the BaseRewardToken contract. Owner can burn any amount of tokens from any address without any approve.
- **Recommendation**
  Do not let anybody access users' balances.

Centralization

Owner Privileges :

- BASE REWARD TOKEN Contract:
    - Owner can mint under capitalization.
    - Owner can burn.

This smart contract has some functions which can be executed by the admin (Owner) only. If the admin wallet private key would be compromised, then it would not create trouble, as smart contract ownership has been renounced.Following are the owner function:

- mint
- burn

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe 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.