



Smart Contract Security Audit Report

BabyBoxer

November 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

BabyBoxer



Deployer address

0xc549d47ccfec53912c92b3ddab4fdbbc868e5163f



Client contacts

BabyBoxer 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 BabyBoxer to perform an audit of smart contracts:

- <https://bscscan.com/token/0xeD7ed82D5A0f1B363309223975f899E7BEd5Fea6#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 understood 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.

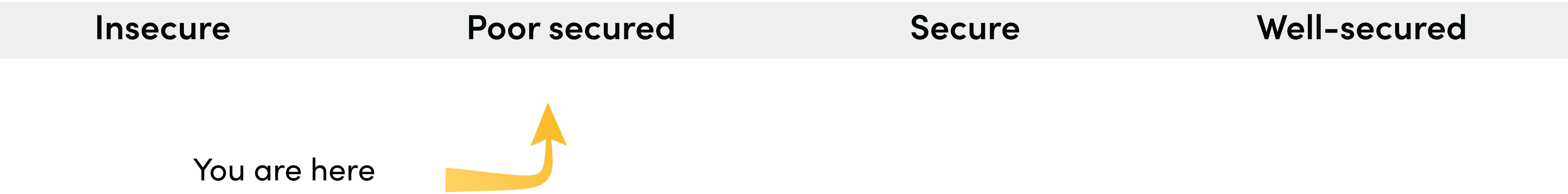
Contract Details

Token contract details for 18.11.2022

Token Type	: DEFI
Contract name	: BabyBoxer
Contract address	: 0xeD7ed82D5A0f1B363309223975f899E7BEd5Fea6
Total supply	: 888,888,888,888,888
Token Ticker	: BBoxer
Decimals	: 9
Token Holders	: 7,896
Transactions count	: 49,292
Compiler version	: v0.8.6+commit.11564f7e
Contract deployer address	: 0xc549d47ccfec53912c92b3ddab4fdbbc868e5163f
Owner address	: 0x36fba56fb56ba6aab0c8f0cbb268a689bfc55b5

Audit Summary

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



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, 1 high, 0 medium and 1 low.

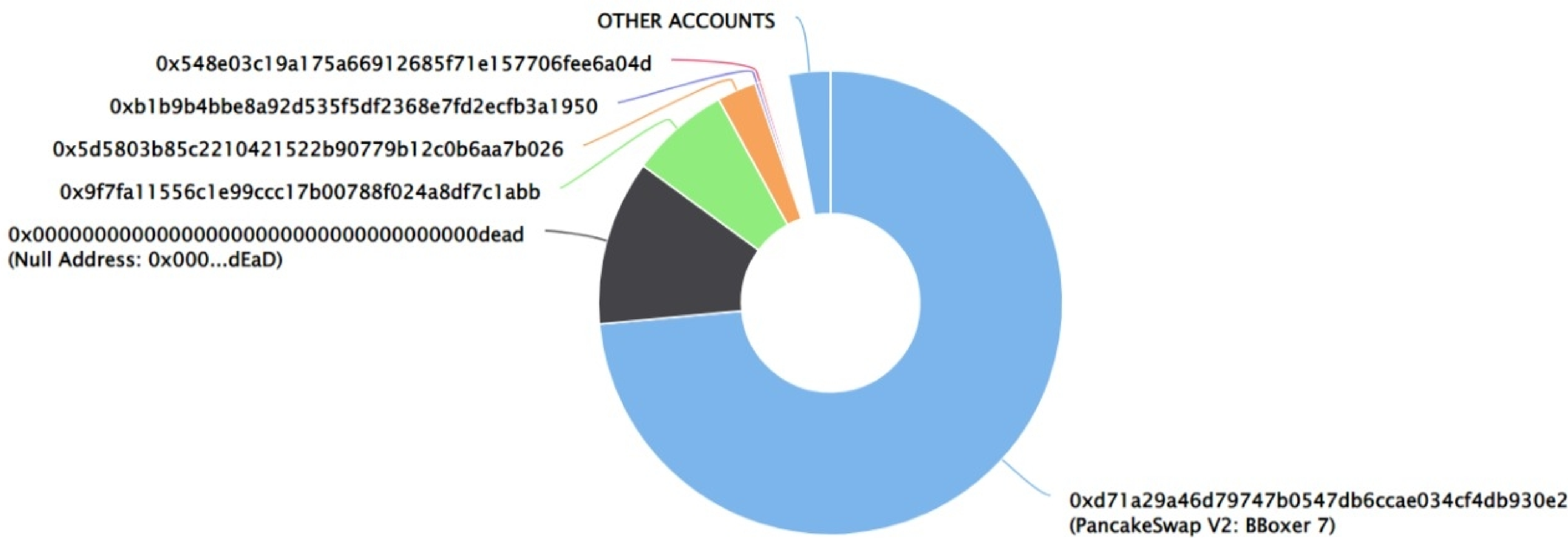
BabyBoxer Distribution

💡 The top 100 holders collectively own 97.09% (863,004,018,830,639.00 Tokens) of BabyBoxer

💡 Token Total Supply: 888,888,888,888,888.00 Token | Total Token Holders: 7,896




BabyBoxer Top 100 Token Holders

Source: BscScan.com



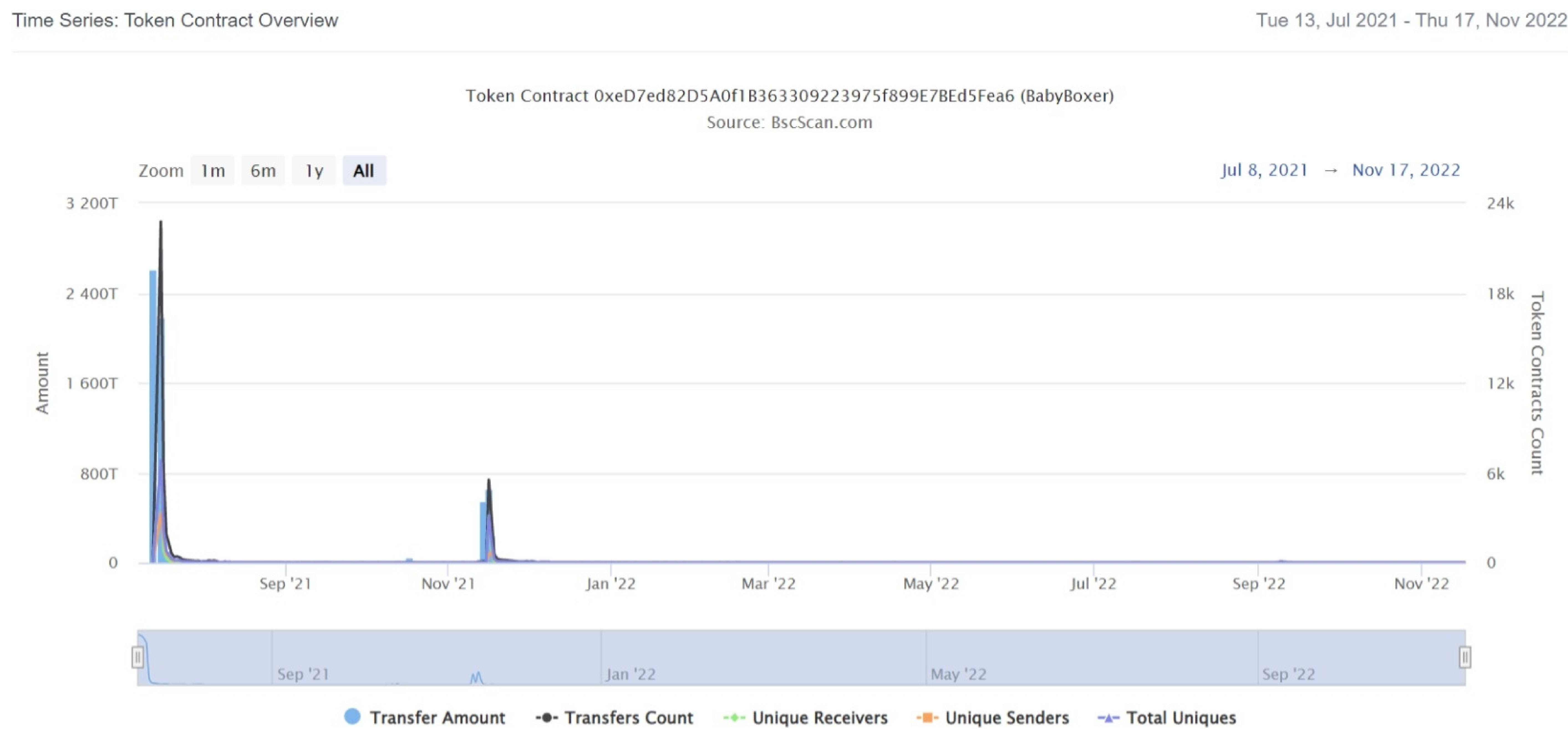
BabyBoxer Top 20 Token Holders

(A total of 863,004,018,830,639.00 tokens held by the top 100 accounts from the total supply of 888,888,888,888,888.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 PancakeSwap V2: BBoxer 7	653,724,211,622,260.599980801	73.5440%
2	Null Address: 0x000...dEaD	102,379,717,539,658.885239278	11.5177%
3	 0x9f7fa11556c1e99ccc17b00788f024a8df7c1abb	61,709,003,280,535.811406529	6.9423%
4	 0x5d5803b85c2210421522b90779b12c0b6aa7b026	24,230,688,878,376.078869268	2.7260%
5	0xb1b9b4bbe8a92d535f5df2368e7fd2ecfb3a1950	2,020,794,384,189.821211863	0.2273%
6	0x548e03c19a175a66912685f71e157706fee6a04d	2,000,059,663,719.643054952	0.2250%
7	0x34c9de1e914928ebd6bd1908b50730937bdfad0b	1,500,298,347,909.853308212	0.1688%
8	0xd3094df925c015bc8443fff8b0480626e308d8a0	1,000,038,834,652.327211246	0.1125%
9	0x6a51df2657fec916c3e1084afd0df638ff27575c	710,709,414,106.754170587	0.0800%
10	0xc2f5b4441a295cb49205d7006a2fb32ba4066495	474,881,112,088.609249881	0.0534%
11	0xf1b90353862937a9e9b115732f56d3bc833b2b8e2	445,448,395,440.721580871	0.0501%
12	0x268f524b66ea876dca692959e25217dc0160f8b9	399,646,787,604.008300676	0.0450%
13	0x1d5cef60b2b4576d77fc59f6a8bd5d8214e450f3	359,202,907,274.11662405	0.0404%
14	0xf14d8e450dc9fdef1400d937bd652f962303eeee	330,594,442,572.498281792	0.0372%
15	0xa09cf0d9d977addc0694ed9d071ac50e37e5d3a3	320,529,138,731.122614966	0.0361%
16	0x4bd85a91c70e4112ecf9059d39cd94642f6ebb3a	320,320,796,499.397365658	0.0360%
17	0xa89965e3db632c6ae1e8d377c21b20f86c578ec0	308,921,671,856.391443172	0.0348%
18	0x25c466e3cde07a9aaf610a9012f150ba2c2b580e	307,990,329,653.847795463	0.0346%
19	0x4d11e2c8257ab03525cb0af80cea894115312b34	289,469,178,736.136659736	0.0326%
20	0x1b9c6965d549add307cfcb8086651885b8a740f3	282,614,137,861.3441906	0.0318%

BabyBoxer Distribution

BabyBoxer Contract Overview



Contract functions details

BabyBoxer.sol

+BabyBoxer (BEP20Base, Ownable)

- <constructor >
- <receive> \$
- [Pub] balanceOf
- [Pub] isExcluded
- [Pub] addToExcludeList #
 - modifiers: onlyOwner
- [Pub] removeFromExcludeList #
 - modifiers: onlyOwner
- [Pub] getAccumulatedAmount
- [Pub] claimAccumulatedAmount #
 - modifiers: lockSwap
- [Int] _transfer #
- [Pvt] _swapAndDistribute #
 - modifiers: lockSwap
- [Pvt] _swapContractTokensForBNB #
- [Pvt] _transferStandard #
- [Pvt] _transferToExcluded #
- [Pvt] _transferFromExcluded #
- [Pvt] _transferBothExcluded #
- [Pvt] _getValues
- [Pvt] _getTValues
- [Pvt] _getRValues
- [Pvt] _getRate
- [Pvt] _tokenFromReflection
- [Pvt] _distributeFees

BEP20Base.sol

+BEP20Base (Context, IBEP20)

- [Pub] name
- [Pub] symbol
- [Pub] decimals
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] increaseAllowance #
- [Pub] decreaseAllowance #

Contract functions details

- [Pub] approve #
- [Pub] transfer #
- [Pub] transferFrom #
- [Int] _approve #
- [Int] _transfer #

Context.sol

+Context

- [Int] _msgSender

IBEP20.sol

+ [Int] IBEP20

- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

IEcosystem.sol

+ [Int] IEcosystem

- [Ext] isWhitelisted

ISwapV2.sol

+ [Int] ISwapV2Factory

- [Ext] createPair

+ [Int] ISwapRouterV2

- [Ext] WETH
- [Ext] factory
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens \$
- [Ext] addLiquidityETH #

Ownable.sol

+Ownable (Context)

- <constructor>
- [Pub] owner

Contract functions details

-[Pub] renounceOwnership #

-modifiers: onlyOwner

-[Pub] transferOwnership #

-modifiers: onlyOwner

-[Pvt] _setOwner #

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
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.	High issue
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.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed
20.	Too old version	Passed

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

One high severity issue found.

1. Timestamp dependence.

- **Description**

The contract have used `block.timestamp` many times in some modifiers such as `_swapContractTokensForBNB` as the miners here can manipulate the smart contract in order to attack the contract.

- **Recommendation**

We advise you to not use `block.timestamp` in your contract and apply the 15-second rule which says that If the scale of your time-dependent event can vary by 15 seconds and maintain integrity, it is safe to use a `block.timestamp`.

✔ Medium Severity Issues

No medium severity issue found.

✔ Low Severity Issues

One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version `^0.8.6` the contract should contain the following line:

```
pragma solidity 0.8.6;
```

Centralization

Owner Privileges :

- BabyBoxer Contract:
 - Owner can transfer and renounce ownership.
 - Owner can add and remove from exclude list.

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 create trouble as smart contract ownership has not been renounced. Following are Admin functions:

- transferOwnership
- renounceOwnership
- addToexcludelist
- removeFromExcludeList

Conclusion

Smart contract contains low and high 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.