



Smart Contract Security Audit Report

Lawtoken

August 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

Lawtoken



Deployer address

0xe080232063e75e29b022B390fdF350032E758A77



Client contacts

Lawtoken



Blockchain

Binance Smart Chain



Website

<https://lawtoken.finance/>

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 Lawtoken to perform an audit of smart contract:

- <https://bscscan.com/address/0xb84aa25ae8e33962de303b21af3d36d4f75d9ea9#code>

The purpose of the audit was to achieve the

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understood 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 02.08.2022

Token Type	: BEP-20
Contract name	: Lawtoken
Contract address	: 0xB84aA25ae8e33962de303b21aF3d36d4f75D9eA9
Compiler version	: v0.6.8+commit.0bbfe453
Total supply	: 500,000,000
Token Ticker	: LAW
Decimals	: 18
Token Holders	: 46,086
Top 100 token holder's	: 99.60%
Transactions count	: 80,289
Contract deployer address	: 0xe080232063e75e29b022B390fdF350032E758A77
Owner address	: 0xe080232063e75e29b022B390fdF350032E758A77

Social profiles

Twitter Profile	: https://twitter.com/Lawtoken1
Telegram Profile	: https://t.me/LawTokenChannel
Coinmarketcap profile	: https://coinmarketcap.com/currencies/law-token/
Coingecko profile	: https://www.coingecko.com/en/coins/law-token/

Audit Summary

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

Insecure	Poor	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, 1 medium and 0 low and some very low-level issues. These issues are not critical ones.

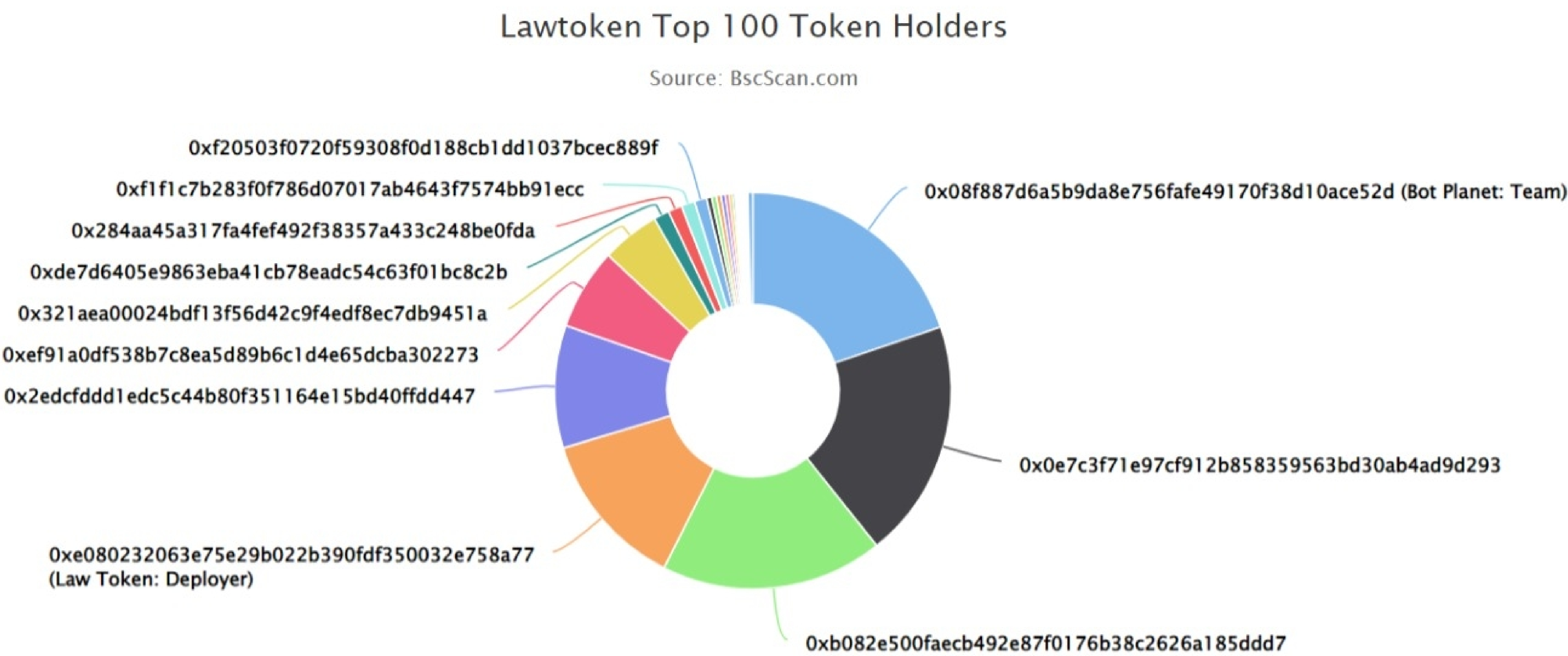
Lawtoken Token Distribution

 The top 100 holders collectively own 99.60% (497,985,110.73 Tokens) of Lawtoken

 Token Total Supply: 500,000,000.00 Token


|

Total Token Holders: 46,083



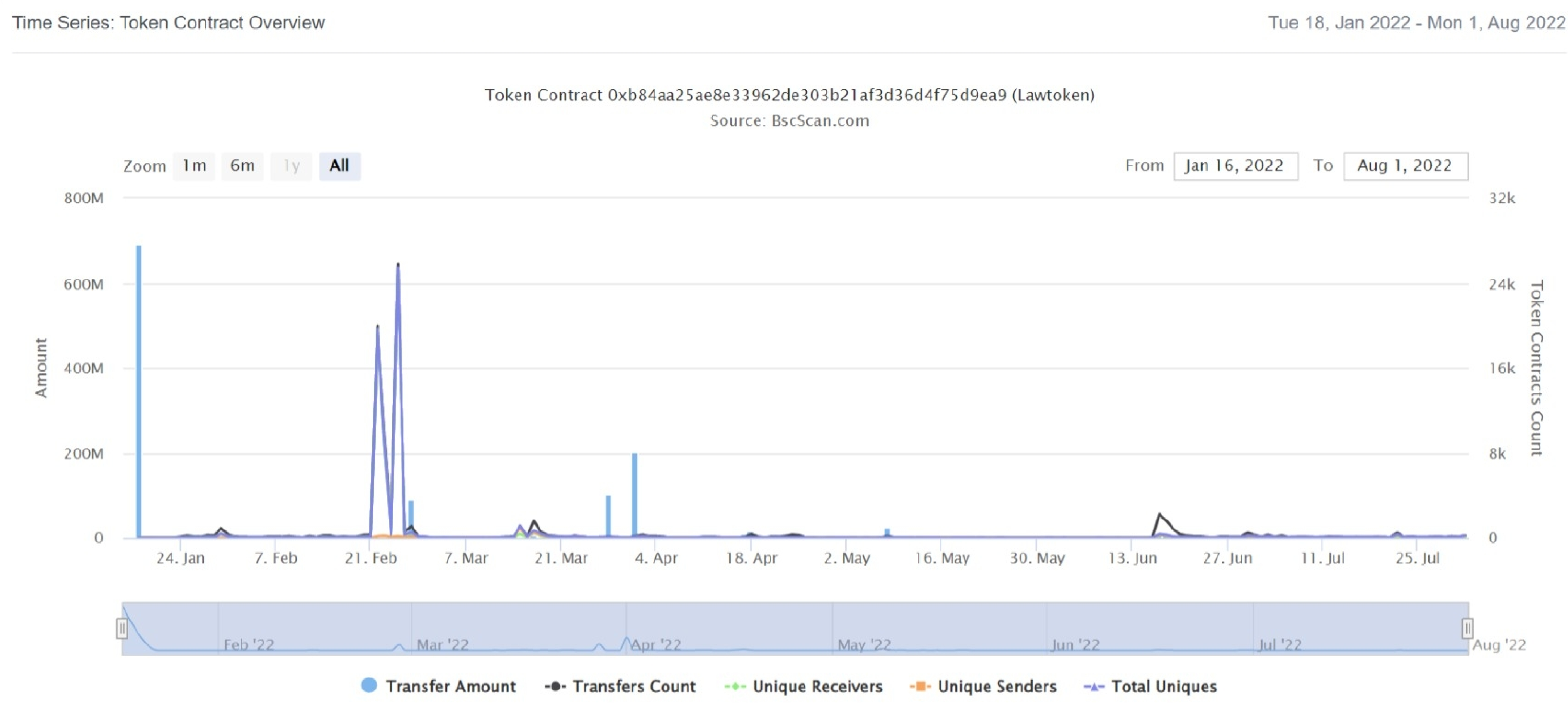
Lawtoken Token Top 20 Token Holders

(A total of 497,985,110.73 tokens held by the top 100 accounts from the total supply of 500,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	 Bot Planet: Team	99,000,000	19.8000%
2	0x0e7c3f71e97cf912b858359563bd30ab4ad9d293	97,381,754.147138183862620462	19.4764%
3	0xb082e500faecb492e87f0176b38c2626a185ddd7	90,717,992.033628334727913343	18.1436%
4	Law Token: Deployer	64,612,370.981097521107886206	12.9225%
5	0x2edcfddd1edc5c44b80f351164e15bd40ffdd447	50,000,000	10.0000%
6	0xef91a0df538b7c8ea5d89b6c1d4e65dcba302273	33,125,000	6.6250%
7	0x321aea00024bdf13f56d42c9f4edf8ec7db9451a	23,779,320	4.7559%
8	0xde7d6405e9863eba41cb78eadc54c63f01bc8c2b	6,344,318.544938586909747658	1.2689%
9	0x284aa45a317fa4fef492f38357a433c248be0fda	5,625,000	1.1250%
10	0xf1f1c7b283f0f786d07017ab4643f7574bb91ecc	5,625,000	1.1250%
11	0xf20503f0720f59308f0d188cb1dd1037bcec889f	5,000,000	1.0000%
12	0xbd3f67369c60fd71b3d51bb5a4f1befd4520c5f6	2,010,755.397284936860735528	0.4022%
13	0xe9d2afff18f08375d5b7a8a804e272b6c81ceb9f	1,962,483.241241825516102893	0.3925%
14	0xecc04c5cd6f8d45005ceb078118fb53c34901bc	1,856,698.749323786299678599	0.3713%
15	0x27be084d6099597434561e2ec5e110f96c5b95a0	1,765,750.888354252932903828	0.3532%
16	0x2ec1fd18a42f9d3aef874bd53a7fe973d512e49a	1,497,120	0.2994%
17	0x625fd872cba136584858a6bc959166dfa804a003	1,445,260.00000000000024	0.2891%
18	CoinTool: Donate	1,000,000	0.2000%
19	0xa8883ffed1dc4f49b58138585dca60ef0cb5bf1a	718,082.8	0.1436%
20	0xa2d3949e23546c6ac1631e5ebcbb9dcc8a21aa3a	696,030.9359999999976	0.1392%

Lawtoken Token Distribution

Lawtoken Token Contract Overview



Contract functions details

+[Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] sub
- [Int] div

+ Lawtoken

- [Pub] <constructor>
- [Pub] name
- [Pub] owner
- [Pub] symbol
- [Int] _msgSender
- [Pub] decimals
- [Pub] cap
- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] allowance
- [Pub] authNum #
- [Pub] transferOwnership #
- [Pub] setAuth #
 - modifiers: onlyOwner
- [Int] _mint#
- [Int] _approve #
- [Pub] transferFrom #
- [Pub] clearBNB
 - modifiers: onlyOwner
- [Pub] mint #
 - modifiers: onlyOwner
- [Int] _transfer #
- [Pub] setVAr #
 - modifiers: onlyOwner
- [Pub] transfer #
- [Pub] getBlock #
- [Pub] LAWTOKENairdrop \$
- [Pub] allocationAirdrop #
 - modifiers: onlyOwner
- [Pub] LAWTOKENpresale \$

Contract functions details

(\$) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	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.	Medium issue
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

No high severity issue found.

✔ Medium Severity Issues

One medium severity issues found.

1. Wrong minting

- **Issue**

The function `_mint()` do not increase total supply but increases cap value.

- **Recommendation**

Increase total supply under cap value not vice versa.

✔ Low Severity Issues

No low severity issue found..

Notes:

`_buyBnb` and `_airdropBnb` used only for checking.

Centralization

Owner privileges:

- Lawtoken Contract:
 - Owner can change contracts presets.
 - Owner can withdraw contract BNBs.
 - Owner can mint tokens below `_totalSupply` value.

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 but smart contract ownership has been renounced. Following are Admin functions functions:

- Setauth
- Clearbnb
- Mint
- Setvar
- Allocationairdrop

Conclusion

Smart contract contains medium 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.