



Building the Futuristic **Blockchain** Ecosystem

SECURITY AUDIT REPORT

LEGO

TOKEN OVERVIEW

Risk Findings

Severity	Found
● High	1
● Medium	0
● Low	0
● Informational	0

Centralization Risks

Owner Privileges	Description
● Can Owner Set Taxes >25% ?	Not Detected
● Owner needs to enable trading ?	Yes, owner needs to enable trades
● Can Owner Disable Trades ?	Not Detected
● Can Owner Mint ?	Not Detected
● Can Owner Blacklist ?	Not Detected
● Can Owner set Max Wallet amount ?	Not Detected
● Can Owner Set Max TX amount ?	Not Detected

TABLE OF CONTENTS

02	Token Overview	
03	Table of Contents	
04	Overview	
05	Contract Details	
06	Audit Methodology	
07	Vulnerabilities Checklist	
08	Risk Classification	
09	Inheritance Trees	
10	Function Details	
14	Testnet Version	
16	Manual Review	
18	About Expelee	
19	Disclaimer	

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	Passed With High Risk
KYC Verification	-
Audit Date	14 August 2023

CONTRACT DETAILS

Name: Lego Token

Symbol: LEGO

Decimals: 18

Network: BSC

Token Address: 0xE9b822C175FeB50D748Fae5D19cB56f6c0907F1C

Owner: 0xef42330ff981A40695756f73FeE553E8b5aC416F

Deployer: 0xef42330ff981A40695756f73FeE553E8b5aC416F

Token Supply: 1,000,000,000

Checksum:

dc464b3fa5034ade74a424dd18af9760a247d54c

Testnet version:

<https://testnet.bscscan.com/token/0xdA49191e8100610d6358e90100Fa99B56592A340>

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

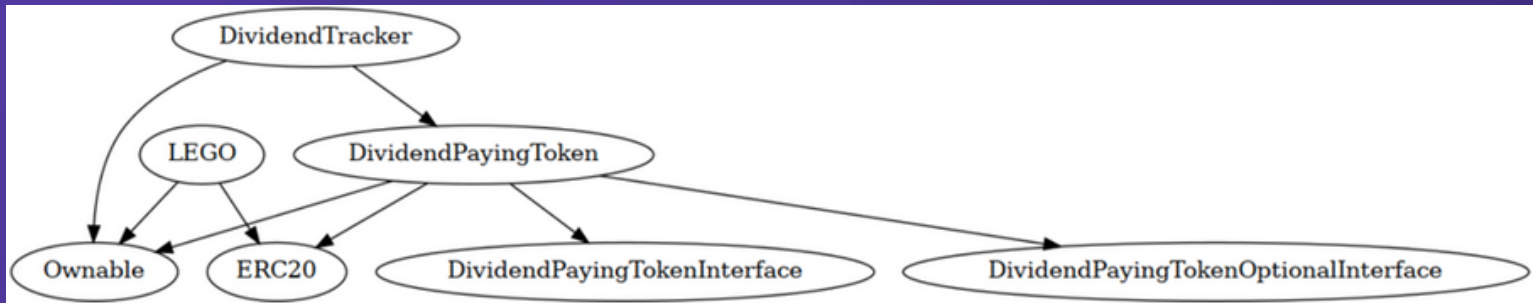
Low Risk

Issues on this level are minor details and warnings that can remain unfixed.

Informational

Issues on this level are minor details and warnings that can remain unfixed.

INHERITANCE TREES



FUNCTION DETAILS

Contract	Type	Bases			
----- ----- ----- ----- -----					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
SafeMathInt Library					
L	mul	Internal	🔒		
L	div	Internal	🔒		
L	sub	Internal	🔒		
L	add	Internal	🔒		
L	abs	Internal	🔒		
L	toUint256Safe	Internal	🔒		
SafeMathUint Library					
L	toInt256Safe	Internal	🔒		
IterableMapping Library					
L	get	Internal	🔒		
L	getIndexOfKey	Internal	🔒		
L	getKeyAtIndex	Internal	🔒		
L	size	Internal	🔒		
L	set	Internal	🔒	●	
L	remove	Internal	🔒	●	
IUniswapV2Factory Interface					
L	feeTo	External	!		NO !
L	feeToSetter	External	!		NO !
L	getPair	External	!		NO !
L	allPairs	External	!		NO !
L	allPairsLength	External	!		NO !
L	createPair	External	!	●	NO !
L	setFeeTo	External	!	●	NO !
L	setFeeToSetter	External	!	●	NO !
IUniswapV2Pair Interface					
L	name	External	!		NO !
L	symbol	External	!		NO !

FUNCTION DETAILS

```

| decimals | External ! | NO ! | | |
| totalSupply | External ! | NO ! |
| balanceOf | External ! | NO ! |
| allowance | External ! | NO ! |
| approve | External ! | ● NO ! |
| transfer | External ! | ● NO ! |
| transferFrom | External ! | ● NO ! |
| DOMAIN_SEPARATOR | External ! | NO ! |
| PERMIT_TYPEHASH | External ! | NO ! |
| nonces | External ! | NO ! |
| permit | External ! | ● NO ! |
| MINIMUM_LIQUIDITY | External ! | NO ! |
| factory | External ! | NO ! |
| token0 | External ! | NO ! |
| token1 | External ! | NO ! |
| getReserves | External ! | NO ! |
| price0CumulativeLast | External ! | NO ! |
| price1CumulativeLast | External ! | NO ! |
| kLast | External ! | NO ! |
| mint | External ! | ● NO ! |
| burn | External ! | ● NO ! |
| swap | External ! | ● NO ! |
| skim | External ! | ● NO ! |
| sync | External ! | ● NO ! |
| initialize | External ! | ● NO ! |
|||||
| **IUniswapV2Router01** | Interface | |||
| factory | External ! | NO ! |
| WETH | External ! | NO ! |
| addLiquidity | External ! | ● NO ! |
| addLiquidityETH | External ! | 🟢 NO ! |
| removeLiquidity | External ! | ● NO ! |
| removeLiquidityETH | External ! | ● NO ! |
| removeLiquidityWithPermit | External ! | ● NO ! |
| removeLiquidityETHWithPermit | External ! | ● NO ! |
| swapExactTokensForTokens | External ! | ● NO ! |
| swapTokensForExactTokens | External ! | ● NO ! |
| swapExactETHForTokens | External ! | 🟢 NO ! |
| swapTokensForExactETH | External ! | ● NO ! |
| swapExactTokensForETH | External ! | ● NO ! |
| swapETHForExactTokens | External ! | 🟢 NO ! |
| quote | External ! | NO ! |
| getAmountOut | External ! | NO ! |
| getAmountIn | External ! | NO ! |
| getAmountsOut | External ! | NO ! |

```

FUNCTION DETAILS

```

| L | getAmountsIn | External ! | | NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! | ● | NO ! |
|
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🟢 | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
|||||
| **DividendPayingTokenInterface** | Interface | |||
| L | dividendOf | External ! | | NO ! |
| L | withdrawDividend | External ! | ● | NO ! |
|||||
| **DividendPayingTokenOptionalInterface** | Interface | |||
| L | withdrawableDividendOf | External ! | | NO ! |
| L | withdrawnDividendOf | External ! | | NO ! |
| L | accumulativeDividendOf | External ! | | NO ! |
|||||
| **DividendPayingToken** | Implementation | ERC20, Ownable, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface |||
| L | <Constructor> | Public ! | ● | ERC20 |
| L | distributeDividends | Public ! | ● | onlyOwner |
| L | withdrawDividend | Public ! | ● | NO ! |
| L | _withdrawDividendOfUser | Internal 🔒 | ● | |
| L | dividendOf | Public ! | | NO ! |
| L | withdrawableDividendOf | Public ! | | NO ! |
| L | withdrawnDividendOf | Public ! | | NO ! |
| L | accumulativeDividendOf | Public ! | | NO ! |
| L | _transfer | Internal 🔒 | ● | |
| L | _mint | Internal 🔒 | ● | |
| L | _burn | Internal 🔒 | ● | |
| L | _setBalance | Internal 🔒 | ● | |
|||||
| **DividendTracker** | Implementation | Ownable, DividendPayingToken |||
| L | <Constructor> | Public ! | ● | DividendPayingToken |
| L | _transfer | Internal 🔒 | | |
| L | withdrawDividend | Public ! | | NO ! |
| L | updateMinimumTokenBalanceForDividends | External ! | ● | onlyOwner |
| L | excludeFromDividends | External ! | ● | onlyOwner |
| L | updateClaimWait | External ! | ● | onlyOwner |
| L | setLastProcessedIndex | External ! | ● | onlyOwner |
| L | getLastProcessedIndex | External ! | | NO ! |
| L | getNumberOfTokenHolders | External ! | | NO ! |
| L | getAccount | Public ! | | NO ! |
| L | getAccountAtIndex | Public ! | | NO ! |
| L | canAutoClaim | Private 🔒 | | |

```

FUNCTION DETAILS

```

| L | setBalance | External | ! | ● | onlyOwner |
| L | process | Public | ! | ● | NO ! |
| L | processAccount | Public | ! | ● | onlyOwner |
|||||
| **LEGO** | Implementation | ERC20, Ownable |||
| L | <Constructor> | Public | ! | 🟢 | ERC20 |
| L | <Receive Ether> | External | ! | 🟢 | NO ! |
| L | withdrawStuckTokens | External | ! | ● | onlyOwner |
| L | withdrawStuckETH | External | ! | ● | onlyOwner |
| L | isContract | Internal | 🔒 | | |
| L | _setAutomatedMarketMakerPair | Private | 🔒 | ● | |
| L | setwhitelist | External | ! | ● | onlyOwner |
| L | iswhitelisted | Public | ! | | NO ! |
| L | changeMarketingWallet | External | ! | ● | onlyOwner |
| L | enableTrading | External | ! | ● | onlyOwner |
| L | _transfer | Internal | 🔒 | ● | |
| L | swapAndSendDividends | Private | 🔒 | ● | |
| L | setSwapTokensAtAmount | External | ! | ● | onlyOwner |
| L | updateGasForProcessing | Public | ! | ● | onlyOwner |
| L | updateMinimumBalanceForDividends | External | ! | ● | onlyOwner |
| L | updateClaimWait | External | ! | ● | onlyOwner |
| L | getClaimWait | External | ! | | NO ! |
| L | getTotalDividendsDistributed | External | ! | | NO ! |
| L | withdrawableDividendOf | Public | ! | | NO ! |
| L | dividendTokenBalanceOf | Public | ! | | NO ! |
| L | totalRewardsEarned | Public | ! | | NO ! |
| L | excludeFromDividends | External | ! | ● | onlyOwner |
| L | getAccountDividendsInfo | External | ! | | NO ! |
| L | getAccountDividendsInfoAtIndex | External | ! | | NO ! |
| L | processDividendTracker | External | ! | ● | NO ! |
| L | claim | External | ! | ● | NO ! |
| L | claimAddress | External | ! | ● | onlyOwner |
| L | getLastProcessedIndex | External | ! | | NO ! |
| L | setLastProcessedIndex | External | ! | ● | onlyOwner |
| L | getNumberOfDividendTokenHolders | External | ! | | NO ! |

```

Legend

Symbol	Meaning
●	Function can modify state
🟢	Function is payable

TESTNET VERSION

Adding Liquidity ✓

Tx:

<https://testnet.bscscan.com/tx/0xf183d107a8c491e3bf91b748752588812c17518a9474c573b018a00052f9ca5d>

=====

Buying when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x7f64c89a61135bc9fd63151b96e35acbccee528e3360ee66a9dc14b93ed98967>

=====

Selling when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xcdd66fc63164d476f381ae724c3f343fd13236fee64f1940405d5bd0f842fa6e>

=====

Transferring when excluded from fees ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x6833f65fbd99691a360dc6b1b994785fd865f12430de1ca0ef4606a8ee5d89ac>

=====

Buying ✓

Tx (4% tax):

<https://testnet.bscscan.com/tx/0x624ca09fafdff64cd14c31e4c96cb7529c564439302c55f7f018bc0b992e7967>

TESTNET VERSION

Selling ✓

Tx (4% tax):

<https://testnet.bscscan.com/tx/0xf04d78ba1341717bdac0173de9fdb5e21bbf3c2371cbf6be01ac460b8e8803a0>

=====

Transferring ✓

Tx (4% tax):

<https://testnet.bscscan.com/tx/0x20658120b3093fb1d697fbba8408fb86672594a1cb8bea1c63dc6d69c04d9abe>

=====

Internal swap (ETH sent to marketing wallet and rewards were sent to dividend tracker)



Tx:

<https://testnet.bscscan.com/tx/0xf04d78ba1341717bdac0173de9fdb5e21bbf3c2371cbf6be01ac460b8e8803a0>

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk cateogroies:

High

Medium

Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
Likelihood				

HIGH RISK FINDING

Category: **Centralization**

Subject: Trades are disabled by default

Status: Open

Impact: **High**

Overview:

The contract has been structured such that all trading is disabled by default, necessitating the contract owner's manual intervention to enable trading. This can lead to a situation where, if trades remain disabled, token holders won't be able to buy, sell, or trade their tokens, causing a severe impact on the token's usability and market liquidity.

```
function enableTrading() external onlyOwner {  
  require(!tradingEnabled, "Trading is already enabled");  
  tradingEnabled = true;  
  startTradingBlock = block.number;  
}
```

Suggestion:

To mitigate this risk, it is recommended that trading be enabled before the token presale. This can be achieved by invoking the "enableTrading" function or by transferring ownership of the contract to a third-party that has established trust with the community, such as a Certified SAFU developer. This reduces the concentration of power and the potential for malicious actions, thereby promoting a more decentralized and fair environment for all participants.

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

 www.expelee.com



expeleeofficial



expelee



Expelee



expelee



expelee_official



expelee-co

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

The logo for Expelee, featuring the word "expelee" in a stylized font. The "ex" is in white, and "pelee" is in orange. The letters are bold and modern.

Building the Futuristic **Blockchain Ecosystem**