

expelee

Building the Futuristic **Blockchain Ecosystem**

Security Audit Report FOR



ShibElon

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
 KYC Verification	Not Done
 Audit Date	23 Feb 2023

PROJECT DESCRIPTION

ShibElon

In the year 1955, a young Shibelon was born onto the far far away planet called Neptune. Technology is too advanced on Neptune but humans could not reach this far to see all the innovations that it has to bring, therefore Shibelon studied astronomy and saw that there was a very high population on earth with very limited resources to reach advanced technology.



Social Media Profiles

ShibElon



- <https://shibelon.net/>
- https://t.me/shibelon_moon
- https://twitter.com/shibelon_moon

It's always good to check the social profiles of the project,
before making your investment.

-Team Expelee

CONTRACT DETAILS

Token Name

ShibElon

Network

ETH

Contract Address (Verified)

0x4c584CD339bdDE73B7F5210486dd8bbeEE3fDe6d

Token Type

ERC 20

Compiler

v0.8.15+commit.e14f2714

Symbol

SHIBELON

Language

Solidity

Total Supply

1,000,000,000,000

Optimization Enabled

Yes with 200 runs

Contract SHA-256 Checksum:

F0E4C2F76C58916EC258F246851BEA091D14D4247A2FC3E18694461B1816E13B

Owner's Wallet

0x0835996ccf48c0d355399954FbA8754BcF64E142

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
- Complier
- Hardhat

FUNCTION OVERVIEW

Can Take Back Ownership	Not Detected
Owner Change Balance	Not Detected
Blacklist	Not Detected
Modify Fees	Not Detected
Proxy	Not Detected
Whitelisted	Not Detected
Anti Whale	Not Detected
Trading Cooldown	Not Detected
Transfer Pausable	Not Detected
Cannot Sell All	Not Detected
Hidden Owner	Not Detected
Mint	Not Detected

VULNERABILITY CHECKLIST

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp 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 Zeppelin module	Passed
Fallback function security	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 warning that can remain unfixed.

Informational

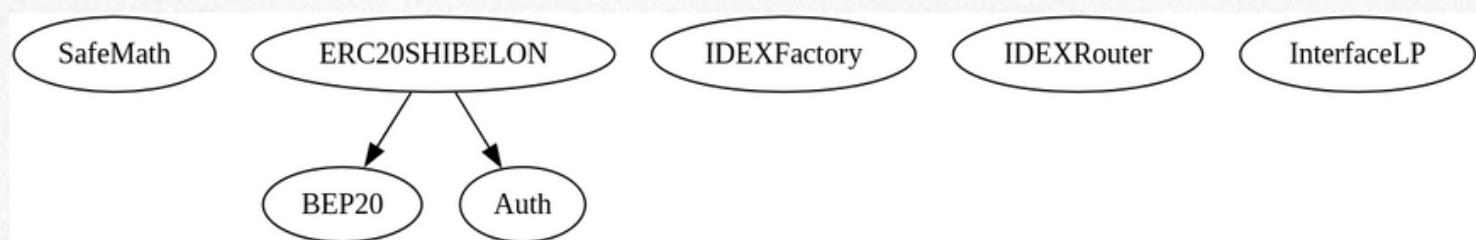
Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.

AUDIT SUMMARY

Used Tools:

- 1. Manual Review:** The code has undergone a line-by-line review by the Expelee team.
- 2. BSC Test Network:** All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.
- 3. Slither:** The code has undergone static analysis using Slither.

Inheritance Trees:



Summary:

- Owner is able to set buy and sell taxes up to 15% but sum of them can not be more than 24%
- Owner is not able to set transfer taxes more than 5%
- Owner is able to set max wallet amount, this max amount can not be less than 1% of supply
- Owner is able to set max tx amount but not less than 0.5% of total supply
- Owner is not able to disable trades
- Owner is not able to mint new tokens

Functional Tests

1- Adding liquidity (**passed**):

<https://testnet.bscscan.com/tx/0x2f05e1ceb8aa5bc8c487e8224bff6bca39edaa3a07a1fe830d254d142a8c9ca4>

2- Buying (7% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x8129aa79ed9e0d74f867d5b83683e57e62f5ae820c4506144abb3dbe0b8fdd6c>

3- Selling (internal swap + auto liquidity included in tx) (7% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x3831623b10f88b24f9b7f4edc22301a1fdcb540f09f3da4c2daf270ad5173d6f>

4- Transferring (2% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x9cf87bb6e4742b401914f9c3ca26ca509f220d3b596750a02c226bc333ce454f>

5- Burning 5% of LP (**passed**):

<https://testnet.bscscan.com/tx/0x697ce3eae7ecc0d57a02dec517145c38ec5d7126ec8f5dd60d4b703883aceb2f>

MANUAL AUDIT

Severity Criteria

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

Vulnerabilities are divided into three primary risk categories: **high**, **medium**, and **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				

FINDINGS

- **High Risk Findings:** 0
 - **Medium Risk Findings:** 0
 - **Low Risk Findings:** 2
 - **Suggestions & discussion:** 0
 - **Gas Optimizations :** 0
-

Low Risk Findings

Centralization

Owner is able to set max tx (can not be less than 0.5% of supply) and max wallet amounts (can not be less than 1% of supply)

```
ftrace | funcSig
function setMaxWalletPercent_base1000(
    uint256 maxWallPercent_base1000,
) external onlyOwner {
    require(
        maxWallPercent_base1000 >= 10,
        "Cannot set max wallet less than 1%"
    );
    maxWalletToken = (totalSupply * maxWallPercent_base1000) / 1000;
    emit config_MaxWallet(maxWalletToken);
}

ftrace | funcSig
function setMaxTxPercent_base1000(
    uint256 maxTXPercentage_base1000,
) external onlyOwner {
    require(
        maxTXPercentage_base1000 >= 5,
        "Cannot set max transaction less than 0.5%"
    );
    maxTxAmount = (totalSupply * maxTXPercentage_base1000) / 1000;
    emit config_MaxTransaction(maxTxAmount);
}
```

Low Risk Findings

Centralization

The burnLP function allows the owner to burn up to 5% of the liquidity pool tokens after each 5-minute interval, which presents a centralization risk as only the owner is able to call the function. If the owner were to misuse this power, it could result in harm to the investors of the protocol. Additionally, reducing the total amount of tokens in the liquidity pool could increase the price impact of each trade, making it more challenging for traders to accurately predict the price of the token and potentially leading to larger price fluctuations. As a result, the burnLP function can be both a centralization and liquidity risk for the protocol.

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 guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect 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. Always 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.