expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

MAKAVELI

TOKEN OVERVIEW

Risk Findings

Severity	Found
🔴 High	0
🟠 Medium	0
🟡 Low	0
🔵 Informational	0

Centralization Risks

Owner Privileges	Description
🟢 Can Owner Set Taxes >25% ?	Not Detected
🟢 Owner needs to enable trading ?	Not Detected
🟢 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

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	**-**
Audit Date	**11 July 2023**

expelee

CONTRACT DETAILS

Token Name: Makaveli2

Symbol: Makaveli

Network: BSC

Language: Solidity

Contract Address:
0x244f4002bcEfcf792423a5de86005ec9E13B7b1e

Total Supply: 420,000,000,000,000,000

Owner's Wallet:
0x860ea1D21E562BCff76666cB292aa9820BF07593

Deployer's Wallet:
0x2D97a0C4d42A334E95bCCa3a7a5B4D9450C20dc8

expelee

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

expelee

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces 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.
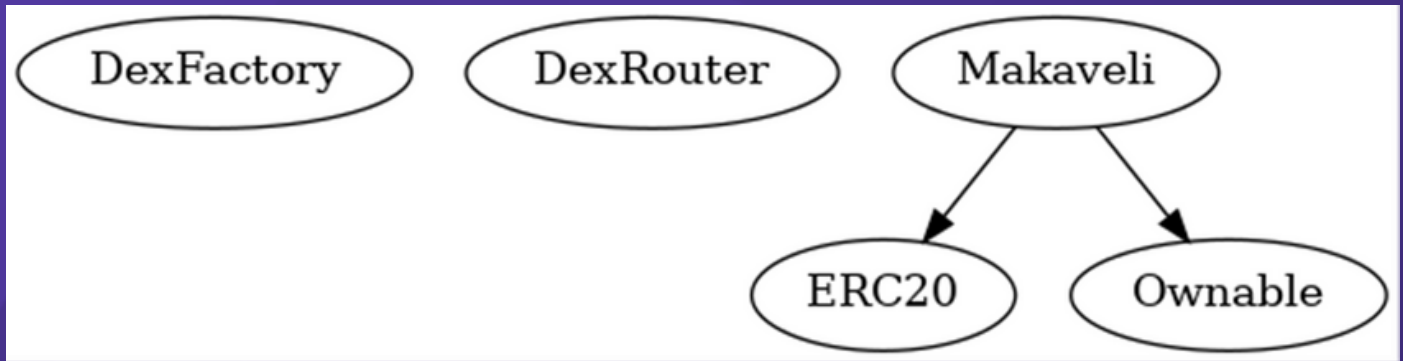
Low Risk

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

Informational

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

INHERITANCE TREES

TESTNET VERSION

Adding Liquidity ✅
Tx:
https://testnet.bscscan.com/tx/0xcb911051af8e37cbd191db1
5214e0e04d31cac994e2ee42caefb78253a4aa8de

===

Buying when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x83a9ff62112505b0ee36459
cf367a31ca34eec7d8deb8904e65449a1502b27c8

===

Selling when excluded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xd8981832344d2108245a4
1be13236dd8fc273563387ef11c84e9f4e5c388b7a3

===

Transferring when exclduded from fees ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x0a8fa9edb8a7f790112abc
4cdfd17d15cb91a0dea9212639e00aafc32b5e64fc

===

expelee

TESTNET VERSION

Buying ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0xc5443ab50093831485e0a4038fa4166c4f501982e3fcff92a710abff76e3b417

===

Selling ✅
Tx (3% tax):
https://testnet.bscscan.com/tx/0xc5443ab50093831485e0a4038fa4166c4f501982e3fcff92a710abff76e3b417

===

Transferring ✅
Tx (0% tax):
https://testnet.bscscan.com/tx/0x381fb8ccb90f1b0db48cac508c1aa4b8e34f82d89adc038cb6ef9e32fd31094a

===

Internal swap (auto-liquidity | BNB to marketing wallet) ✅
Tx:
https://testnet.bscscan.com/tx/0xadffdeae2e9022ec666ec788de56275616533c80031e84f46adc6f1a3986951a

===

FUNCTION DETAILS

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
DexFactory	Interface	|||		
└	createPair	External ❗	🔴	NO ❗	
DexRouter	Interface	|||		
└	factory	External ❗	NO ❗	
└	WETH	External ❗	NO ❗	
└	addLiquidityETH	External ❗	💵 NO ❗	
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🔴 NO ❗	
Makaveli	Implementation	ERC20, Ownable |||		
└	<Constructor>	Public ❗	🔴	ERC20
└	setMarketingWallet	External ❗	🔴	onlyOwner
└	setSwapTokensAtAmount	External ❗	🔴	onlyOwner
└	toggleSwapping	External ❗	🔴	onlyOwner
└	setWhitelistStatus	External ❗	🔴	onlyOwner
└	checkWhitelist	External ❗	NO ❗	
└	_takeTax	Internal 🔒	🔴	
└	_transfer	Internal 🔒	🔴	
└	internalSwap	Internal 🔒	🔴	
└	swapAndLiquify	Internal 🔒	🔴	
└	swapToETH	Internal 🔒	🔴	
└	addLiquidity	Private 🔒	🔴	
└	withdrawStuckETH	External ❗	🔴	onlyOwner
└	withdrawStuckTokens	External ❗	🔴	onlyOwner
└	<Receive Ether>	External ❗	💵 NO ❗	

Legend

Symbol	Meaning
🔴	Function can modify state

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 categroies:
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		

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   in 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.

Building the Futuristic Blockchain Ecosystem