



Building the Futuristic **Blockchain Ecosystem**

# SECURITY AUDIT REPORT

**MPOL**

# TOKEN OVERVIEW

## Risk Findings

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

## 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

02	Token Overview	
03	Table of Contents	
04	Overview	
05	Contract Details	
06	Audit Methodology	
07	Vulnerabilities Checklist	
08	Risk Classification	
09	Inheritance Trees & Risk Overview	
10	Testnet Version	
11	Function Details	
13	Manual Review	
14	Findings	
16	About Expelee	
17	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:

<b>Audit Result</b>	<b>Passed</b>
<b>KYC Verification</b>	-
<b>Audit Date</b>	<b>16 June 2023</b>

# CONTRACT DETAILS

Token Name: metapolice token

Symbol: mpol

Network: Binance smart chain

Language: Solidity

Contract Address:

0x7bA9E62eFC1D8702327FF8A69Bb6756d9fE94B1B

Total Supply: 5,000,000,000

Owner's Wallet:

0x7bA9E62eFC1D8702327FF8A69Bb6756d9fE94B1B

Deployer's Wallet:

0x3d7F628252Aa4F655A7394aE34952fA1E9573Ff6

# 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

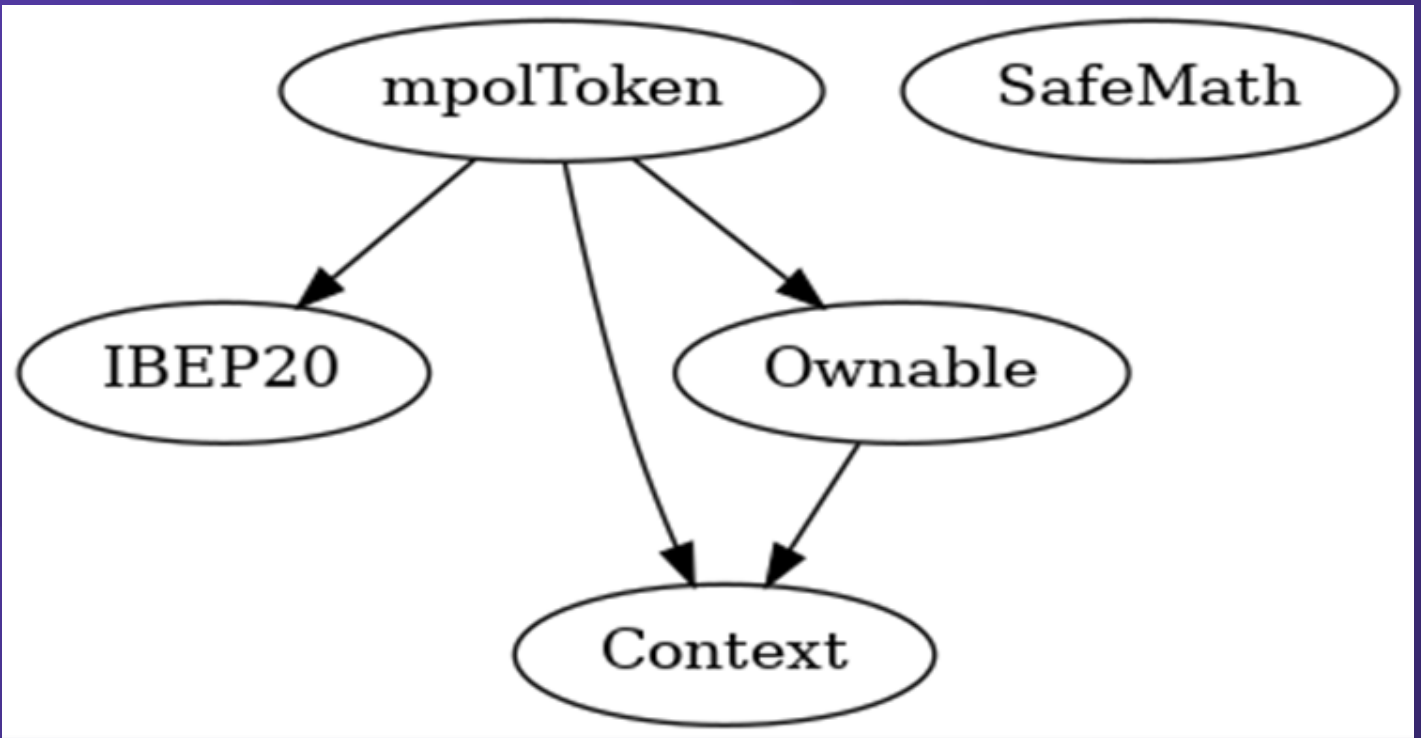
Issues on this level are minor details and warnings that can remain unfixed.

## Informational

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



# INHERITANCE TREES



# TESTNET VERSION

## Adding Liquidity ✓

Tx:

<https://testnet.bscscan.com/tx/0x8b0f578080a5f984a0c3b0756d6da399437dfdd81365b06fb9b4b08b570ef7aa>

=====

## Buying from a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x7e3ecfba0de805490634bfb42b1164b2d0ca15d698d04232584cd0c09c8cf68f>

=====

## Selling from a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xaad5d4e8e0d473bafbf4364b9661d09c3d4c803b941c9cce30a76e840a41510c>

=====

## Transferring using a fee excluded wallet ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x081f7a1f4140076fc093932e01dbee8eb8fb53d34a63f206010e6ee20401b033>



























































=====

# FUNCTION DETAILS

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
**IBEP20**   Interface					
L	totalSupply	External !		NO !	
L	decimals	External !		NO !	
L	symbol	External !		NO !	
L	name	External !		NO !	
L	getOwner	External !		NO !	
L	balanceOf	External !		NO !	
L	transfer	External !		NO !	
L	allowance	External !		NO !	
L	approve	External !		NO !	
L	transferFrom	External !		NO !	
**Context**   Implementation					
L	<Constructor>	Internal 🔒			
L	_msgSender	Internal 🔒			
L	_msgData	Internal 🔒			
**SafeMath**   Library					
L	add	Internal 🔒			
L	sub	Internal 🔒			
L	sub	Internal 🔒			
L	mul	Internal 🔒			
L	div	Internal 🔒			
L	div	Internal 🔒			
L	mod	Internal 🔒			
L	mod	Internal 🔒			
**Ownable**   Implementation   Context					

# FUNCTION DETAILS

```

| L | <Constructor> | Internal  |  || |
| L | owner | Public  | | NO  |
| L | renounceOwnership | Public  | |  | onlyOwner |
| L | transferOwnership | Public  | |  | onlyOwner |
| L | _transferOwnership | Internal  | |  ||
|||||
| **mpolToken** | Implementation | Context, IBEP20, Ownable |||
| L | <Constructor> | Public  | | NO  |
| L | getOwner | External  | | NO  |
| L | decimals | External  | | NO  |
| L | symbol | External  | | NO  |
| L | name | External  | | NO  |
| L | totalSupply | External  | | NO  |
| L | balanceOf | External  | | NO  |
| L | transfer | External  | |  NO  |
| L | allowance | External  | | NO  |
| L | approve | External  | |  NO  |
| L | transferFrom | External  | |  NO  |
| L | increaseAllowance | Public  | |  NO  |
| L | decreaseAllowance | Public  | |  NO  |
| L | mint | Public  | |  onlyOwner |
| L | burn | Public  | |  NO  |
| L | _transfer | Internal  | |  ||
| L | _mint | Internal  | |  ||
| L | _burn | Internal  | |  ||
| L | _approve | Internal  | |  ||
| L | _burnFrom | Internal  | |  ||
### Legend
| Symbol | Meaning |
|:-----:|:-----|
|  | Function can modify state |
|  | Function is payable |

```

# MANUAL REVIEW

## Severity Criteria

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

Vulnerabilities are divided into three primary risk categories:

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:** Minting

**Severity :** High

## Overview

Owner is able to mint new tokens using "mint" function

```
function mint(uint256 amount) public onlyOwner returns (bool) {  
  _mint(_msgSender(), amount);  
  return true;  
}
```

## Suggestion

there are multiple ways to solve this issue

- Setup a max supply
- Renounce ownership (applied)
- Delete mint functions

# INFORMATIONAL

**Category:** Informational

**Subject:** Outdated solidity compiler

**Severity :** Informational

## Overview

Compiler version (5) is outdated, its suggested to use latest solidity compilers ( $\geq 0.8.0$ )

# 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](http://www.expelee.com)

 [expeleeofficial](https://twitter.com/expeleeofficial)

 [expelee](https://medium.com/expelee)

 [Expelee](https://t.me/Expelee)

 [expelee](https://in.linkedin.com/company/expelee)

 [expelee\\_official](https://www.instagram.com/expelee_official)

 [expelee-co](https://github.com/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**