

# expellee

Building the Futuristic **Blockchain Ecosystem**

## SECURITY AUDIT REPORT



## AIPEPE

# TABLE OF CONTENTS

02 Table of Contents

03 Overview

04 Project Description

05 Social Media Profiles

06 Contract Details

07 Owner Privileges

08 Audit Methodology

09 Vulnerabilities Checklist

10 Risk Classification

11 Inheritance Trees

12 Function Details

17 Manual Review

18 Findings

22 About Expelee

23 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>No</b>
<b>Audit Date</b>	<b>21 April 2023</b>

# PROJECT DESCRIPTION

## AIPEPE

He's AI. He's Pepe. He's CEO. The first meme token that gives \$Arb rewards!



# SOCIAL MEDIA PROFILES

## AIPEPE



[https://t.me/AI\\_PEPE\\_CEO](https://t.me/AI_PEPE_CEO)



[https://twitter.com/AI\\_PEPE\\_CEO](https://twitter.com/AI_PEPE_CEO)



<https://www.ai-pepe-ceo.com/>

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

Team Expelee

# CONTRACT DETAILS

Token Name: AI-Pepe-CEO

Symbol: AI-Pepe-CEO

Network: Binance Smart Chain

Language: Solidity

Contract Address: ---

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

Contract SHA-256 Checksum:

aa1e6198802d5b018dde3b30cdd11e09c9e38b00

Owner's Wallet: ---

Deployer's Wallet: ---

Testnet:

<https://testnet.bscscan.com/token/0x179bb17efd81b87e36149a31a4140f9875381377>

# OWNER PRIVILEGES

- Contract owner is not able to set buy/sell taxes over 10% each
- Contract owner is not able to set transfer fee (0% transfer fee)
- Contract owner is not able to set limits for buy/sell/transfer amounts
- Contract owner is not able to blacklist an arbitrary wallet
- Contract owner is not able to disable trades/transfers
- Contract owner is not able to mint new tokens
- Contract owner must enable trades for public

# 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 Zeppelin 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.

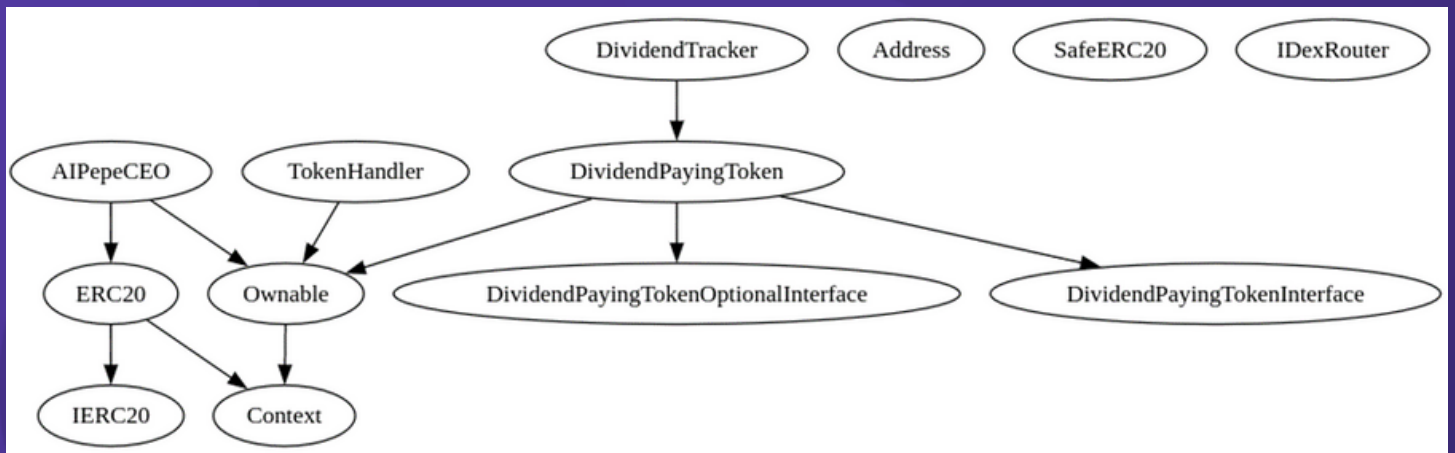
## Low Risk

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

Symbol	Meaning
	Function can modify state
	Function is payable

## Contract Assessment

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
L	<b>**Function Name**</b>	<b>**Visibility**</b>	<b>**Mutability**</b>	<b>**Modifiers**</b>	
<b>**Context**</b>   Implementation					
L	_msgSender	Internal			
L	_msgData	Internal			
<b>**Address**</b>   Library					
L	isContract	Internal			
L	sendValue	Internal			
L	functionCall	Internal			
L	functionCall	Internal			
L	functionCallWithValue	Internal			
L	functionCallWithValue	Internal			
L	functionStaticCall	Internal			
L	functionStaticCall	Internal			
L	functionDelegateCall	Internal			
L	functionDelegateCall	Internal			
L	verifyCallResultFromTarget	Internal			
L	verifyCallResult	Internal			
L	_revert	Private			
<b>**SafeERC20**</b>   Library					
L	safeTransfer	Internal			
L	_callOptionalReturn	Private			
<b>**IERC20**</b>   Interface					
L	totalSupply	External			NO !
L	balanceOf	External			NO !
L	transfer	External			NO !
L	allowance	External			NO !
L	approve	External			NO !

# FUNCTION DETAILS

```

| L | transferFrom | External ! | ● | NO ! |
| L | name | External ! | | NO ! |
| L | symbol | External ! | | NO ! |
| L | decimals | External ! | | NO ! |
|||||
| **ERC20** | Implementation | Context, IERC20 |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | name | Public ! | | NO ! |
| L | symbol | Public ! | | NO ! |
| L | decimals | Public ! | | NO ! |
| L | totalSupply | Public ! | | NO ! |
| L | balanceOf | Public ! | | NO ! |
| L | transfer | Public ! | ● | NO ! |
| L | allowance | Public ! | | NO ! |
| L | approve | Public ! | ● | NO ! |
| L | transferFrom | Public ! | ● | NO ! |
| L | increaseAllowance | Public ! | ● | NO ! |
| L | decreaseAllowance | Public ! | ● | NO ! |
| L | _transfer | Internal 🔒 | ● | |
| L | _createInitialSupply | Internal 🔒 | ● | |
| L | _approve | Internal 🔒 | ● | |
|||||
| **Ownable** | Implementation | Context |||
| L | <Constructor> | Public ! | ● | NO ! |
| L | owner | Public ! | | NO ! |
| L | renounceOwnership | External ! | ● | onlyOwner |
| L | transferOwnership | Public ! | ● | onlyOwner |
|||||
| **IDexRouter** | Interface | |||
| L | factory | External ! | | NO ! |
| L | WETH | External ! | | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! | 🟢 | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! | ● | NO ! |
| L | addLiquidityETH | External ! | 🟢 | NO ! |
| L | addLiquidity | External ! | ● | NO ! |
| L | getAmountsOut | External ! | | NO ! |
| L | removeLiquidity | External ! | ● | NO ! |
|||||
| **DividendPayingTokenOptionalInterface** | Interface | |||
| L | withdrawableDividendOf | External ! | | NO ! |
| L | withdrawnDividendOf | External ! | | NO ! |
| L | accumulativeDividendOf | External ! | | NO ! |
|||||
| **DividendPayingTokenInterface** | Interface | |||

```

# FUNCTION DETAILS

```

| L | dividendOf | External ! | | NO ! |
| L | distributeDividends | External ! | | NO ! |
| L | withdrawDividend | External ! | | NO ! |
|||||
**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 | | |
|||||
**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 | | |
|||||
**DividendPayingToken** | Implementation | DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface, Ownable |||
| L | <Receive Ether> | External ! | | NO ! |
| L | distributeDividends | Public ! | | NO ! |
| L | distributeTokenDividends | 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 | _increase | Internal | | |
| L | _reduce | Internal | | |
| L | _setBalance | Internal | | |
|||||
**DividendTracker** | Implementation | DividendPayingToken |||
| L | <Constructor> | Public ! | | NO ! |
| L | get | Private | | |
| L | getIndexOfKey | Private | | |
| L | getKeyAtIndex | Private | | |
| L | size | Private | | |
| L | set | Private | | |

```

# FUNCTION DETAILS

```

| remove | Private 🔒 | ● | | |
| excludeFromDividends | External ! | ● | onlyOwner |
| includeInDividends | External ! | ● | onlyOwner |
| updateClaimWait | External ! | ● | onlyOwner |
| getLastProcessedIndex | External ! | | NO ! |
| getNumberOfTokenHolders | External ! | | NO ! |
| getAccount | Public ! | | NO ! |
| getAccountAtIndex | Public ! | | NO ! |
| canAutoClaim | Private 🔒 | | |
| setBalance | External ! | ● | onlyOwner |
| process | Public ! | ● | NO ! |
| processAccount | Public ! | ● | onlyOwner |
|||||
| **IDexFactory** | Interface | |||
| | createPair | External ! | ● | NO ! |
|||||
| **ILpPair** | Interface | |||
| | sync | External ! | ● | NO ! |
|||||
| **TokenHandler** | Implementation | Ownable |||
| | sendTokenToOwner | External ! | ● | onlyOwner |
|||||
| **AIPepeCEO** | Implementation | ERC20, Ownable |||
| | <Constructor> | Public ! | ● | ERC20 |
| | createPair | Internal 🔒 | ● | |
| | updateAllowanceForSwapping | External ! | ● | NO ! |
| | startTrading | External ! | ● | onlyOwner |
| | excludeFromDividends | External ! | ● | onlyOwner |
| | includeInDividends | External ! | ● | onlyOwner |
| | removeLimits | External ! | ● | onlyOwner |
| | updateMaxBuyAmt | External ! | ● | onlyOwner |
| | updateMaxSellAmt | External ! | ● | onlyOwner |
| | removeMaxWallet | External ! | ● | onlyOwner |
| | updateSwapTokensAtAmt | External ! | ● | onlyOwner |
| | _excludeFromMaxTransaction | Private 🔒 | ● | |
| | airdropToWallets | External ! | ● | onlyOwner |
| | excludeFromMaxTransaction | External ! | ● | onlyOwner |
| | setAutomatedMarketMakerPair | Public ! | ● | onlyOwner |
| | updateBuyTax | External ! | ● | onlyOwner |
| | updateSellTax | External ! | ● | onlyOwner |
| | excludeFromTax | Public ! | ● | onlyOwner |
| | updateClaimWait | External ! | ● | onlyOwner |
| | getClaimWait | External ! | | NO ! |
| | getTotalDividendsDistributed | External ! | | NO ! |
| | withdrawableDividendOf | Public ! | | NO ! |
| | dividendTokenBalanceOf | Public ! | | NO ! |

```



# FUNCTION DETAILS

```

| L | getAccountDividendsInfo | External ! | [NO ! | |
| L | getAccountDividendsInfoAtIndex | External ! | [NO ! |
| L | claim | External ! | ● [NO ! |
| L | getLastProcessedIndex | External ! | [NO ! |
| L | getNumberOfDividendTokenHolders | External ! | [NO ! |
| L | getNumberOfDividends | External ! | [NO ! |
| L | _transfer | Internal 🔒 | ● ||
| L | swapTokensForREWARDTOKEN | Private 🔒 | ● ||
| L | swapBack | Private 🔒 | ● ||
| L | setMarketingAddress | External ! | ● | onlyOwner |
| L | forceSwapBack | External ! | ● | onlyOwner |
| L | transferForeignToken | External ! | ● | onlyOwner |
| L | updateGasForProcessing | External ! | ● | onlyOwner |

```



# 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			

# FINDINGS

Findings	Severity	Found
High Risk	● High	1
Medium Risk	● Medium	1
Low Risk	● Low	0
Suggestion & discussion	● Informational	0
Gas Optimizations	● Gas Opt.	0

# HIGH RISK FINDING

Enabling trades is not guaranteed

**Category:** Centralization

**Impact:** High

**Overview:**

**The owner of the contract must enable trades for public, otherwise no one would be able to buy/sell/transfer their tokens except whitelisted wallets.**

```
function startTrading() external onlyOwner {
  require(!tradingLive, "Trading is already active, cannot relaunch.");
  require(lpPair != address(0), "Create Pair First");
  tradingLive = true;
  swapEnabled = true;
  tradingLiveBlock = block.number;
  emit StartedTrading();
}
```

## Suggestion

To mitigate this issue there are several options:

- Temporary transfer ownership of the contract to a pinksale safu developer (done)
- Enable tradings before presale

**Issue Status:** Open

# MEDIUM RISK FINDING

## Trade limits

**Category:** Centralization

**Impact:** Medium

### Overview:

The owner of the contract is able to set limits for max amount of buy/sell/holding. The safeguard for this limit is 1% of total supply (meaning this limits can not be lower than this amount).

Max wallet is 1% always, unless disabled by owner using `removeMaxWallet` function (once disabled can not be enabled again)

```
function updateMaxBuyAmt(uint256 newNum) external onlyOwner {
    require(
        newNum >= ((totalSupply() * 1) / 100) / 1e18,
        "Cannot set max sell amt lower than 1%"
    );
    maxBuyAmt = newNum * (10 ** 18);
    emit UpdatedMaxBuyAmt(maxBuyAmt);
}
```

```
function updateMaxSellAmt(uint256 newNum) external onlyOwner {
    require(
        newNum >= ((totalSupply() * 1) / 100) / 1e18,
        "Cannot set max sell amt lower than 1%"
    );
    maxSellAmt = newNum * (10 ** 18);
    emit UpdatedMaxSellAmt(maxSellAmt);
}
```

# MEDIUM RISK FINDING

## Suggestion

To mitigate this issue there are several options:

- Make sure to follow pinksale safu criteria for proper safeguards (done)

Issue Status: **Resolved**

# 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



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**