expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

CATJEDI

HIGH RISK ANALYSIS

No High Risks found

Findings	Found
High Risk	0

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	No
Audit Date	2 June 2023

CONTRACT DETAILS

Token Name: Cat Jedi

Symbol: CAT JEDI

Network: Binance Smart Chain

Language: Solidity

Contract Address:
0x4adFC8C9C4D0a8405E6fF81C80e4a32124a359Bd

Total Supply: 1000000000

Owner's Wallet:
0x5FAfD151cE6503c59D463DbeD1FFdD3eb3Bd8FC8

Deployer's Wallet:
0x5FAfD151cE6503c59D463DbeD1FFdD3eb3Bd8FC8

OWNER PRIVILEGES

- The owner can set fees with limit up to 20%

- Owner can exclude account from reward

- The owner can exclude accounts from fees

- The owner can change swap settings

exexpelee

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 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.
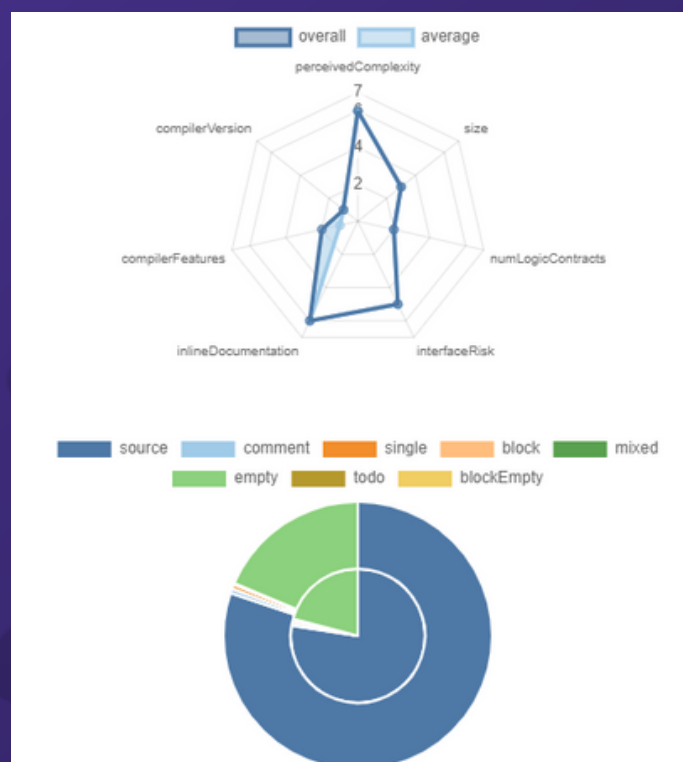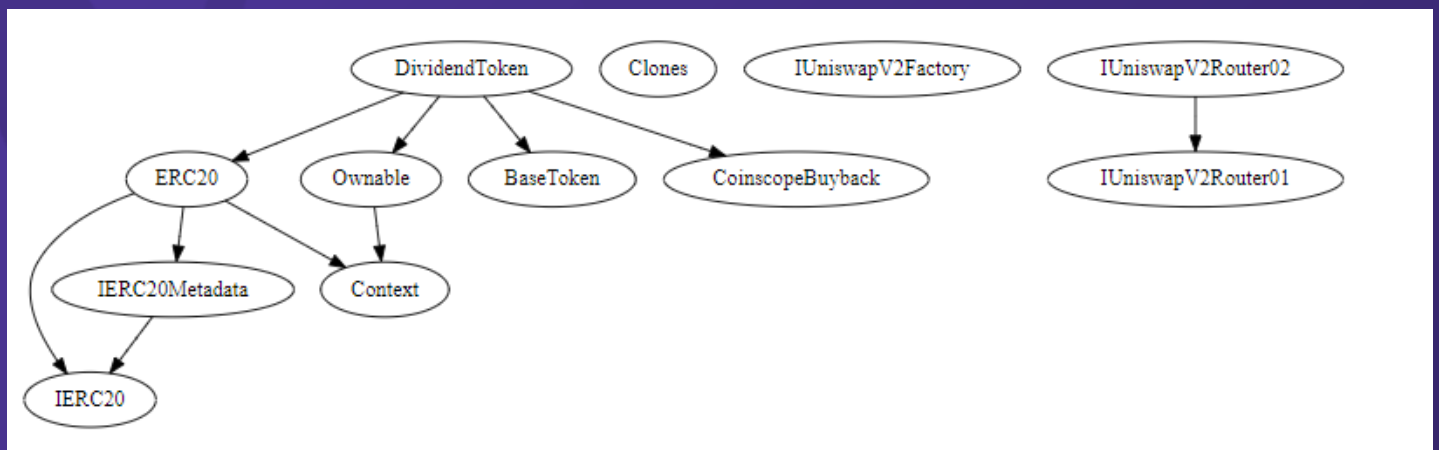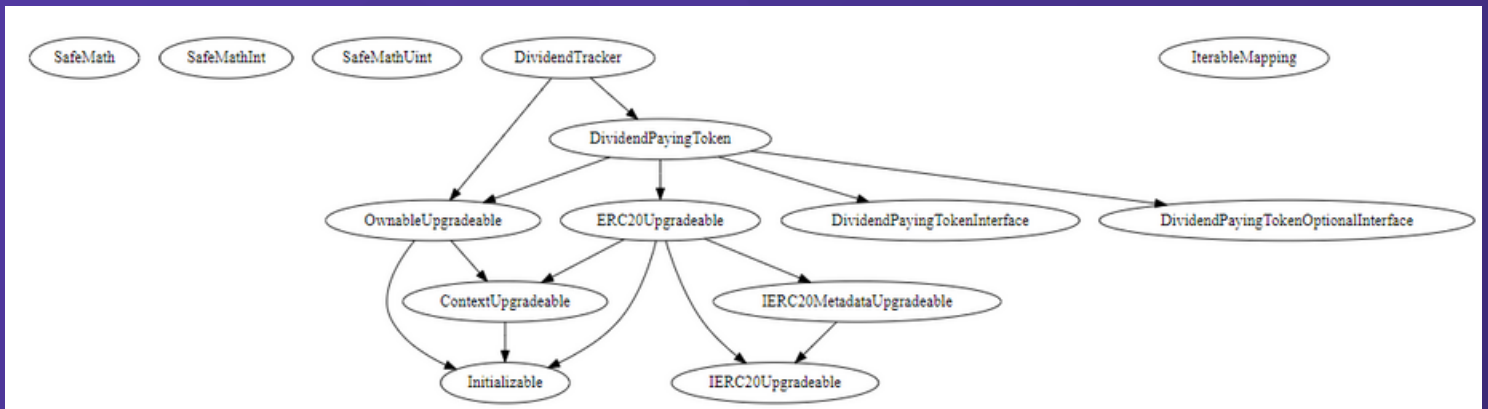
Low Risk

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

FUNCTION DETAILS

```
||||||
| **DividendPayingTokenInterface** | Interface |  |||
| └ | dividendOf | External ! |   |NO! |
| └ | withdrawDividend | External ! |  ● |NO! |
||||||
| **DividendPayingTokenOptionalInterface** | Interface |  |||
| └ | withdrawableDividendOf | External ! |  |NO! |
| └ | withdrawnDividendOf | External ! |  |NO! |
| └ | accumulativeDividendOf | External ! |  |NO! |
||||||
| **DividendPayingToken** | Implementation | ERC20Upgradeable, OwnableUpgradeable, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface |||
| └ | __DividendPayingToken_init | Internal 🔒 |  ●  | initializer |
| └ | distributeCAKEDividends | Public ! |  ●  | onlyOwner |
| └ | withdrawDividend | Public ! |  ● |NO! |
| └ | _withdrawDividendOfUser | Internal 🔒 |  ●  | |
| └ | dividendOf | Public ! |   |NO! |
| └ | withdrawableDividendOf | Public ! |   |NO! |
| └ | withdrawnDividendOf | Public ! |   |NO! |
| └ | accumulativeDividendOf | Public ! |   |NO! |
| └ | _transfer | Internal 🔒 |  ●  | |
| └ | _mint | Internal 🔒 |  ●  | |
| └ | _burn | Internal 🔒 |  ●  | |
| └ | _setBalance | Internal 🔒 |  ●  | |
||||||
| **IterableMapping** | Library |  |||
| └ | get | Public ! |   |NO! |
| └ | getIndexOfKey | Public ! |   |NO! |
| └ | getKeyAtIndex | Public ! |   |NO! |
| └ | size | Public ! |   |NO! |
| └ | set | Public ! |  ● |NO! |
| └ | remove | Public ! |  ● |NO! |
||||||
| **DividendTracker** | Implementation | OwnableUpgradeable, DividendPayingToken |||
| └ | initialize | External ! |  ●  | initializer |
| └ | _transfer | Internal 🔒 |  | |
| └ | withdrawDividend | Public ! |   |NO! |
| └ | excludeFromDividends | External ! |  ●  | onlyOwner |
| └ | isExcludedFromDividends | Public ! |   |NO! |
| └ | updateClaimWait | External ! |  ●  | onlyOwner |
| └ | updateMinimumTokenBalanceForDividends | 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 |
||||||
| **IERC20** | Interface |  |||
| └ | totalSupply | External ! |   |NO! |
| └ | balanceOf | External ! |   |NO! |
| └ | transfer | External ! |  ● |NO! |
| └ | allowance | External ! |   |NO! |
| └ | approve | External ! |  ● |NO! |
| └ | transferFrom | External ! |  ● |NO! |
||||||
```

FUNCTION DETAILS

```
||||||
| **BaseToken** | Implementation |   |||
||||||
| **CoinscopeBuyback** | Implementation |   |||
| └ | coinscopeBuyback | Internal 🔒 | ● | |
||||||
| **DividendToken** | Implementation | ERC20, Ownable, BaseToken, CoinscopeBuyback |||
| └ | <Constructor> | Public ❗ |   | ▓▓ | ERC20 |
| └ | getNativeCurrency | Internal 🔒 |   |   | |
| └ | <Receive Ether> | External ❗ |   | ▓▓ |NO❗ |
| └ | setSwapTokensAtAmount | External ❗ | ● | onlyOwner |
| └ | excludeFromFees | External ❗ | ● | onlyOwner |
| └ | excludeMultipleAccountsFromFees | External ❗ | ● | onlyOwner |
| └ | setMarketingWallet | External ❗ | ● | onlyOwner |
| └ | setTokenRewardsFee | External ❗ | ● | onlyOwner |
| └ | setLiquidityFee | External ❗ | ● | onlyOwner |
| └ | setMarketingFee | External ❗ | ● | onlyOwner |
| └ | updateFees | Internal 🔒 | ● | |
| └ | _setAutomatedMarketMakerPair | Private 🔐 | ● | |
| └ | updateGasForProcessing | Public ❗ | ● | onlyOwner |
| └ | updateClaimWait | External ❗ | ● | onlyOwner |
| └ | getClaimWait | External ❗ |   |NO❗ |
| └ | updateMinimumTokenBalanceForDividends | External ❗ | ● | onlyOwner |
| └ | getMinimumTokenBalanceForDividends | External ❗ |   |NO❗ |
| └ | getTotalDividendsDistributed | External ❗ |   |NO❗ |
| └ | isExcludedFromFees | Public ❗ |   |NO❗ |
| └ | withdrawableDividendOf | Public ❗ |   |NO❗ |
| └ | dividendTokenBalanceOf | Public ❗ |   |NO❗ |
| └ | excludeFromDividends | External ❗ | ● | onlyOwner |
| └ | isExcludedFromDividends | Public ❗ |   |NO❗ |
| └ | getAccountDividendsInfo | External ❗ |   |NO❗ |
| └ | getAccountDividendsInfoAtIndex | External ❗ |   |NO❗ |
| └ | processDividendTracker | External ❗ | ● |NO❗ |
| └ | claim | External ❗ | ● |NO❗ |
| └ | getLastProcessedIndex | External ❗ |   |NO❗ |
| └ | getNumberOfDividendTokenHolders | External ❗ |   |NO❗ |
| └ | _transfer | Internal 🔒 | ● | |
| └ | swap | Private 🔐 | ● | lockTheSwap |
| └ | swapAndLiquify | Private 🔐 | ● | |
| └ | swapTokensForEth | Private 🔐 | ● | |
| └ | addLiquidity | Private 🔐 | ● | |
| └ | swapTokensForReward | Private 🔐 | ● | |
| └ | swapAndSendDividends | Private 🔐 | ● | |
```

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		
	HIGH	Medium	High	Critical
Impact	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
		Likelihood		

FINDINGS

Findings	Severity	Found
High Risk	🔴 High	0
Medium Risk	🟠 Medium	0
Low Risk	🟡 Low	4
Suggestion & discussion	🔵 Informational	0
Gas Optimizations	🟣 Gas Opt.	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

🐦 expeleeofficial   Ⓜ expelee

✈ Expelee   in expelee

📷 expelee_official   🐙 expelee-co

exͣpelee

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.

expelee

Building the Futuristic Blockchain Ecosystem