



Building the Futuristic **Blockchain Ecosystem**

# SECURITY AUDIT REPORT



Candle Catcher

# 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 Tree

12 Function Details

15 Manual Review

16 Findings

19 About Expelee

20 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>DONE</b>
<b>Audit Date</b>	<b>21 April 2023</b>

# PROJECT DESCRIPTION

Candle Catcher is also known as Candle thief as we steal candles from others chart and place it in ours to make it green. We aim to create a unique and sustainable environment for our users by leveraging a distinctive approach to tokenomics and investment strategy.



# SOCIAL MEDIA PROFILES

## CANDLE CATCHER



<https://t.me/CandleCatcherOfficial>



<https://twitter.com/CandleCatcher>



<https://candlecatchercoin.com/>

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

Team Expelee

# CONTRACT DETAILS

Token Name: Candle Catcher

Symbol: CNDL

Network: Binance Smart Chain

Language: Solidity

Contract Address :

0x492AAbEB7cF62BFD7EC95f1094fC696bB4DDa96a

Total Supply: 1,000,000,000,000,000

Contract SHA-256 Checksum:

ae2ccb14ec54f1265b4c1e70fcf67e088586dcd1

Owner's Wallet:

0x2f6db8d76be994bc84ead5a24ef35de84b2a3e45

Testnet:

<https://testnet.bscscan.com/token/0x9089D4548335dA75ACd9F097f6764C1A7Ba9Cc46>



# OWNER PRIVILEGES

- Contract owner is not able to change buy/sell fees (8% each)
- Contract owner is not able to set a 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

# 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.

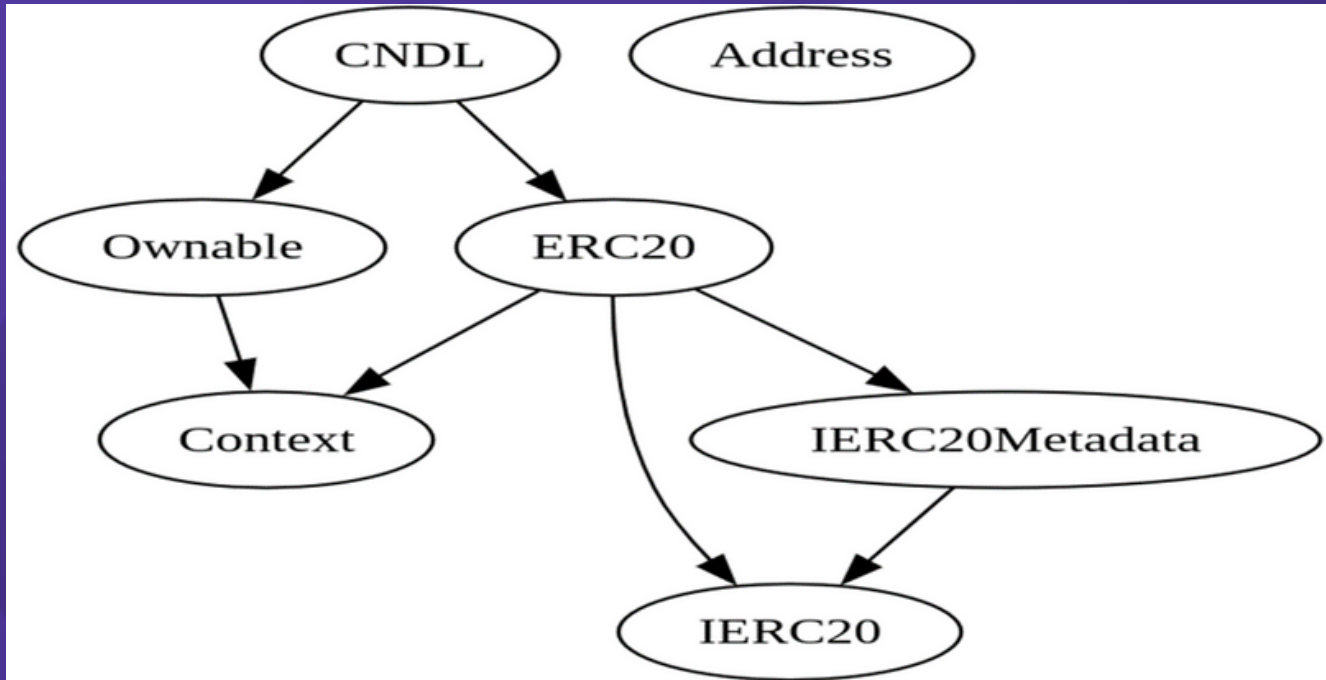
## Low Risk

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



# FUNCTION DETAILS

Symbol	Meaning
	Function can modify state
	Function is payable

```

| Contract |      Type      |      Bases      |      |      |
|:-----:|:-----:|:-----:|:-----:|:-----:|
|  L  | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
|||||
**IUniswapV2Factory** | Interface | |||
|  L  | feeTo | External | ! | | NO ! |
|  L  | feeToSetter | External | ! | | NO ! |
|  L  | getPair | External | ! | | NO ! |
|  L  | allPairs | External | ! | | NO ! |
|  L  | allPairsLength | External | ! | | NO ! |
|  L  | createPair | External | ! | ● | NO ! |
|  L  | setFeeTo | External | ! | ● | NO ! |
|  L  | setFeeToSetter | External | ! | ● | NO ! |
|||||
**IUniswapV2Pair** | Interface | |||
|  L  | name | External | ! | | NO ! |
|  L  | symbol | External | ! | | NO ! |
|  L  | decimals | External | ! | | NO ! |
|  L  | totalSupply | External | ! | | NO ! |
|  L  | balanceOf | External | ! | | NO ! |
|  L  | allowance | External | ! | | NO ! |
|  L  | approve | External | ! | ● | NO ! |
|  L  | transfer | External | ! | ● | NO ! |
|  L  | transferFrom | External | ! | ● | NO ! |
|  L  | DOMAIN_SEPARATOR | External | ! | | NO ! |
|  L  | PERMIT_TYPEHASH | External | ! | | NO ! |
|  L  | nonces | External | ! | | NO ! |
|  L  | permit | External | ! | ● | NO ! |
|  L  | MINIMUM_LIQUIDITY | External | ! | | NO ! |
|  L  | factory | External | ! | | NO ! |
|  L  | token0 | External | ! | | NO ! |
|  L  | token1 | External | ! | | NO ! |
|  L  | getReserves | External | ! | | NO ! |
|  L  | price0CumulativeLast | External | ! | | NO ! |
|  L  | price1CumulativeLast | External | ! | | NO ! |
|  L  | kLast | External | ! | | NO ! |
|  L  | mint | External | ! | ● | NO ! |
|  L  | burn | External | ! | ● | NO ! |
|  L  | swap | External | ! | ● | NO ! |
|  L  | skim | External | ! | ● | NO ! |
|  L  | sync | External | ! | ● | NO ! |
|  L  | initialize | External | ! | ● | NO ! |
|||||
**IUniswapV2Router01** | Interface | |||
|  L  | factory | External | ! | | NO ! |
|  L  | WETH | External | ! | | NO ! |
|  L  | addLiquidity | External | ! | ● | NO ! |
|  L  | addLiquidityETH | External | ! |  | NO ! |
|  L  | removeLiquidity | External | ! | ● | NO ! |
|  L  | removeLiquidityETH | External | ! | ● | NO ! |

```

# FUNCTION DETAILS

```

| L | removeLiquidityWithPermit | External | ! | ● | NO ! |
| L | removeLiquidityETHWithPermit | External | ! | ● | NO ! |
| L | swapExactTokensForTokens | External | ! | ● | NO ! |
| L | swapTokensForExactTokens | External | ! | ● | NO ! |
| L | swapExactETHForTokens | External | ! | 🟢 | NO ! |
| L | swapTokensForExactETH | External | ! | ● | NO ! |
| L | swapExactTokensForETH | External | ! | ● | NO ! |
| L | swapETHForExactTokens | External | ! | 🟢 | NO ! |
| L | quote | External | ! | | NO ! |
| L | getAmountOut | External | ! | | NO ! |
| L | getAmountIn | External | ! | | NO ! |
| L | getAmountsOut | External | ! | | NO ! |
| L | getAmountsIn | External | ! | | NO ! |
|||||
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |||
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External | ! | ● | NO ! |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External | ! | ● | NO ! |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External | ! | ● | NO ! |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External | ! | 🟢 | NO ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External | ! | ● | NO ! |
|||||
| **IERC20** | Interface | |||
| L | totalSupply | External | ! | | NO ! |
| L | balanceOf | External | ! | | NO ! |
| L | transfer | External | ! | ● | NO ! |
| L | allowance | External | ! | | NO ! |
| L | approve | External | ! | ● | NO ! |
| L | transferFrom | External | ! | ● | NO ! |
|||||
| **IERC20Metadata** | Interface | IERC20 |||
| L | name | External | ! | | NO ! |
| L | symbol | External | ! | | NO ! |
| L | decimals | External | ! | | NO ! |
|||||
| **Address** | 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 | 🔒 | | |
|||||
| **Context** | Implementation | |||
| L | _msgSender | Internal | 🔒 | | |

```

# FUNCTION DETAILS

```

| L | _msgData | Internal | 🔒 | | | |
|||||
| **Ownable** | Implementation | Context |||
| L | <Constructor> | Public | ! | ● | NO | ! |
| L | owner | Public | ! | | NO | ! |
| L | renounceOwnership | Public | ! | ● | onlyOwner |
| L | transferOwnership | Public | ! | ● | onlyOwner |
|||||
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |||
| 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 | _mint | Internal | 🔒 | ● | |
| L | _burn | Internal | 🔒 | ● | |
| L | _approve | Internal | 🔒 | ● | |
| L | _beforeTokenTransfer | Internal | 🔒 | ● | |
| L | _afterTokenTransfer | Internal | 🔒 | ● | |
|||||
| **CNDL** | Implementation | ERC20, Ownable |||
| L | <Constructor> | Public | ! | ● | ERC20 |
| L | <Receive Ether> | External | ! | 🟢 | NO | ! |
| L | claimStuckTokens | External | ! | ● | onlyOwner |
| L | excludeFromFees | External | ! | ● | onlyOwner |
| L | isExcludedFromFees | Public | ! | | NO | ! |
| L | changeMarketingWallet | External | ! | ● | onlyOwner |
| L | enableTrading | External | ! | ● | onlyOwner |
| L | _transfer | Internal | 🔒 | ● | |
| L | setSwapEnabled | External | ! | ● | onlyOwner |
| L | setSwapTokensAtAmount | External | ! | ● | onlyOwner |
| L | swapAndLiquify | Private | 🔒 | ● | |
| L | swapAndSendMarketing | Private | 🔒 | ● | |

```



# 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			



# FINDINGS

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

# HIGH RISK FINDING

## Enabling trades is not guaranteed

### Severity : 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 enableTrading() external onlyOwner {  
    require(!tradingEnabled, "Trading already enabled.");  
    tradingEnabled = true;  
    swapEnabled = true;  
}
```

#### 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
- Allowing enabling of the trades after a specifiéc time by any token holder

Example:

```
function enableTrading() external {  
    require(msg.sender == owner || elapsedTimeSincePresale >  
threshold, "Caller must be owner, or threshold must be  
passed");  
    pairAddress = _pairAddress;  
    tradingStatus = true;  
}
```

# HIGH RISK FINDING

## Issue Status: Resolved

Contract is owned and developed by pinksale safu developer (coinsult), hence enabling trades is guaranteed.

# 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**