expelee

A Secure Place For Web3

SMART CONTRACT AUDIT OF

CROCO INU Presale

Contract Address

0xe8b4e776241cDA5F82F48c78C1160aD6D665ff4f

Audit Summary

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**

Ownership: NOT **RENOUNCED**

KYC Verification: Done

Audit Date: 23/07/2022

Audit Team: **EXPELEE**

Be aware that smart contracts deployed on the blockchain aren't resistant to internal exploit, external vulnerability, or hack. For a detailed understanding of risk severity, source code vulnerability, functional hack, and audit disclaimer, kindly refer to the audit.

DISCLAMER

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 guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect 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. Always 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.

Contract Review

Contract Name	CROCO
Compiler Version	v0.7.4+commit.3f05b770
Optimization	No with 200 runs
License	MIT license
Explorer	https://bscscan.com/address/0xe8b4e776241cDA5F82F48c78C1160aD6D665ff4f#code
Symbol	CROCO
Decimals	5
Total Supply	512,788.10753
Domain	https://crocoinu.io/

Project Review

Token Name: CROCO INU

Web Site: https://crocoinu.io/

Twitter: https://twitter.com/CrocoInuToken

Telegram: https://t.me/CrocoInuToken

Contract Address:
0xe8b4e776241cDA5F82F48c78C1160aD6D665ff4f

Platform: Binance Smart Chain

Token Type: BEP 20

Language: SOLIDITY

Audit Methodology

The scope of this report is to audit the smart contract source code. We have scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities	- Unhandled Exceptions - Transaction Order Dependency - Integer Overflow - Unrestricted Action - Incorrect Inheritance Order - Typographical Errors - Requirement Violation
Source Code Review	- Gas Limit and Loops - Deployment Consistency - Repository Consistency - Data Consistency - Token Supply Manipulation
Functional Assessment	- Operations Trail & Event Generation - Assets Manipulation - Liquidity Access

Vulnerability Checklist

№	Description.	Result
1	Compiler warnings.	Passed
2	Race conditions and Re-entrancy. Cross-function raceconditions.	Passed
3	Possible delays in data delivery.	Passed
4	Oracle calls.	Passed
5	Front running.	Passed
6	Timestamp dependence.	Passed
7	Integer Overflow and Underflow.	Passed
8	DoS with Revert.	Passed
9	DoS with block gas limit.	Passed
10	Methods execution permissions.	Passed
11	Economy model.	Passed
12	The impact of the exchange rate on the logic.	Passed
13	Private user data leaks.	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations.	Passed
16	Uninitialized storage pointers.	Passed
17	Arithmetic accuracy.	Passed
18	Design Logic.	Passed
19	Cross-function race conditions.	Passed
20	Safe Zeppelin module.	Passed
21	Fallback function security.	Passed

Manual Audit

🟢 **Low-Risk**

🟢 4 low-risk code issues found

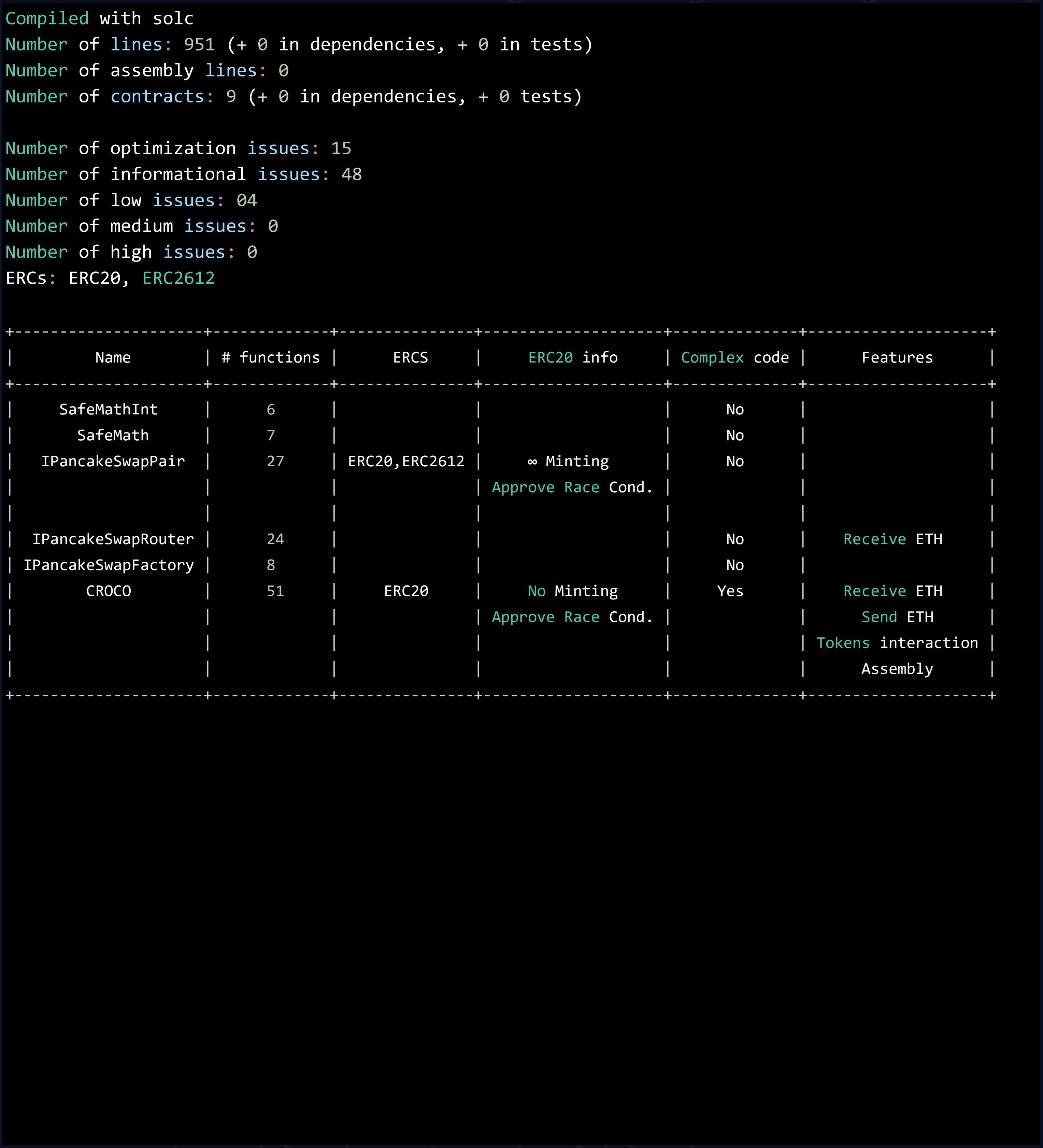
🟡 **Medium-Risk**

🟡 0 medium-risk code issues found

🔴 **High-Risk**

🔴 0 high-risk code issues found

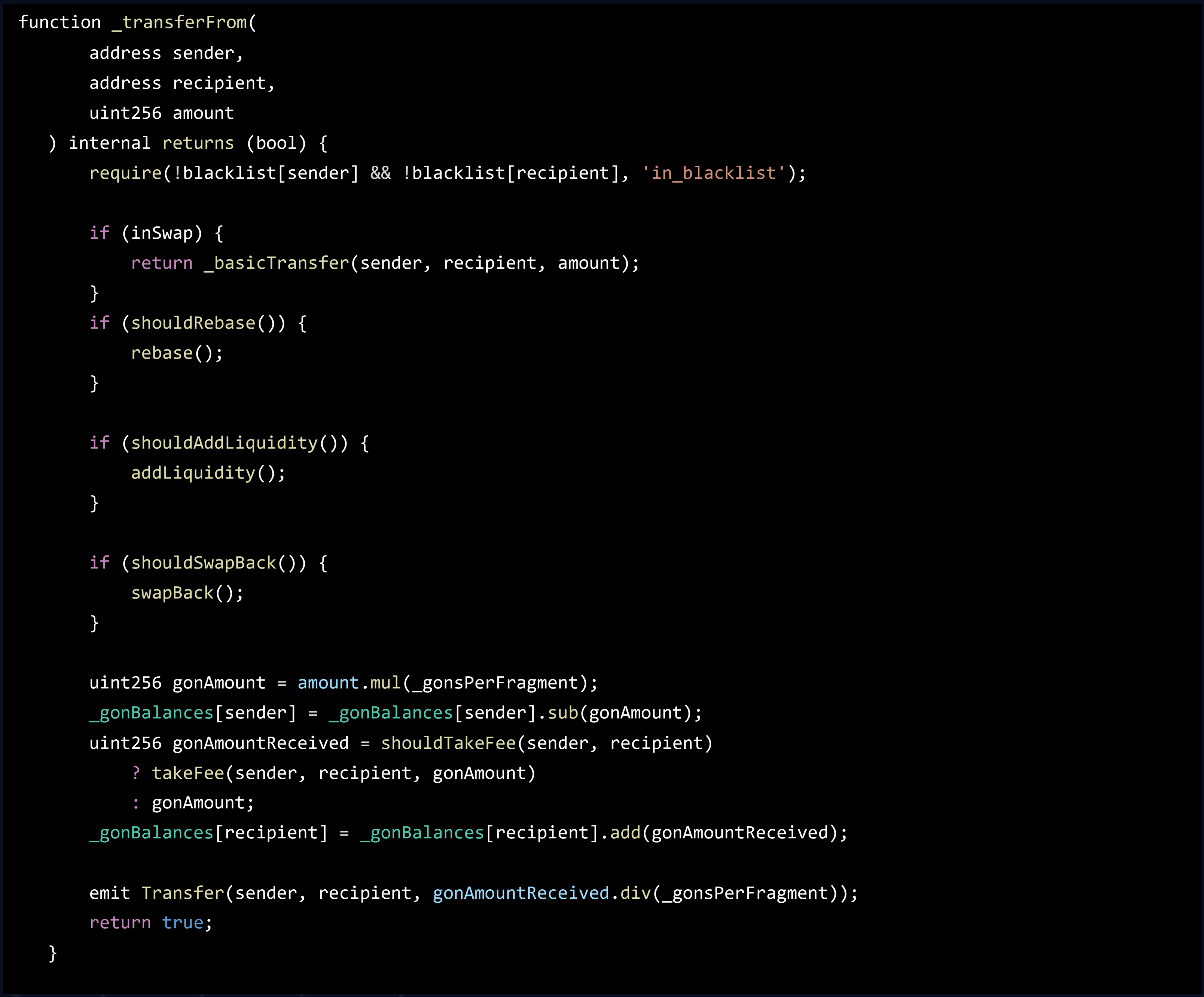
Audit Summary



```
Compiled with solc
Number of lines: 951 (+ 0 in dependencies, + 0 in tests)
Number of assembly lines: 0
Number of contracts: 9 (+ 0 in dependencies, + 0 tests)

Number of optimization issues: 15
Number of informational issues: 48
Number of low issues: 04
Number of medium issues: 0
Number of high issues: 0
ERCs: ERC20, ERC2612

+---------------------+-------------+---------------+-------------------+--------------+--------------------+
|        Name         | # functions |     ERCS      |    ERC20 info     | Complex code |      Features      |
+---------------------+-------------+---------------+-------------------+--------------+--------------------+
|     SafeMathInt     |      6      |               |                   |      No      |                    |
|       SafeMath      |      7      |               |                   |      No      |                    |
|   IPancakeSwapPair  |      27     | ERC20,ERC2612 |     ∞ Minting     |      No      |                    |
|                     |             |               | Approve Race Cond. |              |                    |
|                     |             |               |                   |              |                    |
|  IPancakeSwapRouter |      24     |               |                   |      No      |    Receive ETH     |
| IPancakeSwapFactory |      8      |               |                   |      No      |                    |
|        CROCO        |      51     |     ERC20     |     No Minting    |     Yes      |    Receive ETH     |
|                     |             |               | Approve Race Cond. |              |      Send ETH      |
|                     |             |               |                   |              | Tokens interaction |
|                     |             |               |                   |              |      Assembly      |
+---------------------+-------------+---------------+-------------------+--------------+--------------------+
```

● Low-Risk

1) Contract contains Reentrancy vulnuerabilities



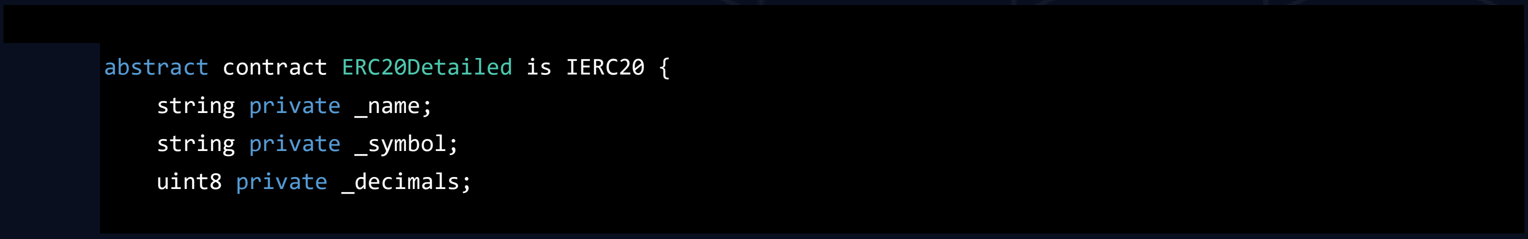
```
function _transferFrom(
       address sender,
       address recipient,
       uint256 amount
   ) internal returns (bool) {
       require(!blacklist[sender] && !blacklist[recipient], 'in_blacklist');

       if (inSwap) {
           return _basicTransfer(sender, recipient, amount);
       }
       if (shouldRebase()) {
           rebase();
       }

       if (shouldAddLiquidity()) {
           addLiquidity();
       }

       if (shouldSwapBack()) {
           swapBack();
       }

       uint256 gonAmount = amount.mul(_gonsPerFragment);
       _gonBalances[sender] = _gonBalances[sender].sub(gonAmount);
       uint256 gonAmountReceived = shouldTakeFee(sender, recipient)
           ? takeFee(sender, recipient, gonAmount)
           : gonAmount;
       _gonBalances[recipient] = _gonBalances[recipient].add(gonAmountReceived);

       emit Transfer(sender, recipient, gonAmountReceived.div(_gonsPerFragment));
       return true;
   }
```

Recommendation

Apply the check-effects-interaction pattern

2) State variable shadowing

Detection of state variables shadowed .



```
abstract contract ERC20Detailed is IERC20 {
    string private _name;
    string private _symbol;
    uint8 private _decimals;
```

Recommendation

Remove the state variable shadowing.

3) Functions that send Ether to arbitary destinations

Unprotected call to a function sending Ether to arbitary address.

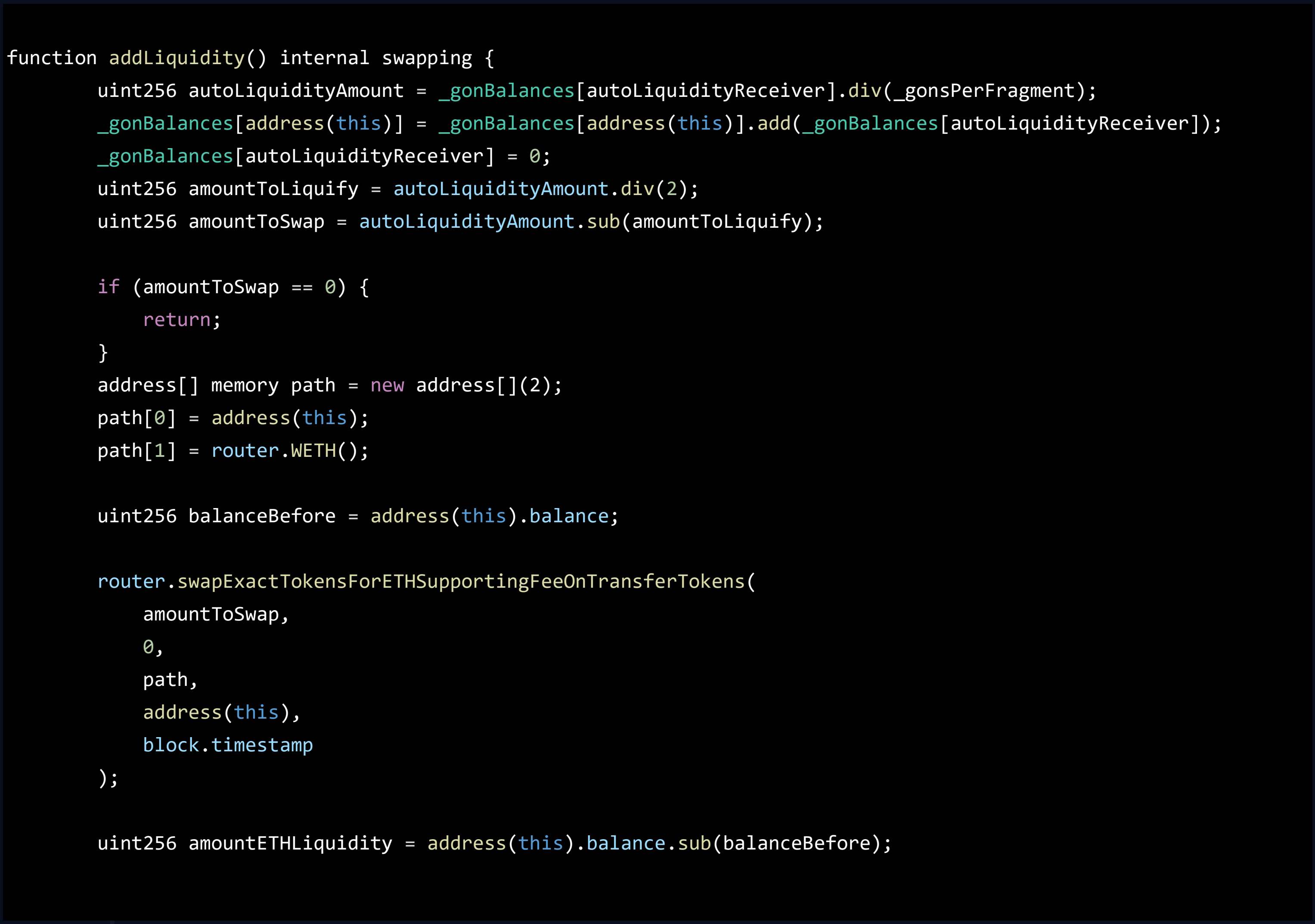
```
function swapBack() internal swapping {
        uint256 amountToSwap = _gonBalances[address(this)].div(_gonsPerFragment);

        if (amountToSwap == 0) {
            return;
        }

        uint256 balanceBefore = address(this).balance;
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = router.WETH();

        router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            amountToSwap,
            0,
            path,
            address(this),
            block.timestamp
        );

        uint256 amountETHTogameTreasuryAndSIF = address(this).balance.sub(balanceBefore);

        (bool success, ) = payable(gameTreasuryReceiver).call{
            value:
amountETHTogameTreasuryAndSIF.mul(gameTreasuryFee).div(gameTreasuryFee.add(CROCOInsuranceFundFee)),
            gas: 30000
        }('');
        (success, ) = payable(CROCOInsuranceFundReceiver).call{
            value: amountETHTogameTreasuryAndSIF.mul(CROCOInsuranceFundFee).div(
                gameTreasuryFee.add(CROCOInsuranceFundFee)
            ),
            gas: 30000
        }('');
    }
```

Recommendation

Ensure that an arbitary user cannot withdraw unauthorized funds

4) Unused return

The return value of an external call is not stored in a local or state variable.

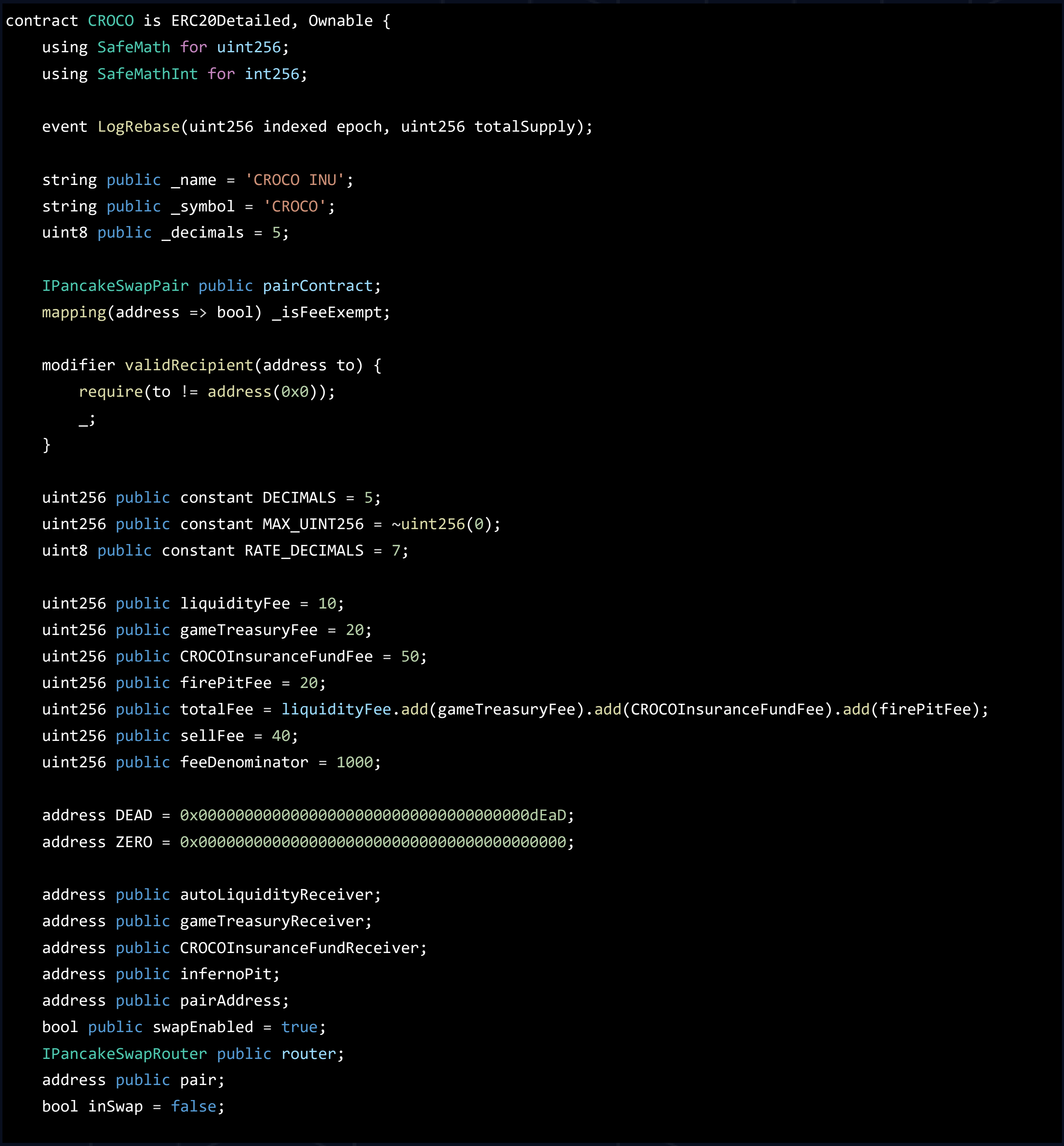


```
function addLiquidity() internal swapping {
        uint256 autoLiquidityAmount = _gonBalances[autoLiquidityReceiver].div(_gonsPerFragment);
        _gonBalances[address(this)] = _gonBalances[address(this)].add(_gonBalances[autoLiquidityReceiver]);
        _gonBalances[autoLiquidityReceiver] = 0;
        uint256 amountToLiquify = autoLiquidityAmount.div(2);
        uint256 amountToSwap = autoLiquidityAmount.sub(amountToLiquify);

        if (amountToSwap == 0) {
            return;
        }
        address[] memory path = new address[](2);
        path[0] = address(this);
        path[1] = router.WETH();

        uint256 balanceBefore = address(this).balance;

        router.swapExactTokensForETHSupportingFeeOnTransferTokens(
            amountToSwap,
            0,
            path,
            address(this),
            block.timestamp
        );

        uint256 amountETHLiquidity = address(this).balance.sub(balanceBefore);
```

Recommendation

Ensure that all the return values of function calls are used.

Manual Audit (Contract Function)



```
contract CROCO is ERC20Detailed, Ownable {
    using SafeMath for uint256;
    using SafeMathInt for int256;

    event LogRebase(uint256 indexed epoch, uint256 totalSupply);

    string public _name = 'CROCO INU';
    string public _symbol = 'CROCO';
    uint8 public _decimals = 5;

    IPancakeSwapPair public pairContract;
    mapping(address => bool) _isFeeExempt;

    modifier validRecipient(address to) {
        require(to != address(0x0));
        _;
    }

    uint256 public constant DECIMALS = 5;
    uint256 public constant MAX_UINT256 = ~uint256(0);
    uint8 public constant RATE_DECIMALS = 7;

    uint256 public liquidityFee = 10;
    uint256 public gameTreasuryFee = 20;
    uint256 public CROCOInsuranceFundFee = 50;
    uint256 public firePitFee = 20;
    uint256 public totalFee = liquidityFee.add(gameTreasuryFee).add(CROCOInsuranceFundFee).add(firePitFee);
    uint256 public sellFee = 40;
    uint256 public feeDenominator = 1000;

    address DEAD = 0x000000000000000000000000000000000000dEaD;
    address ZERO = 0x0000000000000000000000000000000000000000;

    address public autoLiquidityReceiver;
    address public gameTreasuryReceiver;
    address public CROCOInsuranceFundReceiver;
    address public infernoPit;
    address public pairAddress;
    bool public swapEnabled = true;
    IPancakeSwapRouter public router;
    address public pair;
    bool inSwap = false;
```

Important Points To Consider

✓ Verified contract source

✓ Token is sellable (not a honeypot) at this time

✗ Ownership renounced or source does not contain an owner contract

✗ Source does not contain a fee modifier

✗ Source does not contain a mint function

✗ Buy fee is less than 10% (10%)

✗ Sell fee is less than 10% (14%)

✓ Owner/creator wallet contains less than 10% of circulating token supply (4.82%)

About Expelee

Expelee is a community driven organisation dedicated to fostering an anti-rug movement. We're here to keep investment safe from fraudsters. We've encountered several rug pulls and know how it feels to be duped, which is why we don't want anybody else to go through the same experience. We are here to raise awareness through our services so that the future of cryptocurrency can be rug-free.

The auditing process focuses to the following considerations with collaboration of an expert team:

- Functionality test of the Smart Contract to determine if proper logic has been followed throughout the whole process.
- Manually detailed examination of the code line by line by experts.
- Live test by multiple clients using Test net.
- Analysing failure preparations to check how the Smart
- Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.

Social Media

/Expelee

/ExpeleeOfficial

/expelee-co