



Smart Contract Audit

FOR
COCK

DATED : 5 June 23'



AUDIT SUMMARY

Project name – COCK

Date: 5 June, 2023

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:

A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :

The code has undergone static analysis using Slither.

Testnet version:

The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:

<https://testnet.bscscan.com/address/0x7faa60F387Cb657b72FCb0a577E89066CE1CbF15#code>



Token Information

Token Name : COCK

Token Symbol: COCK

Decimals: 18

Token Supply: 1,000,000,000,000

Token Address:

0x2A23ba69221c5e16c343009ECE4138f2EC5c5A27

Checksum:

baed5e343712dc8f3ffa8db9dd3629a3e2e2f2ca

Owner:

0x03E2427859119E497EB856a166F616a2Ce5f8c88

(at time of writing the audit)

Deployer:

0x03E2427859119E497EB856a166F616a2Ce5f8c88



TOKEN OVERVIEW

Fees:

Buy Fees: 0%

Sell Fees: 0%

Transfer Fees: 0%

Fees Privilege: No fees

Ownership: Not Owned

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: - Initial distribution of the token



AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
 - Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
 - Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
 - Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
 - Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
 - Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.
-

VULNERABILITY CHECKLIST

- | | |
|------------------------------------|-------------------------------|
| ✓ Return values of low-level calls | ✓ Gasless Send |
| ✓ Private modifier | ✓ Using block.timestamp |
| ✓ Multiple Sends | ✓ Re-entrancy |
| ✓ Using Suicide | ✓ Tautology or contradiction |
| ✓ Gas Limitand Loops | ✓ Timestamp Dependence |
| ✓ Address hardcoded | ✓ Revert/require functions |
| ✓ Exception Disorder | ✓ Use of tx.origin |
| ✓ Using inline assembly | ✓ Integer overflow/underflow |
| ✓ Divide before multiply | ✓ Dangerous strict equalities |
| ✓ Missing Zero Address Validation | ✓ Using SHA3 |
| ✓ Compiler version not fixed | ✓ Using throw |
-



CLASSIFICATION OF RISK

Severity

Description

◆ Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
◆ High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
◆ Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
◆ Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
◆ Gas Optimization / Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity

Found

◆ Critical	0
◆ High-Risk	0
◆ Medium-Risk	0
◆ Low-Risk	0
◆ Gas Optimization / Suggestions	0



INHERITANCE TREE

SafeMath

InitializableERC20

POINTS TO NOTE

- Fees are 0 (static)
 - Owner is not able to blacklist an arbitrary address.
 - Owner is not able to disable trades
 - Owner is not able to limit buy/sell/transfer/wallet amounts
 - Owner is not able to mint new tokens
 - token is already initialized and can not be initialized again
-



CONTRACT ASSESMENT

Contract	Type	Bases			
----- ----- ----- ----- -----					
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
SafeMath Library					
└	mul	Internal	🔒		
└	div	Internal	🔒		
└	divCeil	Internal	🔒		
└	sub	Internal	🔒		
└	add	Internal	🔒		
└	sqrt	Internal	🔒		
InitializableERC20 Implementation					
└	init	Public	!	●	NO !
└	transfer	Public	!	●	NO !
└	balanceOf	Public	!		NO !
└	transferFrom	Public	!	●	NO !
└	approve	Public	!	●	NO !
└	allowance	Public	!		NO !

Legend

Symbol	Meaning
----- -----	
●	Function can modify state
💰	Function is payable



STATIC ANALYSIS

```
SafeMath.div(uint256,uint256) (contracts/Token.sol#33-36) is never used and should be removed
SafeMath.divCeil(uint256,uint256) (contracts/Token.sol#38-46) is never used and should be removed
SafeMath.mul(uint256,uint256) (contracts/Token.sol#22-31) is never used and should be removed
SafeMath.sqrt(uint256) (contracts/Token.sol#59-66) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.17 (contracts/Token.sol#13) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Parameter InitializableERC20.init(address,uint256,string,string,uint8)._creator (contracts/Token.sol#87) is not in mixedCase
Parameter InitializableERC20.init(address,uint256,string,string,uint8)._totalSupply (contracts/Token.sol#87) is not in mixedCase
Parameter InitializableERC20.init(address,uint256,string,string,uint8)._name (contracts/Token.sol#87) is not in mixedCase
Parameter InitializableERC20.init(address,uint256,string,string,uint8)._symbol (contracts/Token.sol#87) is not in mixedCase
Parameter InitializableERC20.init(address,uint256,string,string,uint8)._decimals (contracts/Token.sol#87) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
(contracts/Token.sol analyzed (2 contracts with 94 detectors) - 11 result(s) found)
```

Result => A static analysis of contract's source code has been performed using slither,

No major issues were found in the output



FUNCTIONAL TESTING

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

1- Adding liquidity (passed):

<https://testnet.bscscan.com/tx/0x5619534bfafd202965472e447a79a330d04d0c76515998b910085300442aef0b>

2- Buying (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x4455a625e870dfbb464d96a594632a4f1b611e247e4ff521d24fe6ddf8adba92>

3- Selling (0% tax) (passed):

<https://testnet.bscscan.com/tx/0x53b425826c1f7d46c4039a75fcfde56d49e265583542bf26184ce30e874e8067>

4- Transferring 0% tax) (passed):

<https://testnet.bscscan.com/tx/0x10d2b9c62baea8a3946beb2eefc88a5ba8ae23d6fdf27c148fd24a3fcce6b1ce>



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 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 Auditace 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 Auditace 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 Auditace team disclaims any liability for the resulting losses.



ABOUT AUDITACE

We specialize in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.



<https://auditace.tech/>



https://t.me/Audit_Ace



https://twitter.com/auditace_



<https://github.com/Audit-Ace>
