



Smart Contract Audit

FOR
Origin Defi

DATED : 17 MAR 23'



AUDIT SUMMARY

Project name – Origin Defi

Date: 17 March, 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 Testnet network:

all tests were done on Bsc Testnet network, each test has its transaction has attached to it.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

<https://testnet.bscscan.com/address/0xd6bAE20da67665Fc51849168F69C8BE3f3d1758c#code>



Token Information

Token Name : Origin Defi

Token Symbol: Origin

Decimals: 18

Token Supply: 5,000,000

Token Address:

0x4239E50b0beFe3B7d61d041a06A96e271eB092E0

Checksum:

c8d108a655abb372341f477ba9f044e219f2b281

Owner:

0xfD581d514e28Cb50FbF7B8BB4C0Df8601AC20B2C
(AT THE TIME OF WRITING AUDIT)



TOKEN OVERVIEW

Fees:

Buy Fees: 0%

Sell Fees: 0%

Transfer Fees: 0%

Fees Privilige: None

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: None



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.

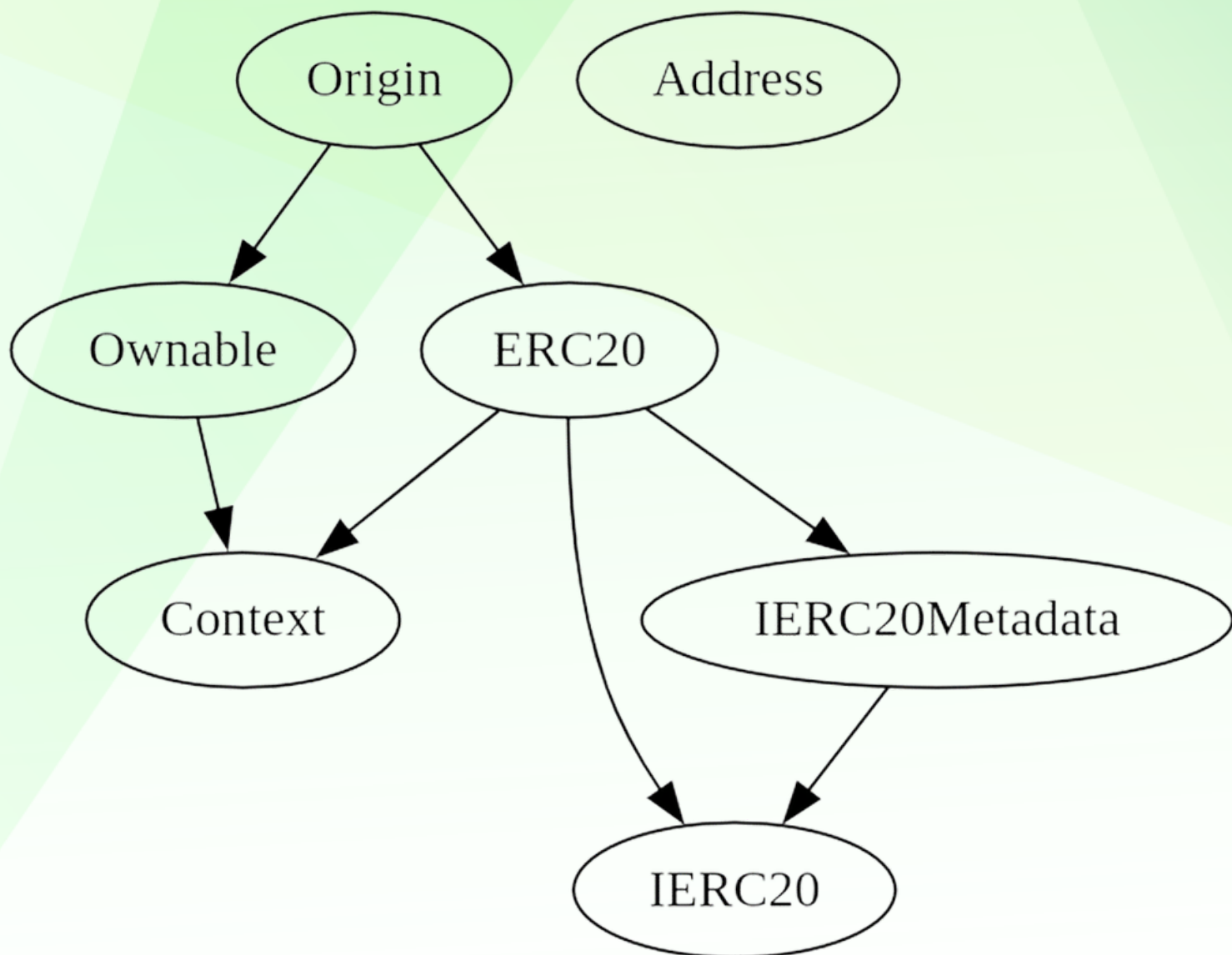
Findings

Severity

Found

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

INHERITANCE TREE



POINTS TO NOTE

- Owner is not able to set buy/sell/transfer fees (0% static)
 - **Owner must enable trading for investors in order for them to be able to trade**
 - Owner is not able to set max buy/sell/transfer/hold amount
 - Owner is not able to blacklist an arbitrary wallet
 - Owner is not able to disable trades
 - Owner is not able to mint new tokens
-



Trades will not be enabled right away

Owner of the contract must call “enableTrading” function in order to enable buys, sells and transfers for non-authorized wallets. Since contract is developed and owned by pinksale’s safu dev its guaranteed that trades will be enabled.

TOKEN DISTRIBUTION

It should be noted that the owner currently holds 100% of the total supply. However, information about the distribution of these tokens is not available, and it is recommended that investors exercise caution when considering this aspect.























CONTRACT ASSESMENT

Contract	Type	Bases			
:-----: :-----: :-----: :-----: :-----:					
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
Context Implementation					
└	_msgSender	Internal	🔒		
└	_msgData	Internal	🔒		
IERC20 Interface					
└	totalSupply	External	!		NO!
└	balanceOf	External	!		NO!
└	transfer	External	!	🛑	NO!
└	allowance	External	!		NO!
└	approve	External	!	🛑	NO!
└	transferFrom	External	!	🛑	NO!
IERC20Metadata Interface IERC20					
└	name	External	!		NO!
└	symbol	External	!		NO!
└	decimals	External	!		NO!
Ownable Implementation Context					
└	<Constructor>	Public	!	🛑	NO!
└	owner	Public	!		NO!
└	renounceOwnership	Public	!	🛑	onlyOwner
└	transferOwnership	Public	!	🛑	onlyOwner
Address Library					
└	sendValue	Internal	🔒	🛑	
ERC20 Implementation Context, IERC20, IERC20Metadata					
└	<Constructor>	Public	!	🛑	NO!
└	name	Public	!		NO!
└	symbol	Public	!		NO!
└	decimals	Public	!		NO!
└	totalSupply	Public	!		NO!
└	balanceOf	Public	!		NO!
└	transfer	Public	!	🛑	NO!
└	allowance	Public	!		NO!
└	approve	Public	!	🛑	NO!
└	transferFrom	Public	!	🛑	NO!
└	increaseAllowance	Public	!	🛑	NO!



CONTRACT ASSESMENT

```

| ^ | decreaseAllowance | Public ! |  | NO ! |
| ^ | _transfer | Internal  |  | |
| ^ | _mint | Internal  |  | |
| ^ | _burn | Internal  |  | |
| ^ | _approve | Internal  |  | |
| ^ | _beforeTokenTransfer | Internal  |  | |
| ^ | _afterTokenTransfer | Internal  |  | |
| | | | |
| **Origin** | Implementation | ERC20, Ownable | | |
| ^ | <Constructor> | Public ! |  | ERC20 |
| ^ | <Receive Ether> | External ! |  | NO ! |
| ^ | claimStuckTokens | External ! |  | onlyOwner |
| ^ | excludeFromFees | External ! |  | onlyOwner |
| ^ | isExcludedFromFees | Public ! | | NO ! |
| ^ | enableTrading | External ! |  | onlyOwner |
| ^ | _transfer | Internal  |  | |

```

Legend

Symbol	Meaning
:-----: -----	
	Function can modify state
	Function is payable



STATIC ANALYSIS

```
Context._msgData() (contracts/Token.sol#30-33) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#274-289) 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#23) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (contracts/Token.sol#114-125):
- (success) = recipient.call{value: amount}() (contracts/Token.sol#120)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Redundant expression "this (contracts/Token.sol#31)" inContext (contracts/Token.sol#25-34)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
```

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

No issues found



FUNCTIONAL TESTING

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

1- Adding Liquidity (**Passed**):

liquidity added on Pancakeswap V2:

<https://testnet.bscscan.com/tx/0x45ae81d7f9668de91bc3b319dbfab31140ce987e283a372c108cbeb42dbf3bf5>

2- Buying when trading not enabled (owner%)(**Passed**):

<https://testnet.bscscan.com/tx/0x586627fae56ae38edf27bb9ac2f82d0a4c3764705a4383293ce0baa7bbe50679>

3- Selling when trading not enabled (0%)(Passed):

<https://testnet.bscscan.com/tx/0xd4d8835100d8bf50fb63e0678439c37c39cf29b3f6aca3d26e11498962978ff8>

4- Transferring when trading not enabled (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x267bf5498818bf6467fd1a1cd37f1c334d81de726539e0bf403c1ce3b6115a14>

5- Buying when trading enabled (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xd04c07aabbdd0f8823cc76963030c80eaa28385e68bdad83a560e6580e8781ea>



FUNCTIONAL TESTING

6- Selling when trading enabled (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0x3de3e37267a89928d66de66b684b9848d596989b3adc5d27d8a0cb258ca41587cd>

7- Transferring when trading enabled (0% tax) (**passed**):

<https://testnet.bscscan.com/tx/0xdc8f108de92e3e7b2149ea77207dc5c89b54165cbf703a6edf7eaa679b69c3d4>



MANUAL TESTING

No Issues Found





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>
