AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

BEN

DATED : 26 MAY 23'

AUDIT SUMMARY

Project name – BEN

Date: 26 May, 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	1	0	0	0

USED TOOLS

Tools:

1.Manual Review: The code has undergone a line-by-line review by the **Ace** team.

2.ETH Test Network: All tests were conducted on the ETH 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/token/0x6c7bC33704416F0BfcA7D9f5c11C595CA0a0ba70

Token Information

Name : Ben

Symbol : BEN

Decimals: 18

Network: BSC

Token Type:BEP20

Token Address:
0xCFA43Ed34809a2fe1bf3552F1918f362C96F3c52

Owner:
0xBfad7c2332E071cb5BFCEf45a7D3939Cf41B9F64
(at time of writing the audit)

Deployer:0xBfad7c2332E071cb5BFCEf45a7D3939Cf41B9F64

Token Information

Fees:

Buy Fees: 0%

Sell Fees: 0%

Transfer Fees: 0%

Fees Privilige: No fees

Ownership :

0xe11d0Ea7e24DCDaB70225beFA94E42c6574D354A

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Priviliges:- Enabling trades

- Fee whitelist

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

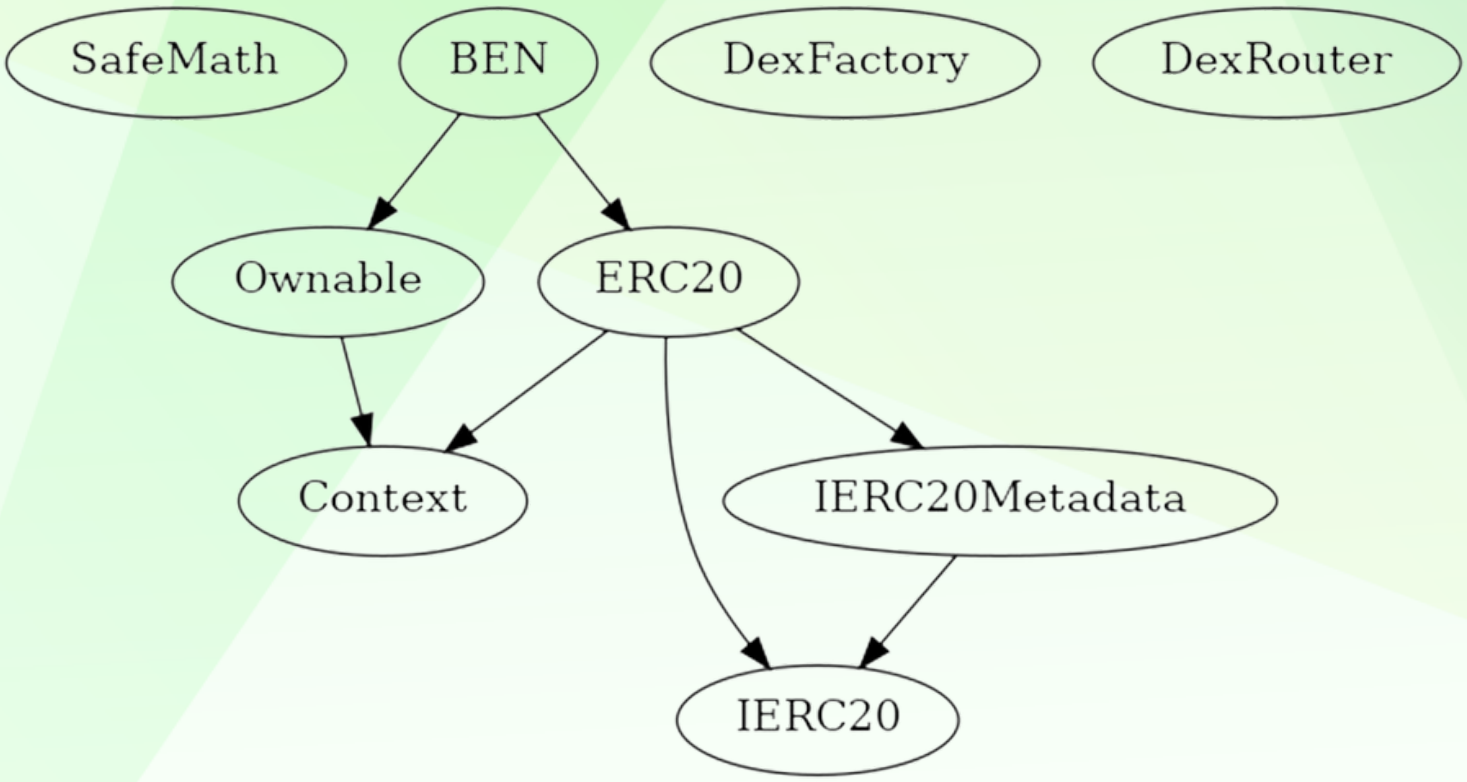
CLASSIFICATION OF RISK

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	1
Medium-Risk	0
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



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
- **Owner must enable trades**

CONTRACT ASSESMENT

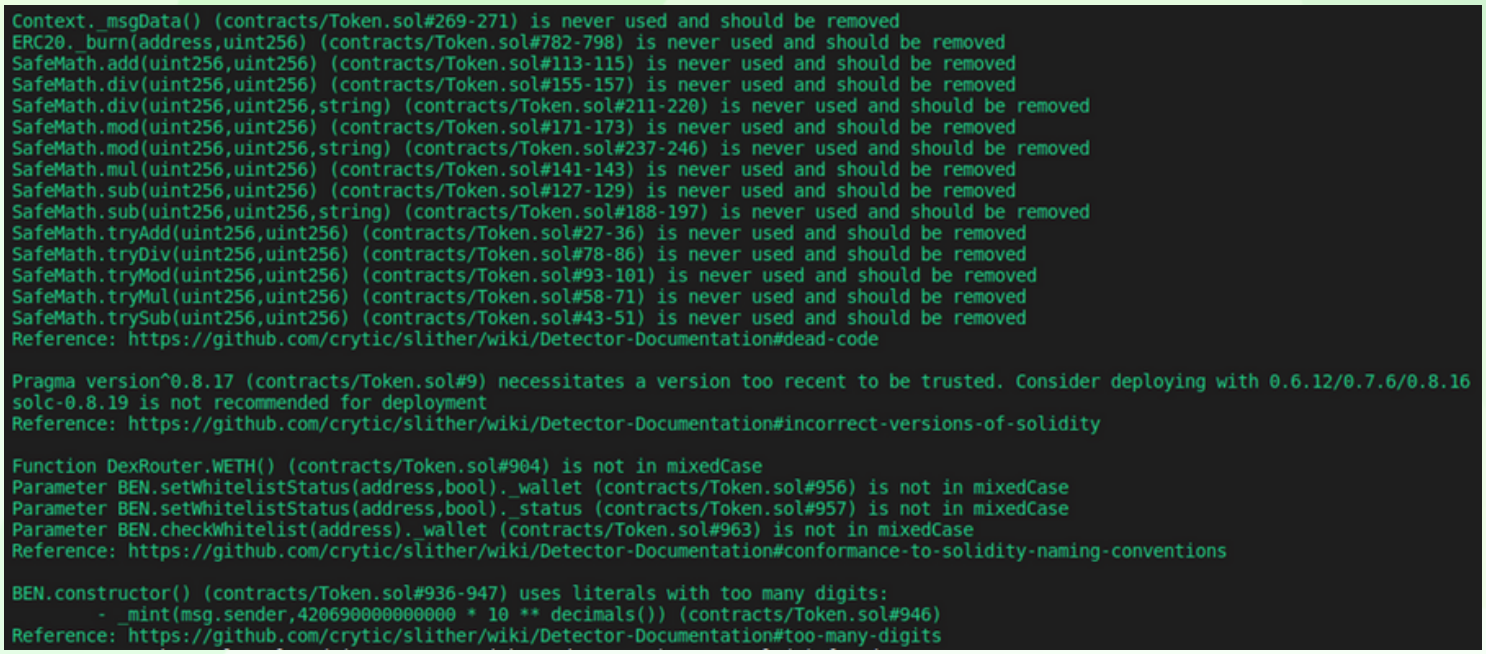
Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
SafeMath	Library			
└	tryAdd	Internal 🔒		
└	trySub	Internal 🔒		
└	tryMul	Internal 🔒		
└	tryDiv	Internal 🔒		
└	tryMod	Internal 🔒		
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	sub	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗
└	owner	Public ❗		NO ❗
└	_checkOwner	Internal 🔒		
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_transferOwnership	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 ❗

CONTRACT ASSESMENT

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 ❗
└	decreaseAllowance	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	_mint	Internal 🔒	🛑	
└	_burn	Internal 🔒	🛑	
└	_approve	Internal 🔒	🛑	
└	_spendAllowance	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	
└	_afterTokenTransfer	Internal 🔒	🛑	
DexFactory	Interface			
└	createPair	External ❗	🛑	NO ❗
DexRouter	Interface			
└	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗
└	addLiquidityETH	External ❗	💵	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
BEN	Implementation	ERC20, Ownable		
└	<Constructor>	Public ❗	🛑	ERC20
└	enableTrading	External ❗	🛑	onlyOwner
└	setWhitelistStatus	External ❗	🛑	onlyOwner
└	checkWhitelist	External ❗		NO ❗
└	_transfer	Internal 🔒	🛑	
Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS



```
Context._msgData() (contracts/Token.sol#269-271) is never used and should be removed
ERC20._burn(address,uint256) (contracts/Token.sol#782-798) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#113-115) is never used and should be removed
SafeMath.div(uint256,uint256) (contracts/Token.sol#155-157) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#211-220) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#171-173) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#237-246) is never used and should be removed
SafeMath.mul(uint256,uint256) (contracts/Token.sol#141-143) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#127-129) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#188-197) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#27-36) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#78-86) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#93-101) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#58-71) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#43-51) 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#9) 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

Function DexRouter.WETH() (contracts/Token.sol#904) is not in mixedCase
Parameter BEN.setWhitelistStatus(address,bool)._wallet (contracts/Token.sol#956) is not in mixedCase
Parameter BEN.setWhitelistStatus(address,bool)._status (contracts/Token.sol#957) is not in mixedCase
Parameter BEN.checkWhitelist(address)._wallet (contracts/Token.sol#963) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

BEN.constructor() (contracts/Token.sol#936-947) uses literals with too many digits:
        - _mint(msg.sender,420690000000000 * 10 ** decimals()) (contracts/Token.sol#946)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

Static Analysis

an static analysis of the code were performed using slither. No issues were found

FUNCTIONAL TESTING

Router (PCS V2):
0xD99D1c33F9fC3444f8101754aBC46c52416550D1

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x55b415e834d775f4dfe24d563bba597eeb1b54b91dd0726dfbda2ae99d6f375b

2- Buying (0% tax) (passed):
https://testnet.bscscan.com/tx/0xb9f3d7b805d14a82be96067d71c4c884db7ac6524b7bd4cd83d379d8230896b8

3- Selling (0% tax) (passed):
https://testnet.bscscan.com/tx/0x365d710cc2e10631c0385cf80d89d900777d542dbe88fc1ec33a2cb5f7e95f0a

4- Transferring 0% tax) (passed):
https://testnet.bscscan.com/tx/0xd0fc17ca214e0f920527ad7830976a771ab1a621a71277ca30d8e48e0b2ea558

FUNCTIONAL TESTING

Centralization – Owner must enable trades

Severity: High

function: enableTrading

Status: Solved (Safu Contract)

Overview:

Owner must enable trades for investors manually. If trades remain disabled, no one would be able to buy/sell/transfer tokens (except owner)

```
function enableTrading() external onlyOwner {
    require(!tradingEnabled, "Trading is already enabled");
    tradingEnabled = true;
    startTradingBlock = block.number;
}
```

Suggestion

To mitigate this issue, there are several options:

- Enable trades before starting the presale

- Transfer ownership of the contract to a trust 3rd party like pinksale (safu dev) in order to guarantee that trades will be enabled

- create a mechanism which will enable trades automatically after a preiod of time

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 specializes 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