AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Bigfoot Moe

DATED : 18 May 23'

AUDIT SUMMARY

Project name – Bigfoot Moe

Date: 18 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	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 done on BSC Test 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/token/0xECAD48Ca59ffF0D28f6c7237d396618d70602A19

Payment Mode:
https://bscscan.com/tx/0x7167149f61d827cbb46f1423c48db1e3605367044000ad20b087574113059466

Token Information

Token Name : Bigfoot Moe

Token Symbol: MOE

Decimals: 18

Token Supply:100,000,000,000,000

Token Address:
0x8431A160d63dD1ac42c3E0E2c32bf3e2FbdfD0B2

Checksum:
ec2b367923ced2e994343ffd6e8ee63ea882ee88

Owner:
0x2Ef2211ab3ee40414BF553A3BFfbE3Be37970cDa

TOKEN OVERVIEW

Fees:

Buy Fees: upto 0%

Sell Fees: upto 0 %

Transfer Fees: 0%

Fees Privilige: none

Ownership :0x2Ef2211ab3ee40414BF553A3BFfbE3Be37970cD

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Priviliges: initial distribution of tokens

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

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

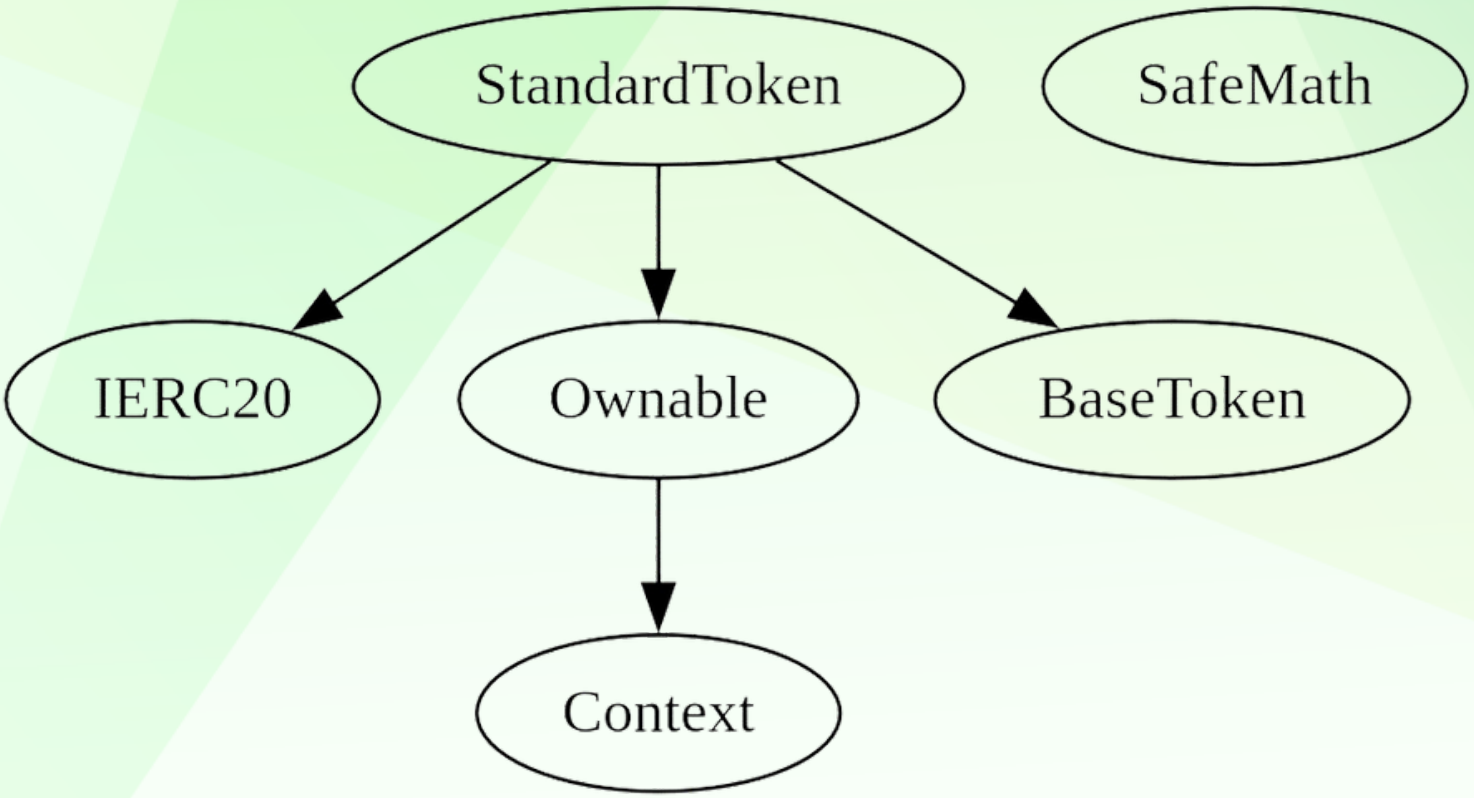
CLASSIFICATION OF RISK

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 change current fees (0% for buy/sell and 0% for transfers)
- 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

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
└	totalSupply	External ❗		NO❗
└	balanceOf	External ❗		NO❗
└	transfer	External ❗	🛑	NO❗
└	allowance	External ❗		NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO❗
└	owner	Public ❗		NO❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	_setOwner	Private 🔐	🛑	
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 🔒		
BaseToken	Implementation			
StandardToken	Implementation	IERC20, Ownable, BaseToken		
└	<Constructor>	Public ❗	💵	NO❗

CONTRACT ASSESMENT

└	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 🔒	🛑	
└	_setupDecimals	Internal 🔒	🛑	
└	_beforeTokenTransfer	Internal 🔒	🛑	

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Contract locking ether found:
        Contract StandardToken (contracts/Token.sol#476-805) has payable functions:
         - StandardToken.constructor(string,string,uint8,uint256) (contracts/Token.sol#489-501)
        But does not have a function to withdraw the ether
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#contracts-that-lock-ether

StandardToken.allowance(address,address).owner (contracts/Token.sol#571) shadows:
        - Ownable.owner() (contracts/Token.sol#159-161) (function)
StandardToken._approve(address,address,uint256).owner (contracts/Token.sol#764) shadows:
        - Ownable.owner() (contracts/Token.sol#159-161) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

Context._msgData() (contracts/Token.sol#118-120) is never used and should be removed
SafeMath.div(uint256,uint256) (contracts/Token.sol#349-351) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#405-414) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#365-367) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#431-440) is never used and should be removed
SafeMath.mul(uint256,uint256) (contracts/Token.sol#335-337) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#321-323) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#221-230) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#272-280) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#287-295) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#252-265) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#237-245) is never used and should be removed
StandardToken._burn(address,uint256) (contracts/Token.sol#737-748) is never used and should be removed
StandardToken._setupDecimals(uint8) (contracts/Token.sol#782-784) 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#469) 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

Variable StandardToken._totalSupply (contracts/Token.sol#487) is too similar to StandardToken.constructor(string,string,uint8,uint256).totalSupply_ (contracts/
Token.sol#493)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

StandardToken._name (contracts/Token.sol#484) should be immutable
StandardToken._symbol (contracts/Token.sol#485) should be immutable
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-immutable
```

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

All the functionalities have been tested, no issues were found

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x0ff32ebb97d2bbad1e889b6b7642c48a61ba3665fdd687b1dff24f45c507a956

2- Buying when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x83676c5d56fe4db37198e47a1d45ebb3b8a2bdbb31f1447aa85ad3ea87684231

3- Selling when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xde4c51528ea225c9221d127bbc93701b851a1cf9e24bfa007d0a63b681e1e7cb

4- Transferring when excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xdb4a13dc53b985d0e4e21ae14480e07239db2117520bd611889e59b60d1eb439

5- Buying when not excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x3feea49718ad4e898cfc0cb326437ec1ca0c75e91624eb9168fe78e161ede3da

6- Selling when not excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0xa338dc9f4280d735c35f60515191ba2cd7f796cc41a9fa9278305a3a7f0d29b1

FUNCTIONAL TESTING

7- Transferring when not excluded (0% tax) (passed):
https://testnet.bscscan.com/tx/0x01772416e4e16137cee693e3c46af1aa52549a322eba9da727f0397c77a45c92

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