auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

SHIBELON 2.0

DATED : 18 July 23'

MANUAL TESTING

Centralization – Trades are disabled by default

Severity: High

function: launch

Status: Not Resolved

Overview:

Owner must enable trades manually, otherwise holders wont be able to buy/sell/transfer tokens.

```
function launch() external onlyOwner {
    require(startTradeBlock == 0, "already started");
    startTradeBlock = block.number;
}
```

Suggestion

It is suggested to either enable trades prior to presale, or transfer ownership of the contract to a trusted 3rd party like a certified Pinksale safu developer.

AUDIT SUMMARY

Project name – SHIBELON 2.0

Date: 18 July, 2023

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

Audit Status: **Passed with High Risk**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	1	2	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/token/0xb0495c49D4744FC6E7D84a2e5968bf955923AB6f

Token Information

Token Name: SHIBELON 2.0

Token Symbol: ShibElon 2.0

Decimals: 18

Token Supply: 420,690,000,00

Token Address:
0xeBaaAb988b7Bc5a5a07A4C19ecECfdD1f8EdE54E

Checksum:
5efaecff6741c3a8a9c215080d43b3aee201e187

Owner:
0x667f28c090e2Ef778439c74AF7789F24fb498A2E
(at time of writing the audit)

Deployer:
0xCbbB74c36De813C3F39347f3dD5A29323BbF26cE

TOKEN OVERVIEW

Fees:

Buy Fees: 0-25%

Sell Fees: 0-25%

Transfer Fees: 0%

Fees Privilege: owner

Ownership: owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: no

Blacklist: No

Other Privileges: Initial distribution of the tokens

enabling trades

modifying fees

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

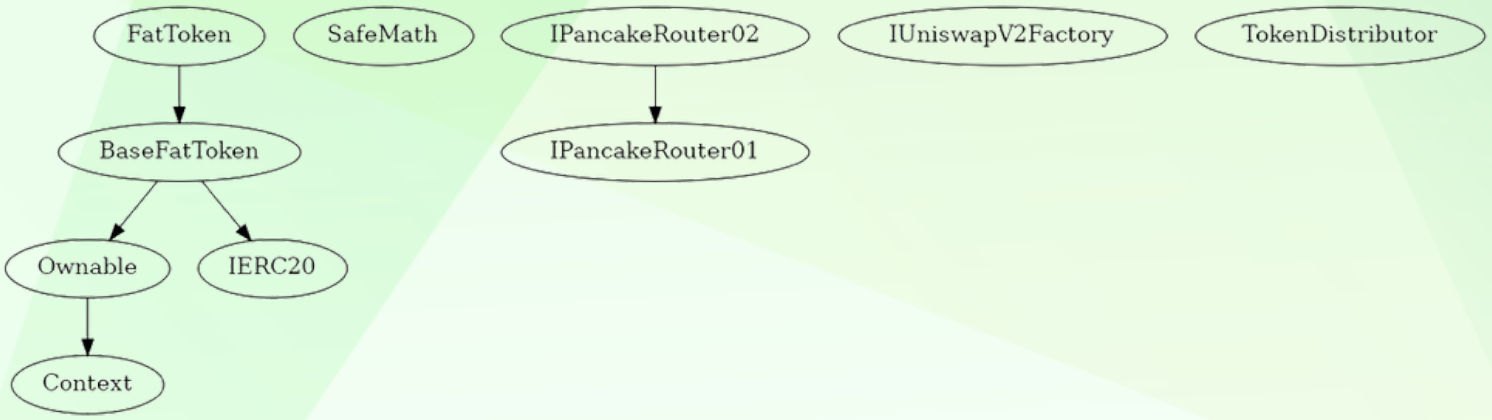
CLASSIFICATION OF RISK

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	1
Medium-Risk	2
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- Owner is able to change current fee structure (0-25% for buy and sell and 0% for transfers)
- Owner is not able to blacklist an arbitrary address.
- Owner is not able to set max wallet/transfer/buy/sell
- Owner is not able to mint new tokens
- **Owner must enable trades manually**

CONTRACT ASSESMENT

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
└	_msgSender	Internal 🔒		
└	_msgData	Internal 🔒		
Ownable	Implementation	Context		
└	<Constructor>	Public ❗	🛑	NO ❗
└	renounceOwnership	Public ❗	🛑	onlyOwner
└	transferOwnership	Public ❗	🛑	onlyOwner
└	owner	Public ❗		NO ❗
SafeMath	Library			
└	add	Internal 🔒		
└	sub	Internal 🔒		
└	sub	Internal 🔒		
└	mul	Internal 🔒		
└	div	Internal 🔒		
└	div	Internal 🔒		
└	mod	Internal 🔒		
└	mod	Internal 🔒		
IERC20	Interface			
└	name	External ❗		NO ❗
└	symbol	External ❗		NO ❗
	totalSupply	External ❗		NO ❗
	decimals	External ❗		NO ❗
	balanceOf	External ❗		NO ❗
	transfer	External ❗	🛑	NO ❗
	allowance	External ❗		NO ❗
	approve	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
IPancakeRouter01	Interface			
	factory	External ❗		NO ❗
└	WETH	External ❗		NO ❗

CONTRACT ASSESMENT

| └ | addLiquidity | External ❗ | 🛑 |NO ❗
└	addLiquidityETH	External ❗	🛑	NO ❗
IPancakeRouter02	Interface	IPancakeRouter01		
└	swapExactTokensForTokensSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	NO ❗
IUniswapV2Factory	Interface			
└	feeTo	External ❗	NO ❗
└	feeToSetter	External ❗	NO ❗
└	getPair	External ❗	NO ❗
└	allPairs	External ❗		NO ❗
└	allPairsLength	External ❗		NO ❗
└	createPair	External ❗	🛑	NO ❗
└	setFeeTo	External ❗	🛑	NO ❗
└	setFeeToSetter	External ❗	🛑	NO ❗
BaseFatToken	Implementation	IERC20, Ownable		
└	setFundAddress	External ❗	🛑	onlyOwner
└	changeSwapLimit	External ❗	🛑	onlyOwner
└	changeWalletLimit	External ❗	🛑	onlyOwner
└	launch	External ❗	🛑	onlyOwner
└	disableSwapLimit	Public ❗	🛑	onlyOwner
└	disableWalletLimit	Public ❗	🛑	onlyOwner
└	disableChangeTax	Public ❗	🛑	onlyOwner
└	completeCustoms	External ❗	🛑	onlyOwner
└	transfer	External ❗	🛑	NO ❗
└	transferFrom	External ❗	🛑	NO ❗
└	balanceOf	Public ❗	NO ❗
└	allowance	Public ❗	NO ❗
└	approve	Public ❗	🛑	NO ❗
└	_approve	Private 🔐	🛑	
└	setFeeWhiteList	External ❗	🛑	onlyOwner
└	multi_bclist	Public ❗	🛑	onlyOwner
TokenDistributor	Implementation			
└	<Constructor>	Public ❗	🛑	NO ❗

CONTRACT ASSESMENT

FatToken	Implementation	BaseFatToken		
└	<Constructor>	Public ❗	🛑	NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	transferFrom	Public ❗	🛑	NO ❗
└	setkb	Public ❗	🛑	onlyOwner
└	isReward	Public ❗		NO ❗
└	setAirDropEnable	Public ❗	🛑	onlyOwner
└	_basicTransfer	Internal 🔒	🛑	
└	setAirdropNumbs	Public ❗	🛑	onlyOwner
└	setEnableTransferFee	Public ❗	🛑	onlyOwner
└	_transfer	Private 🔐	🛑	
└	setTransferFee	Public ❗	🛑	onlyOwner
└	_tokenTransfer	Private 🔐	🛑	
└	swapTokenForFund	Private 🔐	🛑	lockTheSwap
└	_takeTransfer	Private 🔐	🛑	
└	setSwapPairList	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Reentrancy in FatToken._transfer(address,address,uint256) (contracts/Token.sol#489-561):
        External calls:
        - swapTokenForFund(numTokensSellToFund,swapFee) (contracts/Token.sol#544)
                - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
        External calls sending eth:
        - swapTokenForFund(numTokensSellToFund,swapFee) (contracts/Token.sol#544)
                - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
                - _swapRouter.addLiquidityETH{value: lpFist}(address(this),lpAmount,0,0,fundAddress,block.timestamp) (contracts/Token.sol#667-671)
        State variables written after the call(s):
        - _tokenTransfer(from,to,amount,takeFee,isSell,isTransfer) (contracts/Token.sol#560)
                - _balances[to] = _balances[to] + tAmount (contracts/Token.sol#698)
                - _balances[sender] = _balances[sender] - tAmount (contracts/Token.sol#578)
        Event emitted after the call(s):
        - Transfer(sender,to,tAmount) (contracts/Token.sol#699)
                - _tokenTransfer(from,to,amount,takeFee,isSell,isTransfer) (contracts/Token.sol#560)
Reentrancy in FatToken.swapTokenForFund(uint256,uint256) (contracts/Token.sol#627-695):
        External calls:
        - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
        External calls sending eth:
        - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
        - _swapRouter.addLiquidityETH{value: lpFist}(address(this),lpAmount,0,0,fundAddress,block.timestamp) (contracts/Token.sol#667-671)
        Event emitted after the call(s):
        - Failed_AddLiquidityETH() (contracts/Token.sol#670)
Reentrancy in FatToken.transferFrom(address,address,uint256) (contracts/Token.sol#438-444):
        External calls:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#439)
                - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
        External calls sending eth:
        - _transfer(sender,recipient,amount) (contracts/Token.sol#439)
                - address(fundAddress).transfer(fundAmount) (contracts/Token.sol#663)
                - _swapRouter.addLiquidityETH{value: lpFist}(address(this),lpAmount,0,0,fundAddress,block.timestamp) (contracts/Token.sol#667-671)
        State variables written after the call(s):
        - _allowances[sender][msg.sender] = _allowances[sender][msg.sender] - amount (contracts/Token.sol#441)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-4

Variable IPancakeRouter01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (contracts/Token.sol#158) is too simil
ar to IPancakeRouter01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (contracts/Token.sol#159)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

BaseFatToken.deadAddress (contracts/Token.sol#247) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

BaseFatToken._mainPair (contracts/Token.sol#258) should be immutable
BaseFatToken._swapRouter (contracts/Token.sol#254) should be immutable
BaseFatToken.currency (contracts/Token.sol#225) should be immutable
BaseFatToken.currencyIsEth (contracts/Token.sol#215) should be immutable
BaseFatToken.decimals (contracts/Token.sol#244) should be immutable
BaseFatToken.enableKillBlock (contracts/Token.sol#218) should be immutable
BaseFatToken.enableOffTrade (contracts/Token.sol#217) should be immutable
BaseFatToken.enableRewardList (contracts/Token.sol#219) should be immutable
BaseFatToken.name (contracts/Token.sol#242) should be immutable
BaseFatToken.symbol (contracts/Token.sol#243) should be immutable
BaseFatToken.totalSupply (contracts/Token.sol#245) should be immutable
FatToken._tokenDistributor (contracts/Token.sol#352) should be immutable
FatToken.enableTransferFee (contracts/Token.sol#478) 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

1- Adding liquidity (passed):

https://testnet.bscscan.com/tx/0x9289040f077ed7192c8b1224ea8298603c8f6e97917fde234c4d0f7cc66bf20a

2- Buying when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0x4c010e6d78def6dd0e3507800760c3fc2491366c5a5f3ed4c3143668a6647295

3- Selling when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0x0c8c6dd04d197f4e7c4fb53b8293c36d99607a076f495df89917052229fa2250

4- Transferring when excluded from fees (0% tax) (passed):

https://testnet.bscscan.com/tx/0x724351d959c54ee9aaa99ff00e04332be3a8e1182bc3edca96451a09bc0cc961

5- Buying when not excluded from fees (0-25% tax) (passed):

https://testnet.bscscan.com/tx/0x034d72e8896d22e03b6d425c4cb919f3a267985997d903083159a918b9310c97

6- Selling when not excluded from fees (0-25% tax) (passed):

https://testnet.bscscan.com/tx/0xdb052a696cdae4c0e93b910cdbfa206d2c749af1788f931ef4afafe8b4201767

FUNCTIONAL TESTING

7- Transferring when not excluded from fees (1% tax) (passed):

https://testnet.bscscan.com/tx/0x4bc763d38db9586bfff2e950f8b8f027b120930b72c976f0b7528b6b0273c0c4

8- Internal swap (passed):

All of below features can be seen in the given tx

- Fund wallet received BNB
- Auto-liquidity
- Airdrop (maximum 3 wallets airdroped 1 wei)
- Burn

https://testnet.bscscan.com/tx/0xdb052a696cdae4c0e93b910cdbfa206d2c749af1788f931ef4afafe8b4201767

MANUAL TESTING

Centralization – Trades are disabled by default

Severity: High

function: launch

Status: Not Resolved

Overview:

Owner must enable trades manually, otherwise holders wont be able to buy/sell/transfer tokens.

```
function launch() external onlyOwner {
    require(startTradeBlock == 0, "already started");
    startTradeBlock = block.number;
}
```

Suggestion

It is suggested to either enable trades prior to presale, or transfer ownership of the contract to a trusted 3rd party like a certified Pinksale safu developer.

MANUAL TESTING

Centralization – Excessive fees

Severity: Medium

function: completeCustoms

Status: Not Resolved

Overview:

Owner is able to set up to 25% tax for buy or sells separately.

```
    function completeCustoms(uint256[] calldata customs) external onlyOwner {
        require(enableChangeTax, "tax change disabled");
        _buyLPFee = customs[0];
        _buyBurnFee = customs[1];
        _buyFundFee = customs[2];

        _sellLPFee = customs[3];
        _sellBurnFee = customs[4];
        _sellFundFee = customs[5];

        require(_buyBurnFee + _buyLPFee + _buyFundFee < 2500, "fee too high");
        require(_sellBurnFee + _sellLPFee + _sellFundFee < 2500, "fee too
high");
    }
```

Suggestion

Ensure that fees are within a safe and reasonable range. Usually 0-10% (For each type of tax) is suggested by Pinksale safu criteria.

MANUAL TESTING

Centralization – EOA receiving LP tokens

Severity: Medium

function: completeCustoms

Status: Not Resolved

Overview:

fundAddress which is an EOA in the contract, receives LP tokens generated from auto-liquidity. This LP tokens could be used to remove a portion of liquidity pool (BNB and SHIBELON)

```
if (lpAmount > 0 && lpFist > 0) {
    // add the liquidity
    try _swapRouter.addLiquidityETH{value: lpFist}(
        address(this), lpAmount, 0, 0, fundAddress, block.timestamp
    ) {} catch {
        emit Failed_AddLiquidityETH();
    }
}
```

Suggestion

Ensure that new LP tokens are either burnt (sending to an in accessible wallet such as address zero) or get locked

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