auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

XSHIB

DATED : 27 July 23'

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

function: enableTrading

Status: Resolved (Contract is owned by safu developer)

Overview:

Owner of the contract must enable trades manually for investors, otherwise no one would be able to buy/sell/transfer their tokens.

```
function enableTrading() external onlyOwner {
  require(!tradingEnabled, "Cannot re-enable trading");
  tradingEnabled = true;
  providingLiquidity = true;
}
```

Suggestion

It's suggested to either enable trades prior to presale, or transfer ownership of the contract to a certified pinsksale safu developer to guarantee enabling of trades.

AUDIT SUMMARY

Project name –XSHIB

Date: 27 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	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/token/0x9e7520B1039288FE2E6116315fE7dC31498c0c05

Token Information

Token Name : X-Shiba

Token Symbol: XSHIB

Decimals: 18

Token Supply: 100,000,000

Token Address:
0xFA10A77109e9a291554879D46f71d00639ca1345

Checksum:
e0d2779ee2e0b4797dfcc28d5dcbb06faa5a4bee

Owner:
0x9fA316d096e46A8BAfae21c5451b30BF49D384DF
(at time of writing the audit)

Deployer:
0x9fA316d096e46A8BAfae21c5451b30BF49D384DF

TOKEN OVERVIEW

Fees:

Buy Fees: 0-10%

Sell Fees: 0-10%

Transfer Fees: 0-10%

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

modifying fees

enabling trades

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

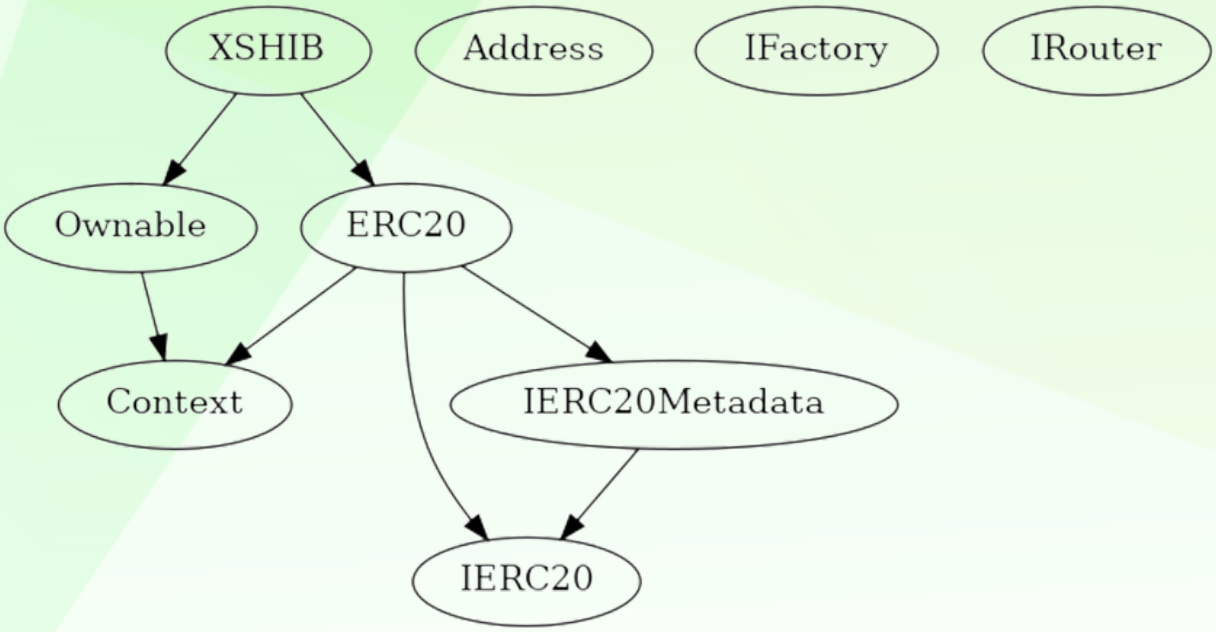
CLASSIFICATION OF RISK

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	0
Low-Risk	0
Gas Optimization / Suggestions	0

INHERITANCE TREE



POINTS TO NOTE

- **Owner is able to update fees within 0-10% for buy/sell/transfers**
- Owner is not able to blacklist an address
- Owner is not able to disable buy/sell/transfers
- Owner is not able to set max wallet limit and minimum wallet limits
- 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 🔒		
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 ❗
ERC20	Implementation	Context, IERC20, IERC20Metadata		
└	<Constructor>	Public ❗	🛑	NO ❗
└	name	Public ❗		NO ❗

CONTRACT ASSESMENT

└	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 🔒	🛑		
└	_tokengeneration	Internal 🔒	🛑		
└	_approve	Internal 🔒	🛑		
Address	Library				
└	sendValue	Internal 🔒	🛑		
Ownable	Implementation	Context			
└	<Constructor>	Public ❗	🛑	|NO ❗
└	owner	Public ❗		|NO ❗
└	renounceOwnership	Public ❗	🛑	onlyOwner	
└	transferOwnership	Public ❗	🛑	onlyOwner	
└	_setOwner	Private 🔐	🛑		
IFactory	Interface				
└	createPair	External ❗	🛑	|NO ❗
IRouter	Interface				
└	factory	External ❗		|NO ❗
└	WETH	External ❗		|NO ❗
└	addLiquidityETH	External ❗	💸	|NO ❗
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External ❗	🛑	|NO ❗
XSHIB	Implementation	ERC20, Ownable			
└	<Constructor>	Public ❗	🛑	ERC20	
└	approve	Public ❗	🛑	|NO ❗
└	transferFrom	Public ❗	🛑	|NO ❗
└	increaseAllowance	Public ❗	🛑	|NO ❗

CONTRACT ASSESMENT

└	decreaseAllowance	Public ❗	🛑	NO ❗
└	transfer	Public ❗	🛑	NO ❗
└	_transfer	Internal 🔒	🛑	
└	Liquify	Private 🔐	🛑	lockTheSwap
└	swapTokensForETH	Private 🔐	🛑	
└	addLiquidity	Private 🔐	🛑	
└	updateLiquidityProvide	External ❗	🛑	onlyOwner
└	SetBuyTaxes	External ❗	🛑	onlyOwner
└	SetSellTaxes	External ❗	🛑	onlyOwner
└	UpdateMarketingWallet	External ❗	🛑	onlyOwner
└	updateLiquidityTreshhold	External ❗	🛑	onlyOwner
└	enableTrading	External ❗	🛑	onlyOwner
└	excludeFromFee	External ❗	🛑	onlyOwner
└	includeFromFee	External ❗	🛑	onlyOwner
└	rescueBNB	External ❗	🛑	NO ❗
└	rescueBEP2020	External ❗	🛑	onlyOwner
└	<Receive Ether>	External ❗	💵	NO ❗

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

XSHIB.excludeFromFee(address) (contracts/Token.sol#703-707) compares to a boolean constant:
        -require(bool,string)(exemptFee[account] != true,Account is already excluded) (contracts/Token.sol#704)
XSHIB.includeFromFee(address) (contracts/Token.sol#709-713) compares to a boolean constant:
        -require(bool,string)(exemptFee[account] != false,Account is already included) (contracts/Token.sol#710)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#boolean-equality

Context._msgData() (contracts/Token.sol#23-26) 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#16) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.21 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#334-342):
        - (success) = recipient.call{value: amount}() (contracts/Token.sol#337)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Variable ERC20._balances (contracts/Token.sol#72) is not in mixedCase
Variable ERC20._allowances (contracts/Token.sol#74) is not in mixedCase
Function IRouter.WETH() (contracts/Token.sol#392) is not in mixedCase
Event XSHIBincludeFromFeeUpdated(address) (contracts/Token.sol#446) is not in CapWords
Function XSHIB.Liquify(uint256,XSHIB.Taxes) (contracts/Token.sol#585-623) is not in mixedCase
Function XSHIB.SetBuyTaxes(uint256,uint256) (contracts/Token.sol#662-668) is not in mixedCase
Parameter XSHIB.SetBuyTaxes(uint256,uint256)._marketing (contracts/Token.sol#663) is not in mixedCase
Parameter XSHIB.SetBuyTaxes(uint256,uint256)._liquidity (contracts/Token.sol#664) is not in mixedCase
Function XSHIB.SetSellTaxes(uint256,uint256) (contracts/Token.sol#670-676) is not in mixedCase
Parameter XSHIB.SetSellTaxes(uint256,uint256)._marketing (contracts/Token.sol#671) is not in mixedCase
Parameter XSHIB.SetSellTaxes(uint256,uint256)._liquidity (contracts/Token.sol#672) is not in mixedCase
Function XSHIB.UpdateMarketingWallet(address) (contracts/Token.sol#678-683) is not in mixedCase
Parameter XSHIB.UpdateMarketingWallet(address)._newWallet (contracts/Token.sol#678) is not in mixedCase
Parameter XSHIB.updateLiquidityTreshhold(uint256).new_amount (contracts/Token.sol#685) is not in mixedCase
Constant XSHIB.Contract_Version (contracts/Token.sol#428) is not in UPPER_CASE_WITH_UNDERSCORES
Constant XSHIB.Contract_Dev (contracts/Token.sol#429) is not in UPPER_CASE_WITH_UNDERSCORES
Constant XSHIB.Contract_Edition (contracts/Token.sol#430) is not in UPPER_CASE_WITH_UNDERSCORES
Constant XSHIB.deadWallet (contracts/Token.sol#433-434) is not in UPPER_CASE_WITH_UNDERSCORES
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Redundant expression "this (contracts/Token.sol#24)" inContext (contracts/Token.sol#18-27)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

XSHIB.constructor() (contracts/Token.sol#458-476) uses literals with too many digits:
        - _tokengeneration(msg.sender,100000000 * 10 ** decimals()) (contracts/Token.sol#459)
XSHIB.updateLiquidityTreshhold(uint256) (contracts/Token.sol#685-695) uses literals with too many digits:
        - require(bool,string)(new_amount <= 1000000,Swap threshold amount should be lower or equal to 1% of tokens) (contracts/Token.sol#686-689)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits

XSHIB.pair (contracts/Token.sol#419) should be immutable
XSHIB.router (contracts/Token.sol#418) 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/0x09638612d2c8dc608c5bb2c5c10c8300f6fc1860f2a7c14fd19832e2c32c43ab

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

https://testnet.bscscan.com/tx/0xb9403b1f75fdf71e15dd48ef741d0d0c7a793cc2e609f4a4860c282a7f300d27

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

https://testnet.bscscan.com/tx/0x5827c090b9f69eee80d34c884291cf09abc156ac82d2ca742d39f0772b96df8c

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

https://testnet.bscscan.com/tx/0xc1bffe2cf43bfefbc6ea9b14d3f640f732472d0fcf01a24595b73ce4b0febc6d

5- Buying when not excluded from fees (0-10% tax) (passed):

https://testnet.bscscan.com/tx/0xa0918e0a0ee721523679e9dc06f1b3bf809e974ded929cc596e40707f62ef27d

6- Selling when not excluded from fees (0-10% tax) (passed):

https://testnet.bscscan.com/tx/0x8a0c1c096b41290f194514f4ff6b21e02bc6218d4120d30dbb77d65c4c95bf86

FUNCTIONAL TESTING

7- Transferring (0-10% tax) (passed):

https://testnet.bscscan.com/tx/0x1414b9dd67946aa06dbb070b637f2ec376820a4bfb56491134f5f359357445b2

8- Internal swap(ETH sent to marketing wallet) (passed):

https://testnet.bscscan.com/tx/0x8a0c1c096b41290f194514f4ff6b21e02bc6218d4120d30dbb77d65c4c95bf86

MANUAL TESTING

Centralization – Enabling Trades

Severity: High
function: enableTrading
Status: Resolved (Contract is owned by safu developer)
Overview:
Owner of the contract must enable trades manually for investors, otherwise no one would be able to buy/sell/transfer their tokens.

```
function enableTrading() external onlyOwner {
  require(!tradingEnabled, "Cannot re-enable trading");
  tradingEnabled = true;
  providingLiquidity = true;
}
```

Suggestion

It's suggested to either enable trades prior to presale, or transfer ownership of the contract to a certified pinsksale safu developer to guarantee enabling of trades.

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