expelee

Building the Futuristic Blockchain Ecosystem

SECURITY AUDIT REPORT

SAFUMOON

TOKEN OVERVIEW

Risk Findings

Severity	Found
High	0
Medium	0
Low	5
Informational	0

Centralization Risks

Owner Privileges	Description
Can Owner Set Taxes >25% ?	Not Detected
Owner needs to enable trading ?	Yes, owner needs to enable trades
Can Owner Disable Trades ?	Not Detected
Can Owner Mint ?	Not Detected
Can Owner Blacklist ?	Not Detected
Can Owner set Max Wallet amount ?	Not Detected
Can Owner Set Max TX amount ?	Not Detected

TABLE OF CONTENTS

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	**Passed**
KYC Verification	**-**
Audit Date	**8 June 2023**

CONTRACT DETAILS

Token Name: SafuMoon

Symbol: SMO

Network: Binance Smart Chain

Language: Solidity

Contract Address:
Local File

Total Supply: 10000

Owner's Wallet: Local File

Deployer's Wallet: Local File

Testnet Link:

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch , that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zepplin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and acces control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

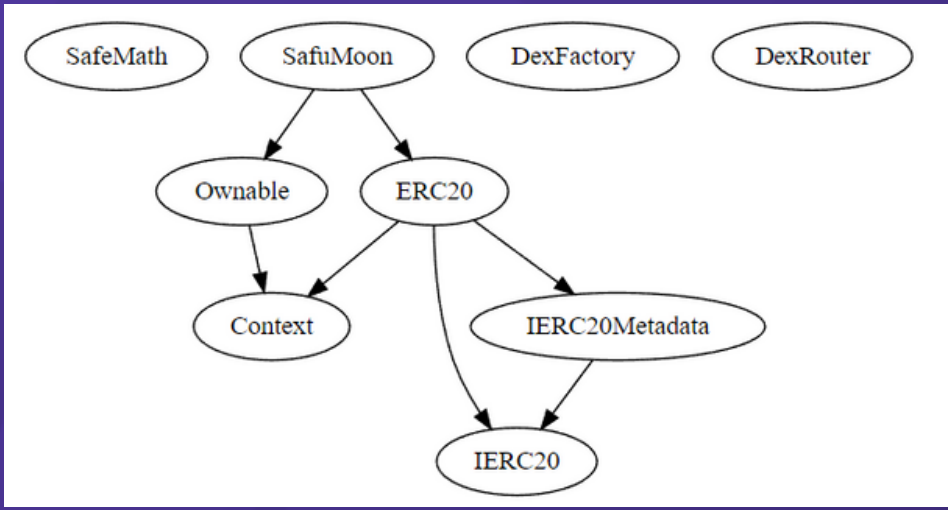
Low Risk

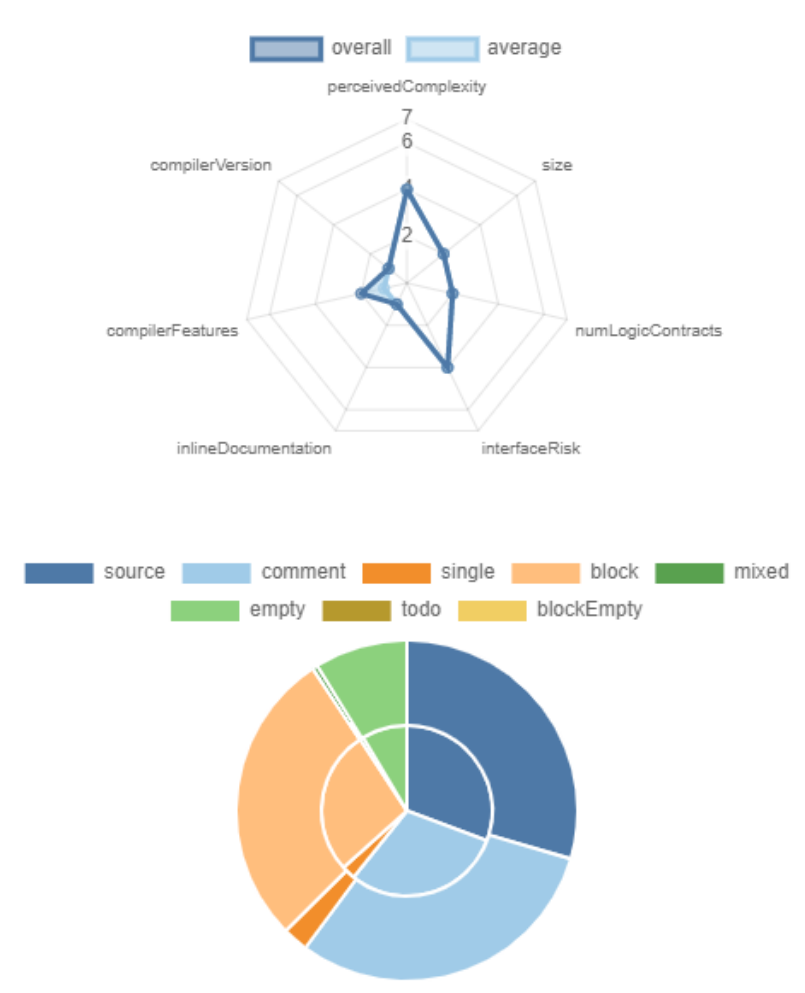
Issues on this level are minor details and warning that can remain unfixed.

Informational

Issues on this level are minor details and warning that can remain unfixed.

INHERITANCE TREES





FUNCTION DETAILS

DexFactory	Interface				
└	createPair	External	!	🔴	NO !
DexRouter	Interface				
└	factory	External	!		NO !
└	WETH	External	!		NO !
└	addLiquidityETH	External	!	💵	NO !
└	swapExactTokensForETHSupportingFeeOnTransferTokens	External	!	🔴	NO !
SafuMoon	Implementation	ERC20, Ownable			
└	<Constructor>	Public	!	🔴	ERC20
└	setmarketingWallet	External	!	🔴	onlyOwner
└	enableTrading	External	!	🔴	onlyOwner
└	setBuyTaxes	External	!	🔴	onlyOwner
└	setSellTaxes	External	!	🔴	onlyOwner
└	setTransferFees	External	!	🔴	onlyOwner
└	setSwapTokensAtAmount	External	!	🔴	onlyOwner
└	toggleSwapping	External	!	🔴	onlyOwner
└	setWhitelistStatus	External	!	🔴	onlyOwner
└	checkWhitelist	External	!		NO !
└	_takeTax	Internal 🔒		🔴	
└	_transfer	Internal 🔒		🔴	
└	internalSwap	Internal 🔒		🔴	
└	swapToETH	Internal 🔒		🔴	
└	withdrawStuckETH	External	!	🔴	onlyOwner
└	withdrawStuckTokens	External	!	🔴	onlyOwner
└	<Receive Ether>	External	!	💵	NO !

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standarts.

Vulnerabilities are dividend into three primary risk categroies:
High
Medium
Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

LOW RISK FINDING

Trade must be enabled by the owner

Severity : Low

Overview

Owner must enable trading to enable public to trade their tokens, otherwise no one would be able to buy /sell their tokens except whitelisted wallets.

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

Recommendation

To mitigate this issue you should enable trading before presale or transfer ownership to safu dev for initial days after presale.

LOW RISK FINDING

Owner can exclude account from fees

Severity : Low

Overview

Excludes/Includes an address from the collection of fees

```
function setWhitelistStatus(address _wallet,bool _status) external onlyOwner {
    whitelisted[_wallet] = _status;
    emit Whitelist(_wallet, _status);
}
```

Recommendation

It is recommended to add additional access control measures, such as multi-factor authentication or time-based restrictions, to limit the number of authorized users who can call these functions. The contract owner account is well secured and only accessible by authorized parties.

LOW RISK FINDING

Owner can change buy and sell fees 5% transfer fee 1% at max

Severity : Low

Overview

Functions that allows the owner of the contract to update the buy/sell/transfer fees of the contract. For buy fees and sell fees maximum limit of 5% and transfer fees maximum limit 1%.

```
function setBuyTaxes(uint256 _marketingTax) external onlyOwner { //@audit-issu
    buyTaxes = _marketingTax;
    require(_marketingTax ≤ 50, "Can not set buy fees higher than 5%");
    emit BuyFeesUpdated(_marketingTax);
}

0 references | Control flow graph | 0940bbc7 | ftrace | funcSig
function setSellTaxes(uint256 _marketingTax) external onlyOwner {
    sellTaxes = _marketingTax;
    require(_marketingTax ≤ 50, "Can not set buy fees higher than 5%");
    emit SellFeesUpdated(_marketingTax);
}

0 references | Control flow graph | d26ed3e3 | ftrace | funcSig
function setTransferFees(uint256 _transferTaxes) external onlyOwner { //@audit
    transferTaxes = _transferTaxes;
    require(_transferTaxes ≤ 10, "Can not set transfer tax higher than 1%");
    emit TransferFeesUpdated(_transferTaxes);
}
```

Recommendation

It is recommended to add additional access control measures, such as multi-factor authentication or time-based restrictions, to limit the number of authorized users who can call these functions.

LOW RISK FINDING

Owner can change swap setting

Severity : Low

Overview

setSwapTokensAtAmount function allows the owner of the contract to update the value of **swapTokensAtAmount**. **toggleSwapping** function allows the contract owner to **enable** or **disable** the automatic **swapping**.

```
function setSwapTokensAtAmount(uint256 _newAmount) external onlyOwner { //@audit-issue
    require(
        _newAmount > 0 && _newAmount ≤ (_totalSupply * 5) / 1000,
        "Minimum swap amount must be greater than 0 and less than 0.5% of total supply!"
    );
    swapTokensAtAmount = _newAmount;
    emit SwapThresholdUpdated(swapTokensAtAmount);
}

0 references | Control flow graph | ef586f71 | ftrace | funcSig
function toggleSwapping() external onlyOwner {
    swapAndLiquifyEnabled = (swapAndLiquifyEnabled) ? false : true;
}
```

Recommendation

If the threshold is set too low, it could result in frequent and unnecessary swaps, which would increase gas fees and potentially lead to losses due to slippage. On the other hand, if the threshold is set too high, it could result in liquidity being insufficient to handle large trades, which could negatively impact the token price and liquidity pool. Be ensure that the contract owner account is well secured and only accessible by authorized parties.

LOW RISK FINDING

Owner can claim stuck tokens except native token

Severity : Low

Overview

Allows the contract owner to withdraw locked or stuck ETH and ERC20 tokens from the contract. The functions are properly restricted to only be executed by the contract owner.

```
function withdrawStuckETH() external onlyOwner { //@audit-issue Owner can withdr
    (bool success, ) = address(msg.sender).call{
        value: address(this).balance
    }("");
    require(success, "transferring ETH failed");
}

0 references | Control flow graph | cb963728 | ftrace | funcSig
function withdrawStuckTokens(address BEP20_token) external onlyOwner {
    bool success = IERC20(BEP20_token).transfer(
        msg.sender,
        IERC20(BEP20_token).balanceOf(address(this))
    );
    require(success, "transferring tokens failed!");
    require(BEP20_token ≠ address(this), "Owner cannot claim native tokens");
    }
```

Recommendation

While the functions are currently restricted to only be called by the contract owner, it is recommended to consider implementing a more robust access control mechanism.

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

www.expelee.com

expeleeofficial
expelee
Expelee
expelee
expelee_official
expelee-co

expelee

Building the Futuristic Blockchain Ecosystem

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 guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee 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 Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway 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 Expelee team disclaims any liability for the resulting losses.