auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

CHAVO

DATED : 11 June 23'

AUDIT SUMMARY

Project name – CHAVO

Date: 11 June, 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 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/address/0x7cFf52A332F50BC96FcF49e6661aE191CB585C02#code

Token Information

Token Name : El Chavo

Token Symbol: CHAVO

Decimals: 18

Token Supply:10,000,000,000,000

Token Address: 0xB727138FF528A73BF75D75437553aa8941977A0b

Checksum:
0928f6e3bab6cfe385f543885d97ae201a11f238

Owner: 0xb0dA84661Ba953a2aB8D086F83068Da796739a0B

Deployer: 0x5545c7557DDCf4f80f37BFFA174106F6E5F0D917

TOKEN OVERVIEW

Fees:

Buy Fees: 0-2%

Sell Fees: 0-2%

Transfer Fees: 0-2%

Fees Privilege: Owner

Ownership: Owned

Minting: None

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: - changing fees

- initial distribution of the 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

- 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

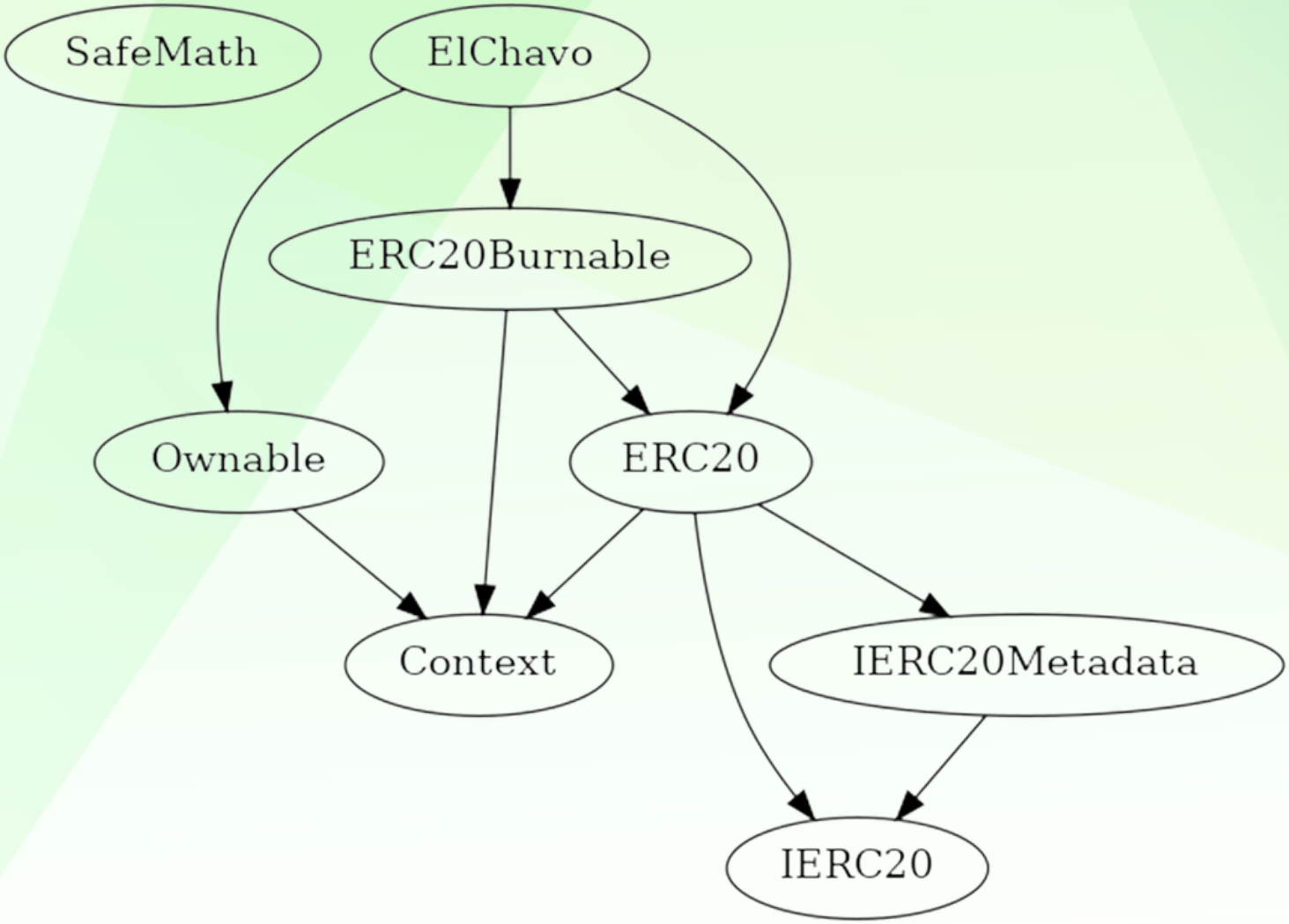
CLASSIFICATION OF RISK

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

INHERITANCE TREE



POINTS TO NOTE

- fees are disabled for all wallets by default, owner include an arbitary wallet in fees
- owner is not able to set buy/sell/transfer fees more than 2% each
- owner is not able to blacklist an arbitrary wallet
- owner is not able to set limit for buy/sell/transfer/holding amounts
- owner is not able to mint new tokens
- owner is not able to disable trades
- owner can exclude/include an address from fees
- owner can update buy/sell/transfer fees
- owner can claim stuck tokens
- owner can transfer ownership
- owner can renounce ownership

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 🔒	🛑	
ERC20Burnable	Implementation	Context, ERC20		
└	burn	Public ❗	🛑	NO ❗
└	burnFrom	Public ❗	🛑	NO ❗
ElChavo	Implementation	ERC20, Ownable, ERC20Burnable		
└	<Constructor>	Public ❗	🛑	ERC20
└	setTaxWallet	External ❗	🛑	onlyOwner
└	setWalletsIncludedFromFee	External ❗	🛑	onlyOwner
└	unsetWalletsIncludedFromFee	External ❗	🛑	onlyOwner
└	setTax	External ❗	🛑	onlyOwner
└	recoverTokensFromContract	External ❗	🛑	onlyOwner
└	recoverEthFromContract	External ❗	🛑	onlyOwner
└	_transfer	Internal 🔒	🛑	
└	burnFrom	Public ❗	🛑	NO ❗

CONTRACT ASSESMENT

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

STATIC ANALYSIS

```
Reentrancy in ElChavo.recoverTokensFromContract(address) (contracts/Token.sol#890-894):
        External calls:
        - IERC20(_tokenAddress).transfer(msg.sender,balance) (contracts/Token.sol#892)
        Event emitted after the call(s):
        - TokensRecovered(balance) (contracts/Token.sol#893)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3

Different versions of Solidity are used:
        - Version used: ['^0.8.0', '^0.8.17']
        - ^0.8.0 (contracts/Token.sol#5)
        - ^0.8.0 (contracts/Token.sol#222)
        - ^0.8.0 (contracts/Token.sol#248)
        - ^0.8.0 (contracts/Token.sol#331)
        - ^0.8.0 (contracts/Token.sol#411)
        - ^0.8.0 (contracts/Token.sol#439)
        - ^0.8.0 (contracts/Token.sol#803)
        - ^0.8.17 (contracts/Token.sol#839)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used

Context._msgData() (contracts/Token.sol#239-241) is never used and should be removed
SafeMath.add(uint256,uint256) (contracts/Token.sol#94-96) is never used and should be removed
SafeMath.div(uint256,uint256,string) (contracts/Token.sol#188-193) is never used and should be removed
SafeMath.mod(uint256,uint256) (contracts/Token.sol#152-154) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (contracts/Token.sol#210-215) is never used and should be removed
SafeMath.sub(uint256,uint256) (contracts/Token.sol#108-110) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (contracts/Token.sol#169-174) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (contracts/Token.sol#23-29) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (contracts/Token.sol#65-70) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (contracts/Token.sol#77-82) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (contracts/Token.sol#48-58) is never used and should be removed
SafeMath.trySub(uint256,uint256) (contracts/Token.sol#36-41) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code

Pragma version^0.8.0 (contracts/Token.sol#5) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#222) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#248) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#331) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#411) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#439) allows old versions
Pragma version^0.8.0 (contracts/Token.sol#803) allows old versions
Pragma version^0.8.17 (contracts/Token.sol#839) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.16
solc-0.8.20 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Parameter ElChavo.setTax(uint256)._tax (contracts/Token.sol#884) is not in mixedCase
Parameter ElChavo.recoverTokensFromContract(address)._tokenAddress (contracts/Token.sol#890) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

Reentrancy in ElChavo.recoverEthFromContract() (contracts/Token.sol#896-900):
        External calls:
        - address(owner()).transfer(balance) (contracts/Token.sol#898)
        Event emitted after the call(s):
        - ETHRecovered(balance) (contracts/Token.sol#899)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-4

ElChavo.constructor() (contracts/Token.sol#857-861) uses literals with too many digits:
        - _mint(msg.sender,10000000000000 * 10 ** decimals()) (contracts/Token.sol#858)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
```

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

1- Adding liquidity (passed):
https://testnet.bscscan.com/tx/0x650f3d834d6cccbaa0edbe7b6d4f3d71a7981832fc3fcd156f950138ae7b95bc

2- Buying (0% tax) when not included in fees (passed):
https://testnet.bscscan.com/tx/0x3f70fd443636921a6cf4d48cb7edd988fbf3b62a728fd3b46820f6fbcf69b17a

3- Selling (0% tax) when not included in fees (passed):
https://testnet.bscscan.com/tx/0xdd5a92f4e797b959478d52284639ad3a0e5aa2480a0a15ffb3fdb4823105364a

4- Transferring (0% tax) when not included in fees(passed):
https://testnet.bscscan.com/tx/0xa4ae6d89418b79ac5a9ddd98bfb19d5c3dcc94f0a01efff7ecc1c5416d72d082

5- Buying when included in fees (0-2% tax) (passed):
https://testnet.bscscan.com/tx/0x8cdded1f31dc2f8b737a9a3a8abf1e4ab0bfd27bdcadcd00629ad2d5440f8e8e

6- Selling when included in fees (0-2% tax) (passed):
https://testnet.bscscan.com/tx/0x90fa7b2e2f7d90b4f7e917362f5192eba8a2948251186c41206c38cde13bdf4b

FUNCTIONAL TESTING

7- Transferring when included in fees (0-2% tax) (passed):

https://testnet.bscscan.com/tx/0xff90dc3a302b52464f8601d546e2040596b1ba9d1d3f7a84ab868ce250014093

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