



# Smart Contract Audit

FOR  
**Smurfs**

DATED : 19 June 23'



# AUDIT SUMMARY

---

**Project name** – Smurfs

**Date:** 19 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/token/0x94035B40df874850be42F8a8e849150CF712421F>

---



# Token Information

---

**Token Name :** The Smurfs

**Token Symbol:** Smurfs

**Decimals:** 12

**Token Supply:** 2,100,000,000,000,000

**Token Address:**

0x98d90e16a4BFB2bd1722811179151af02d85eB76

**Checksum:**

0ac8b43689586ec2f0b310755151bdcd87dba981

**Owner:**

0xb745Eb8F10FD4653042B45015CD92e3D9dbcafb7  
(at time of writing the audit)

**Deployer:**

0xb745Eb8F10FD4653042B45015CD92e3D9dbcafb7

---



# TOKEN OVERVIEW

---

## **Fees:**

Buy Fees: 0-%

Sell Fees: 0-%

Transfer Fees: 0-%

---

**Fees Privilege:** No fees

---

**Ownership:** not owned

---

**Minting:** none

---

**Max Tx Amount/ Max Wallet Amount:** No

---

**Blacklist:** No

---

**Other Privileges:-** 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 is exercised 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 | ✓ Gasless Send                |
| ✓ Private modifier                 | ✓ Using block.timestamp       |
| ✓ Multiple Sends                   | ✓ Re-entrancy                 |
| ✓ Using Suicide                    | ✓ Tautology or contradiction  |
| ✓ Gas Limitand Loops               | ✓ Timestamp Dependence        |
| ✓ Address hardcoded                | ✓ Revert/require functions    |
| ✓ Exception Disorder               | ✓ Use of tx.origin            |
| ✓ Using inline assembly            | ✓ Integer overflow/underflow  |
| ✓ Divide before multiply           | ✓ Dangerous strict equalities |
| ✓ Missing Zero Address Validation  | ✓ Using SHA3                  |
| ✓ Compiler version not fixed       | ✓ 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

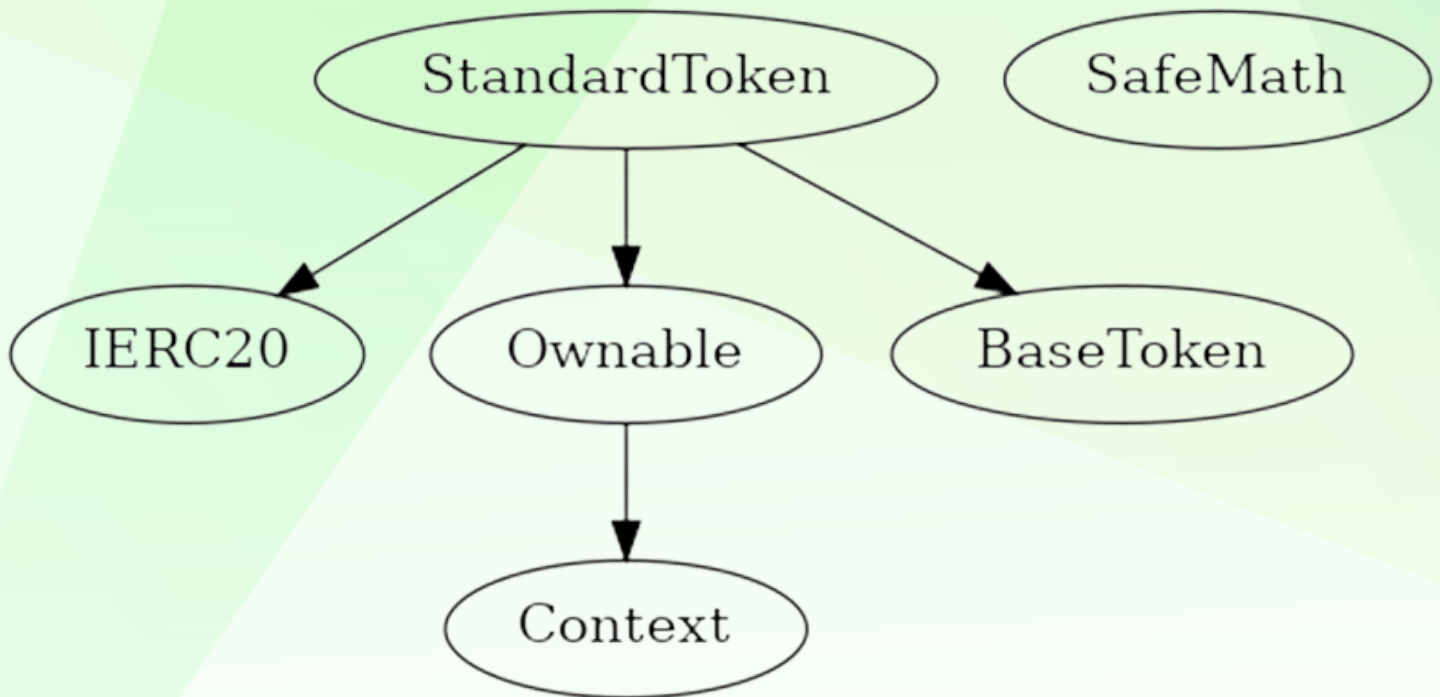
### ◆ Gas Optimization / Suggestions

0



# INHERITANCE TREE

---





# POINTS TO NOTE

---

- Fees are 0 (static)
  - 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	!
└┐	name	Public	!	NO	!
└┐	symbol	Public	!	NO	!



# CONTRACT ASSESMENT

		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

```
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#765) 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#737-749) is never used and should be removed
StandardToken._setupDecimals(uint8) (contracts/Token.sol#783-785) 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
(contracts/Token.sol analyzed: 16 contracts with 81 detectors) - 22 result(s) found
```

**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/0x15825b70f1306f56a6d68d9ca9c3cd6fa0660070fdf3b010df63c3da83f3351d>

**2- Buying (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0xee0943a6f9120ef3e1d3f0754ecacfe01cb1bcfe56bf59edc732b7c73c829366>

**3- Selling (0% tax) (passed):**

<https://testnet.bscscan.com/tx/0xee30015d30219933b97dc6d47e8e0bb33cd5a2d0cbbedee5a972f00adfe50e516>

**4- Transferring 0% tax) (passed):**

<https://testnet.bscscan.com/tx/0x89b574aba606f749a2353eb3d0eea0dbcf769caaf194ad9f4707f0e552beef>

---



# 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 specialize 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://t.me/Audit_Ace)**



**[https://twitter.com/auditace\\_](https://twitter.com/auditace_)**



**<https://github.com/Audit-Ace>**

---