



Smart Contract Audit

FOR
Save The Earth Token

DATED : 19 FEB 23'



AUDIT SUMMARY

Project name – Save The Earth Token

Date: 19 February, 2023

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

Audit Status: Passed (Contract developed by Pinksale Safu Dev)

Issues Found

| Status | Critical | High | Medium | Low | Suggestion |
|--------------|----------|------|--------|-----|------------|
| Open | 0 | 0 | 0 | 0 | 2 |
| 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 done on BSC Test network, each test has its transaction has attached to it.

3- Slither : Static Analysis

Testnet Link: all tests were done using this contract, tests are done on BSC Testnet

<https://testnet.bscscan.com/token/0xCde3990f4E476f7e7F23e8A083Ead4aCe9082877>



Token Information

Token Name : Save The Earth Token

Token Symbol: STE

Decimals: 9

Token Supply: 1,000,000,000

Token Address: Not Provided

Checksum:

F0E4C2F76C58916EC258F246851BEA091D14D4247
A2FC3E18694461B1816E13B

Owner: Not Provided



TOKEN OVERVIEW

Fees:

Buy Fees: can be up to 10%

Sell Fees: can be up to 10%

Transfer Fees: can be up to 10%

Fees Privilege: Owner

Ownership : Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges: None



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

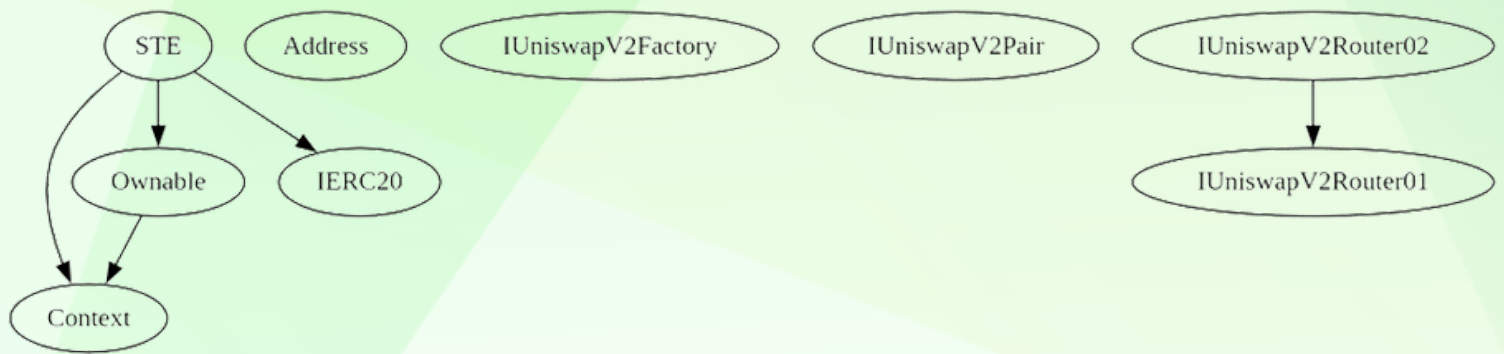
◆ Low-Risk

0

◆ Gas Optimization / Suggestions

2

INHERITANCE TREE





POINTS TO NOTE

- **Owner is not able to set buy/sell/transfer taxes over 10%**
 - **Owner is not able to blacklist an arbitrary wallet**
 - **Owner is not able to set max buy/sell/transfer amounts**
 - **Owner is not able to disable trades**
 - **Owner is not able to mint new tokens**
-























CONTRACT ASSESMENT

| Contract | Type | Bases | | | |
|---|------------------------------|-----------------------|-----------------------|----------------------|-----------|
| :-----: :-----: :-----: :-----: :-----: | | | | | |
| L | **Function Name** | **Visibility** | **Mutability** | **Modifiers** | |
| | | | | | |
| | **Context** | Implementation | | | |
| L | _msgSender | Internal | | | |
| L | _msgData | Internal | | | |
| | | | | | |
| | **Ownable** | Implementation | Context | | |
| L | <Constructor> | Public | ! | | NO ! |
| L | owner | Public | ! | | NO ! |
| L | renounceOwnership | Public | ! | | onlyOwner |
| L | transferOwnership | Public | ! | | onlyOwner |
| | | | | | |
| | **IERC20** | Interface | | | |
| L | totalSupply | External | ! | | NO ! |
| L | balanceOf | External | ! | | NO ! |
| L | transfer | External | ! | | NO ! |
| L | allowance | External | ! | | NO ! |
| L | approve | External | ! | | NO ! |
| L | transferFrom | External | ! | | NO ! |
| | | | | | |
| | **Address** | Library | | | |
| L | isContract | Internal | | | |
| L | sendValue | Internal | | | |
| L | functionCall | Internal | | | |
| L | functionCall | Internal | | | |
| L | functionCallWithValue | Internal | | | |
| L | functionCallWithValue | Internal | | | |
| L | _functionCallWithValue | Private | | | |
| | | | | | |
| | **IUniswapV2Factory** | Interface | | | |
| L | feeTo | External | ! | | NO ! |
| L | feeToSetter | External | ! | | NO ! |
| L | getPair | External | ! | | NO ! |
| L | allPairs | External | ! | | NO ! |
| L | allPairsLength | External | ! | | NO ! |
| L | createPair | External | ! | | NO ! |
| L | setFeeTo | External | ! | | NO ! |
| L | setFeeToSetter | External | ! | | NO ! |
| | | | | | |
| | **IUniswapV2Pair** | Interface | | | |



CONTRACT ASSESMENT

```
|  | name | External ! | | NO ! |
|  | symbol | External ! | | NO ! |
|  | decimals | External ! | | NO ! |
|  | totalSupply | External ! | | NO ! |
|  | balanceOf | External ! | | NO ! |
|  | allowance | External ! | | NO ! |
|  | approve | External ! |  | NO ! |
|  | transfer | External ! |  | NO ! |
|  | transferFrom | External ! |  | NO ! |
|  | DOMAIN_SEPARATOR | External ! | | NO ! |
|  | PERMIT_TYPEHASH | External ! | | NO ! |
|  | nonces | External ! | | NO ! |
|  | permit | External ! |  | NO ! |
|  | MINIMUM_LIQUIDITY | External ! | | NO ! |
|  | factory | External ! | | NO ! |
|  | token0 | External ! | | NO ! |
|  | token1 | External ! | | NO ! |
|  | getReserves | External ! | | NO ! |
|  | price0CumulativeLast | External ! | | NO ! |
|  | price1CumulativeLast | External ! | | NO ! |
|  | kLast | External ! | | NO ! |
|  | burn | External ! |  | NO ! |
|  | swap | External ! |  | NO ! |
|  | skim | External ! |  | NO ! |
|  | sync | External ! |  | NO ! |
|  | initialize | External ! |  | NO ! |
|  |  |  |  |  |
| **IUniswapV2Router01** | Interface | | |
|  | factory | External ! | | NO ! |
|  | WETH | External ! | | NO ! |
|  | addLiquidity | External ! |  | NO ! |
|  | addLiquidityETH | External ! |  | NO ! |
|  | removeLiquidity | External ! |  | NO ! |
|  | removeLiquidityETH | External ! |  | NO ! |
|  | removeLiquidityWithPermit | External ! |  | NO ! |
|  | removeLiquidityETHWithPermit | External ! |  | NO ! |
|  | swapExactTokensForTokens | External ! |  | NO ! |
|  | swapTokensForExactTokens | External ! |  | NO ! |
|  | swapExactETHForTokens | External ! |  | NO ! |
|  | swapTokensForExactETH | External ! |  | NO ! |
|  | swapExactTokensForETH | External ! |  | NO ! |
```

CONTRACT ASSESMENT

```

|  | swapETHForExactTokens | External ! |  | NO! |
|  | quote | External ! | | NO! |
|  | getAmountOut | External ! | | NO! |
|  | getAmountIn | External ! | | NO! |
|  | getAmountsOut | External ! | | NO! |
|  | getAmountsIn | External ! | | NO! |
|  |  |
|  |  |
| **IUniswapV2Router02** | Interface | IUniswapV2Router01 |  |
|  | removeLiquidityETHSupportingFeeOnTransferTokens | External ! |  | NO! |
|  | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External ! |  | NO! |
|  | swapExactTokensForTokensSupportingFeeOnTransferTokens | External ! |  | NO! |
|  | swapExactETHForTokensSupportingFeeOnTransferTokens | External ! |  | NO! |
|  | swapExactTokensForETHSupportingFeeOnTransferTokens | External ! |  | NO! |
|  |  |
| **STE** | Implementation | Context, IERC20, Ownable |  |
|  | <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! |
|  | isExcludedFromReward | Public ! | | NO! |
|  | totalReflectionDistributed | Public ! | | NO! |
|  | deliver | Public ! |  | NO! |
|  | reflectionFromToken | Public ! | | NO! |
|  | tokenFromReflection | Public ! | | NO! |
|  | excludeFromReward | Public ! |  | onlyOwner |
|  | includeInReward | External ! |  | onlyOwner |
|  | <Receive Ether> | External ! |  | NO! |
|  | claimStuckTokens | External ! |  | onlyOwner |
|  | _reflectFee | Private  |  |  |
|  | _getValues | Private  |  |  |
|  | _getTValues | Private  |  |  |
|  | _getRValues | Private  |  |  |
|  | _getRate | Private  |  |  |


```

CONTRACT ASSESMENT

| ^ | _getCurrentSupply | Private  | | |
 | ^ | _takeLiquidity | Private   | | |
 | ^ | _takeBNB | Private   | | |
 | ^ | calculateTaxFee | Private  | | |
 | ^ | calculateLiquidityFee | Private  | | |
 | ^ | calculateBNBFee | Private  | | |
 | ^ | removeAllFee | Private   | | |
 | ^ | setBuyFee | Private   | | |
 | ^ | setSellFee | Private   | | |
 | ^ | isExcludedFromFee | Public  | | NO  |
 | ^ | _approve | Private   | | |
 | ^ | tradeEnable | External   | onlyOwner |
 | ^ | _transfer | Private   | | |
 | ^ | swapAndLiquify | Private   | | |
 | ^ | swapAndSendBNB | Private   | | |
 | ^ | setSwapTokensAtAmount | External   | onlyOwner |
 | ^ | setSwapEnabled | External   | onlyOwner |
 | ^ | _tokenTransfer | Private   | | |
 | ^ | _transferStandard | Private   | | |
 | ^ | _transferToExcluded | Private   | | |
 | ^ | _transferFromExcluded | Private   | | |
 | ^ | _transferBothExcluded | Private   | | |
 | ^ | excludeFromFees | External   | onlyOwner |
 | ^ | changeDevWallet | External   | onlyOwner |
 | ^ | changeCharityWallet | External   | onlyOwner |
 | ^ | setBuyFeePercentages | External   | onlyOwner |
 | ^ | setSellFeePercentages | External   | onlyOwner |
 | ^ | enableWalletToWalletTransferWithoutFee | External   | onlyOwner |

| Symbol | Meaning |

| :-----: | ----- |

|  | Function can modify state |

|  | Function is payable |



STATIC ANALYSIS

```
Variable STE. getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#612) is too similar to STE._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#847)
Variable STE. getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#612) is too similar to STE._getTValues(uint256).tTransferAmount (contracts/Token.sol#603)
Variable STE. transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#879) is too similar to STE._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#857)
Variable STE._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#847) is too similar to STE._getValues(uint256).tTransferAmount (contracts/Token.sol#594)
Variable STE._transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#879) is too similar to STE._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#879)
Variable STE.reflectionFromToken(uint256,bool).rTransferAmount (contracts/Token.sol#541) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._transferToExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#857)
Variable STE._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#847) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE._getValues(uint256).rTransferAmount (contracts/Token.sol#595) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE._transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#879)
Variable STE. getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#612) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE. transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#857) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE._transferStandard(address,address,uint256).rTransferAmount (contracts/Token.sol#847) is too similar to STE._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#879)
Variable STE. transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#857) is too similar to STE._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#847)
Variable STE. transferBothExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#879) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE. getRValues(uint256,uint256,uint256,uint256,uint256).rTransferAmount (contracts/Token.sol#612) is too similar to STE._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#879)
Variable STE. transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._getTValues(uint256).tTransferAmount (contracts/Token.sol#603)
Variable STE. transferToExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#857) is too similar to STE._transferBothExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#879)
Variable STE. transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._transferFromExcluded(address,address,uint256).tTransferAmount (contracts/Token.sol#868)
Variable STE. transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._transferStandard(address,address,uint256).tTransferAmount (contracts/Token.sol#847)
Variable STE. transferFromExcluded(address,address,uint256).rTransferAmount (contracts/Token.sol#868) is too similar to STE._getValues(uint256).tTransferAmount (contracts/Token.sol#594)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-too-similar

STE._decimals (contracts/Token.sol#351) should be constant
STE._name (contracts/Token.sol#349) should be constant
STE._symbol (contracts/Token.sol#350) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant

STE._total (contracts/Token.sol#354) should be immutable
STE.charityFeeOnBuy (contracts/Token.sol#367) should be immutable
STE.charityFeeOnSell (contracts/Token.sol#368) should be immutable
STE.devFeeOnBuy (contracts/Token.sol#370) should be immutable
STE.devFeeOnSell (contracts/Token.sol#371) should be immutable
STE.uniswapV2Pair (contracts/Token.sol#388) should be immutable
STE.uniswapV2Router (contracts/Token.sol#387) 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

Router (PCS V2):

0xD99D1c33F9fC3444f8101754aBC46c52416550D1

1- Adding Liquidity (**Passed**):

liquidity added on Pancakeswap V2:

<https://testnet.bscscan.com/tx/0x94364a6448e6c4829528d3743ad9d4daf049cd726d0bd25162c551abba626c96>

no issue were found on adding liquidity.

2- Buying (liquidity + charity + dev fees = 10%) (**Passed**):

<https://testnet.bscscan.com/tx/0x549c5476ae0a581a5c97c290f8049d6cc9773cf315396f55ae05b32bc839409c>

3- Selling (liquidity + charity + dev fees = 10%) (**Passed**):

<https://testnet.bscscan.com/tx/0xf1f13254991730bbf757635aa78b6d49aac5e13117573b2f6b3d3820bd28747e>

4-Transferring (0% tax while wallet to wallet transfer without fee is enabled)(**Passed**):

<https://testnet.bscscan.com/tx/0xefe4b54c743f80ec52331a8c800e695dae1e038dd513d1a615d15a3792f005b8>



FUNCTIONAL TESTING

5-Auto Liquidity(Passed):
dead wallet received LP share tokens

[https://testnet.bscscan.com/token/0x806a1d2a3f3295d4228cb664ed4711bbbf6c2bf?
a=0x00dead](https://testnet.bscscan.com/token/0x806a1d2a3f3295d4228cb664ed4711bbbf6c2bf?a=0x00dead)

6-Internal Swap(Passed):
this wallet received BNB from contract (internal swap)

charity wallet:
<https://testnet.bscscan.com/address/0xe79af6e63df99afdd8855390fb176cb90e325c4b#internaltx>

dev wallet:
<https://testnet.bscscan.com/address/0x5ee1ab42c7ef664f438fe99da724af81f7356012#internaltx>

MANUAL TESTING

Suggestions and Optimizations

Suggestions

- use indexed keyword to declare events

Optimizations

- Declare this variables as constant: `_nymbol` - `_symbol` - `_decimals` - `_tTotal`



Social Media Overview

**Here are the Social Media Accounts of
Save The Earth**



<https://t.me/Savetheearth>



https://twitter.com/savetheearth1_?t



<https://www.savetheearthtoken.finance>



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://twitter.com/auditace_



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