



Cyberscope

# Audit Report

## **StepShiba**

May 2022

Type           BEP20

Network       BSC

Address       0x56e28e7f6a9981383cd991a6889d1f89ddb49be3

Audited by   © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Source Files</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>Contract Diagnostics</b>	<b>5</b>
<b>L01 - Public Function could be Declared External</b>	<b>6</b>
Description	6
Recommendation	6
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>7</b>
Description	7
Recommendation	7
<b>L05 - Unused State Variable</b>	<b>8</b>
Description	8
Recommendation	8
<b>L07 - Missing Events Arithmetic</b>	<b>9</b>
Description	9
Recommendation	9
<b>L09 - Dead Code Elimination</b>	<b>10</b>
Description	10
Recommendation	10
<b>L12 - Using Variables before Declaration</b>	<b>11</b>
Description	11
Recommendation	11
<b>L14 - Uninitialized Variables in Local Scope</b>	<b>12</b>
Description	12

<b>Recommendation</b>	<b>12</b>
<b>L15 - Local Scope Variable Shadowing</b>	<b>13</b>
<b>Description</b>	<b>13</b>
<b>Recommendation</b>	<b>13</b>
<b>Contract Functions</b>	<b>14</b>
<b>Contract Flow</b>	<b>24</b>
<b>Domain Info</b>	<b>25</b>
<b>Summary</b>	<b>26</b>
<b>Disclaimer</b>	<b>27</b>
<b>About Cyberscope</b>	<b>28</b>

## Contract Review

<b>Contract Name</b>	AntiBotBABYTOKEN
<b>Compiler Version</b>	v0.8.4+commit.c7e474f2
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0x56e28e7f6a9981383cd991a6889d1f89ddb49be3">https://bscscan.com/token/0x56e28e7f6a9981383cd991a6889d1f89ddb49be3</a>
<b>Symbol</b>	STEPS
<b>Decimals</b>	18
<b>Total Supply</b>	100,000,000
<b>Domain</b>	stepshiba.io

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	e6bae5fb5e6f079b0c37bcb775b4495de429e2cd3499a9d9b3c07a192ea01713

## Audit Updates

<b>Initial Audit</b>	22nd May 2022
<b>Corrected</b>	

# Contract Analysis

● Critical   ● Medium   ● Minor   ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

# Contract Diagnostics

● Critical    ● Medium    ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L05	Unused State Variable
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination
●	L12	Using Variables before Declaration
●	L14	Uninitialized Variables in Local Scope
●	L15	Local Scope Variable Shadowing

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L203,211,228,235,254,262,273,291,319,338,553,561,1414,1422,1439,1465,1473,1484,1502,1530,1549,1771,1779,1946,1950,1961,1969,2131,2334,2183,2202,2351,2436,2484,2756,2781,2803,2836,2862,2902,2906,2914,2926

### Description

Public functions that are never called by the contract should be declared external to save gas.

```
isExcludedFromDividends  
dividendTokenBalanceOf  
withdrawableDividendOf  
isExcludedFromFees  
updateGasForProcessing  
setAutomatedMarketMakerPair  
excludeMultipleAccountsFromFees  
updateUniswapV2Router  
updateDividendTracker  
...
```

### Recommendation

Use the external attribute for functions never called from the contract.

## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L931,1330,1334,1343,1401,1406,1708,1740,1745,1789,1812,1813,1830,2121,2122,2123,2124,2183,2190,2202,2216,2101,2387,2746,2617

### Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow \_ at the beginning of the mixed\_case match for private variables and unused parameters.

```
_marketingWalletAddress
_enable
_account
magnitude
_owner
_symbol
_name
_rewardToken
__DividendPayingToken_init
...
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>



## L05 - Unused State Variable

**Criticality**

minor

**Location**

contract.sol#L1858,1789

### Description

There are segments that contain unused state variables.

```
__gap  
MAX_INT256
```

### Recommendation

Remove unused state variables.

## L07 - Missing Events Arithmetic

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L2752,2818,2824,2830

### Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
marketingFee = value
liquidityFee = value
totalFees = tokenRewardsFee.add(liquidityFee).add(marketingFee)
swapTokensAtAmount = amount
```

### Recommendation

Emit an event for critical parameter changes.

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L845,879,859,1330,2235,416,1573,1904

### Description

Functions that are not used in the contract, and make the code's size bigger.

```
abs
_transfer
_burn
__Context_init
predictDeterministicAddress
cloneDeterministic
```

### Recommendation

Remove unused functions.

## L12 - Using Variables before Declaration

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L3071,3070,3072

### Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
lastProcessedIndex  
iterations  
claims
```

### Recommendation

The variables should be declared before any usage of them.

## L14 - Uninitialized Variables in Local Scope

**Criticality**

minor

**Location**

contract.sol#L3070,3071,3072

### Description

These are variables that are defined in the local scope and are not initialized.

`lastProcessedIndex``claims``iterations`

### Recommendation

All the local scoped variables should be initialized.

## L15 - Local Scope Variable Shadowing

**Criticality**

minor

**Location**

contract.sol#L2123,2124,2183,2190,2202,2216

### Description

There are variables that are defined in the local scope containing the same name from an upper scope.

```
_owner  
_symbol  
_name
```

### Recommendation

The local variables should have different names from the upper scoped variables.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-

	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
<b>SafeMath</b>	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		
<b>Clones</b>	Library			
	clone	Internal	✓	



	cloneDeterministic	Internal	✓	
	predictDeterministicAddress	Internal		
	predictDeterministicAddress	Internal		
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Router01</b>	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-

<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>IPinkAntiBot</b>	Interface			
	setTokenOwner	External	✓	-
	onPreTransferCheck	External	✓	-
<b>IERC20Upgradeable</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>IERC20MetadataUpgradeable</b>	Interface	IERC20Upgradeable		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>Initializable</b>	Implementation			
<b>ContextUpgradeable</b>	Implementation	Initializable		
	__Context_init	Internal	✓	initializer

	__Context_init_unchained	Internal	✓	initializer
	_msgSender	Internal		
	_msgData	Internal		
<b>ERC20Upgradable</b>	Implementation	Initializable, ContextUpgradable, IERC20Upgradable, IERC20MetadataUpgradable		
	__ERC20_init	Internal	✓	initializer
	__ERC20_init_unchained	Internal	✓	initializer
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
<b>OwnableUpgradable</b>	Implementation	Initializable, ContextUpgradable		
	__Ownable_init	Internal	✓	initializer
	__Ownable_init_unchained	Internal	✓	initializer
	owner	Public		-

	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
<b>IUniswapV2Pair</b>	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>SafeMathInt</b>	Library			
	mul	Internal		

	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
	toUint256Safe	Internal		
<b>SafeMathUint</b>	Library			
	toInt256Safe	Internal		
<b>IterableMapping</b>	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
<b>DividendPayingTokenInterface</b>	Interface			
	dividendOf	External		-
	withdrawDividend	External	✓	-
<b>DividendPayingTokenOptionalInterface</b>	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-
<b>DividendPayingToken</b>	Implementation	ERC20Upgradable, OwnableUpgradable, DividendPayingTokenInterface, DividendPayingTokenOp		

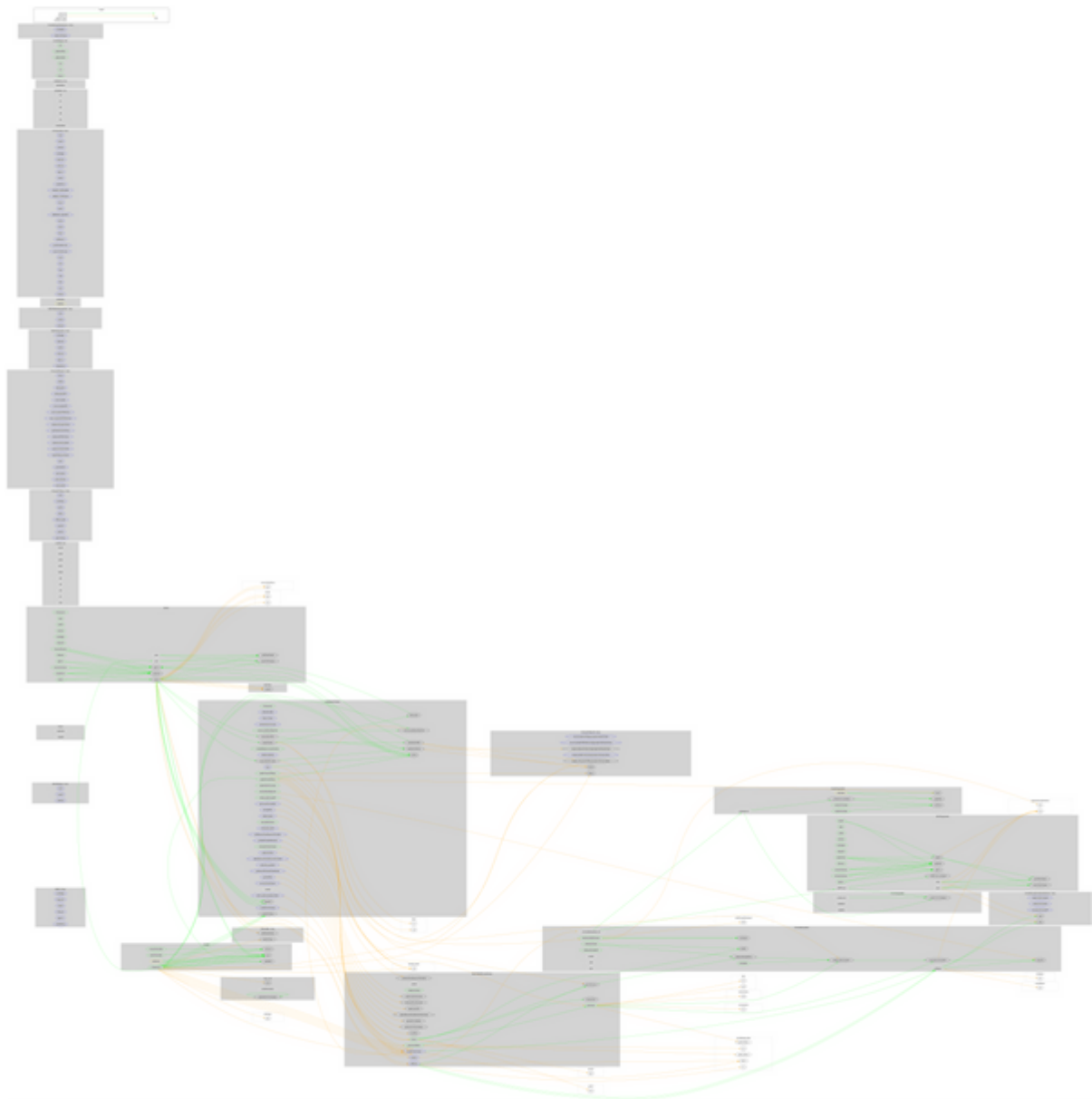
		tionallInterfa ce		
	__DividendPayingToken_init	Internal	✓	initializer
	distributeCAKEDividends	Public	✓	onlyOwner
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	
<b>BABYTOKEND dividendTracker</b>	Implementation	OwnableUp gradeable, DividendPay ingToken		
	initialize	External	✓	initializer
	_transfer	Internal		
	withdrawDividend	Public		-
	excludeFromDividends	External	✓	onlyOwner
	isExcludedFromDividends	Public		-
	updateClaimWait	External	✓	onlyOwner
	updateMinimumTokenBalanceForDivi dends	External	✓	onlyOwner
	getLastProcessedIndex	External		-
	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	External	✓	onlyOwner
	process	Public	✓	-
	processAccount	Public	✓	onlyOwner
<b>BaseToken</b>	Implementation			

<b>AntiBotBABYTOKEN</b>	Implementation	ERC20, Ownable, BaseToken		
	<Constructor>	Public	Payable	ERC20
	setEnabledAntiBot	External	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	setSwapTokensAtAmount	External	✓	onlyOwner
	updateDividendTracker	Public	✓	onlyOwner
	updateUniswapV2Router	Public	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	setMarketingWallet	External	✓	onlyOwner
	setTokenRewardsFee	External	✓	onlyOwner
	setLiquiditFee	External	✓	onlyOwner
	setMarketingFee	External	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	updateGasForProcessing	Public	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getClaimWait	External		-
	updateMinimumTokenBalanceForDividends	External	✓	onlyOwner
	getMinimumTokenBalanceForDividends	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	excludeFromDividends	External	✓	onlyOwner
	isExcludedFromDividends	Public		-
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-

	_transfer	Internal	✓	
	swapAndSendToFee	Private	✓	
	swapAndLiquify	Private	✓	
	swapTokensForEth	Private	✓	
	swapTokensForCake	Private	✓	
	addLiquidity	Private	✓	
	swapAndSendDividends	Private	✓	



# Contract Flow



## Domain Info

<b>Domain Name</b>	stepshiba.io
<b>Registry Domain ID</b>	6ba92cc6aa6c43e88ec455f0f3e38c4b-DONUTS
<b>Creation Date</b>	2022-05-18T09:52:20Z
<b>Updated Date</b>	2022-05-18T09:54:55Z
<b>Registry Expiry Date</b>	2023-05-18T09:52:20Z
<b>Registrar WHOIS Server</b>	whois.godaddy.com/
<b>Registrar URL</b>	<a href="http://www.godaddy.com/domains/search.aspx?ci=8990">http://www.godaddy.com/domains/search.aspx?ci=8990</a>
<b>Registrar</b>	GoDaddy.com, LLC
<b>Registrar IANA ID</b>	146

The domain has been created 4 days before the creation of the audit. It will expire in 12 months.

There is no public billing information, the creator is protected by the privacy settings.

## Summary

StepShiba Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. There is also a limit of max 25% fees.

# 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.

Cyberscope 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 Cyberscope 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 Cyberscope 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 Cyberscope team disclaims any liability for the resulting losses.

## About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provide all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>