Audit Report

HotCams

February 2022

Type	BEP20
Network	BSC
Address	0x6D1B3fdf5096465fb8B81A9B6e734a9641b50c24
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	ReflectionToken
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	MIT
Explorer	https://bscscan.com/token/0x6D1B3fdf5096465fb8B81A9B6e734a9641b50c24
Symbol	HC
Decimals	18
Total Supply	1,000,000,000
Source	contract.sol
Domain	hotcamstoken.com

Audit Updates

Initial Audit	1st February 2022
Corrected	

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

ST - Stop Transactions

Criticality	minor
Location	contract.sol#L741

Description

The contract owner has the authority to significantly reduce the sale amount for all users excluding the owner. The owner may take advantage of it by setting the `_sellMaxTxAmount` to `0.001%` of the total supply.

```
function setMaxTxPercents(uint256 buyPercent, uint256 buyDivisor, uint256
sellPercent, uint256 sellDivisor) public onlyOwner() {
    _buyMaxTxAmount = (_tTotal * buyPercent) / buyDivisor;
    buyMaxTxAmountUI = (startingSupply * buyPercent) / buyDivisor;
    _sellMaxTxAmount = (_tTotal * sellPercent) / sellDivisor;
    sellMaxTxAmountUI = (startingSupply * sellPercent) / sellDivisor;
    require(_sellMaxTxAmount >= (_tTotal / 10000) && _buyMaxTxAmount >= (_tTotal
/ 10000), "Max Transaction amts must be above 0.01% of total supply.");
}
```

Recommendation

The contract could embody a check for not allowing setting the _maxTxAmount less than a more reasonable amount like `0.01%` of the total supply. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L759

Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `setBlacklistEnabled` function.

```
if (isSniperOrBlacklisted(from) || isSniperOrBlacklisted(to)) {
    revert("Sniper rejected.");
}
```

Recommendation

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L05	Unused State Variable
	L04	Conformance to Solidity Naming Conventions
	L09	Dead Code Elimination
	L11	Unnecessary Boolean equality
	L07	Missing Events Arithmetic

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L723,L706,L698 and 6 more

Description

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

```
enableTrading
setMaxWalletSize
setMaxTxPercents
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L371,L372,L377 and 8 more

Description

Constant state variables should be declared constant to save gas.

```
sellMaxTxPercent
sellMaxTxDivisor
maxWalletPercent
...
```

Recommendation

Add the constant attribute to state variables that never change.

L05 - Unused State Variable

Criticality	minor
Location	contract.sol#L380,L374,L369 and 1 more

Description

There are segments that contains unused state variable.

```
_previousMaxWalletSize
_sellPreviousMaxTxAmount
_buyPreviousBuyMaxTxAmount
...
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L395,L361,L360 and 28 more

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.

```
_hasLiqBeenAdded
ZERO
DEAD
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L539,L5,L9

Description

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

```
_approve
_msgSender
_msgData
```

Recommendation

Remove unused functions.

L11 - Unnecessary Boolean equality

Criticality	minor
Location	contract.sol#L686,L584

Description

The comparison to boolean constants is redundant. Boolean constants can be used directly and do not need to be compared to true or false.

```
enabled == false
require(bool)(init == false)
```

Recommendation

Remove the equality to the boolean constant.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L706,L698,L645 and 4 more

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.

```
_maxWalletSize = check
_buyMaxTxAmount = (_tTotal * buyPercent) / buyDivisor
reflectorGas = gas
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	Interface			

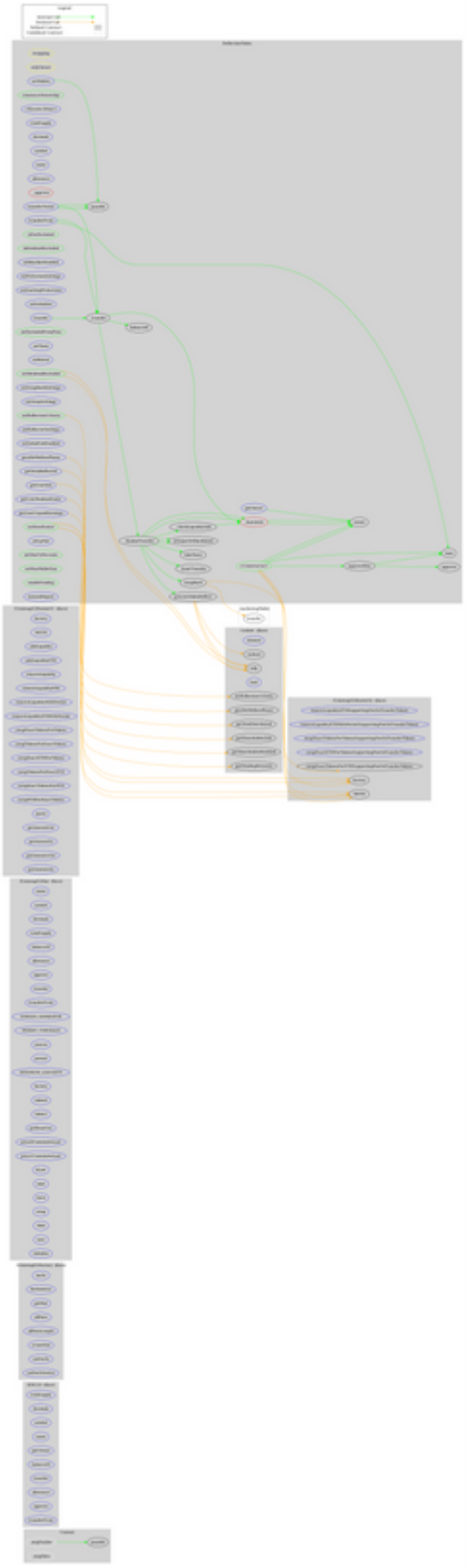
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	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	✓	-
IUniswapV2Router01	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		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
Cashier	Interface			
	whomst	External		-
	setReflectionCriteria	External	✓	-
	tally	External	✓	-
	load	External	Payable	-
	cashout	External	✓	-
	giveMeWelfarePlease	External	✓	-
	getTotalDistributed	External		-
	getShareholderInfo	External		-
	getShareholderRealized	External		-

	getPendingRewards	External		-
ReflectionToken	Implementation	IERC20		
	<Constructor>	Public	Payable	-
	owner	Public		-
	transferOwner	External	✓	onlyOwner
	renounceOwnership	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	totalSupply	External		-
	decimals	External		-
	symbol	External		-
	name	External		-
	getOwner	External		-
	balanceOf	Public		-
	allowance	External		-
	approve	Public	✓	-
	approveMax	Public	✓	-
	_approve	Private	✓	
	transfer	External	✓	-
	transferFrom	External	✓	-
	isSniperOrBlacklisted	Public		-
	isFeeExcluded	Public		-
	isDividendExcluded	Public		-
	setBlacklistEnabled	External	✓	onlyOwner
	setProtectionSettings	External	✓	onlyOwner
	setStartingProtections	External	✓	onlyOwner
	setInitializer	External	✓	onlyOwner
	setDividendExcluded	Public	✓	onlyOwner
	setExcludedFromFees	Public	✓	onlyOwner
	setTaxes	External	✓	onlyOwner
	setRatios	External	✓	onlyOwner
	setWallets	External	✓	onlyOwner
	setSwapBackSettings	External	✓	onlyOwner
	setSwapSettings	External	✓	onlyOwner
	setReflectionCriteria	Public	✓	onlyOwner

	setReflectorSettings	External	✓	onlyOwner
	setInitialSubEnabled	External	✓	onlyOwner
	giveMeWelfarePlease	External	✓	-
	getTotalReflected	External		-
	getUserInfo	External		-
	getUserRealizedGains	External		-
	getUserUnpaidEarnings	External		-
	setNewRouter	Public	✓	onlyOwner
	setLpPair	External	✓	onlyOwner
	setMaxTxPercents	Public	✓	onlyOwner
	setMaxWalletSize	Public	✓	onlyOwner
	_hasLimits	Private		
	enableTrading	Public	✓	onlyOwner
	_transfer	Internal	✓	
	_finalizeTransfer	Internal	✓	
	processTokenReflect	Internal	✓	
	_basicTransfer	Internal	✓	
	takeTaxes	Internal	✓	
	swapBack	Internal	✓	swapping
	manualDepost	External	✓	onlyOwner
	_checkLiquidityAdd	Private	✓	

Contract Flow



Domain Info

Domain Name	
Registry Domain ID	2641221339_DOMAIN_COM-VRSN
Creation Date	2021-09-15T14:29:30Z
Updated Date	2021-09-15T14:29:32Z
Registry Expiry Date	
Registrar WHOIS Server	whois.reg.com
Registrar URL	https://www.reg.com
Registrar	Registrar of domain names REG.RU LLC
Registrar IANA ID	1606

The domain has been created 5 months before the creation of the audit.

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

Summary

HotCams is aiming to build online services and products for adults. There are some functions that can be abused by the owner, like significantly decreasing the transfer amount and blacklisting contracts. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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.

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

About Coinscope

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.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co