



# Audit Report

## Baby Manchester City Fan Token

July 2022

Type           BEP20

Network       BSC

Address       0x9F31b91a1d9bD0664Dd94c9B360cceC52B07a9D5

Audited by   © SecureZilla



## Contents

<b>Contract Review .....</b>	<b>3</b>
<b>Source Files .....</b>	<b>3</b>
<b>Audit Updates .....</b>	<b>3</b>
<b>Vulnerability &amp; Risk Level .....</b>	<b>4</b>
<b>Contract Analysis.....</b>	<b>5</b>
<b>Contract Diagnostics .....</b>	<b>6</b>
<b>S01 - Public Function could be Declared External .....</b>	<b>7</b>
Description .....	7
Recommendation .....	7
<b>S04 - State Variables could be Declared Constant .....</b>	<b>8</b>
Description .....	8
Recommendation .....	8
<b>S05 - Conformance to Solidity Naming Conventions .....</b>	<b>9</b>
Description .....	9
Recommendation .....	9
<b>S07 - Missing Events Arithmetic.....</b>	<b>10</b>
Description .....	10
Recommendation .....	10
<b>S09 - Dead Code Elimination.....</b>	<b>11</b>
Description .....	11
Recommendation .....	11
<b>S13 - Divide before Multiply Operation.....</b>	<b>12</b>
Description .....	12
Recommendation .....	12
<b>S15 – Local Scope Variable Shadowing .....</b>	<b>13</b>
Description .....	13



<b>Recommendation .....</b>	<b>13</b>
<b>Contract Functions.....</b>	<b>14</b>
<b>Contract Flow.....</b>	<b>20</b>
<b>Domain Info.....</b>	<b>21</b>
<b>Summary .....</b>	<b>22</b>
<b>Disclaimer .....</b>	<b>23</b>
<b>About SecureZilla.....</b>	<b>24</b>



## Contract Review

<b>Contract Name</b>	Baby Manchester City Fan Token
<b>Compiler Version</b>	v0.8.9commit.e5eed63a
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0x9F31b91a1d9bD0664Dd94c9B360cceC52B07a9D5">https://bscscan.com/token/0x9F31b91a1d9bD0664Dd94c9B360cceC52B07a9D5</a>
<b>Symbol</b>	BCITY
<b>Decimals</b>	8
<b>Total Supply</b>	1,000,000,000
<b>Domain</b>	bmcity.club

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	67d5b7803f50c7a07cc6770468bb46735e03dba95df7c7c517552dd39fe9b8ab

## Audit Updates

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



## Vulnerability & Risk Level









Risk represents the probability that a certain source-threat will exploit vulnerability, and the impact of that event on the organization or system. Risk Level is computed based on CVSS version 3.0.

Level	Value	Vulnerability	Risk (Required Action)
 <b>Critical</b>	9 +	A vulnerability that creates a risk that the contract may be damaged.	Instant action to lessen risk level.
 <b>High</b>	7 +	A vulnerability that disturbs the anticipated outcome when using contract.	Application of counteractive actions asap.
 <b>Medium</b>	4 +	A vulnerability that could affect the contract in a specific scenario.	Execution of educative actions in a certain period.
 <b>Low</b>	2 +	A vulnerability that does not have a major effect.	Operation of certain helpful actions or accepting the risk.
 <b>Informational</b>	0 – 1.9	A vulnerability that have informational appeal but is not effecting any of the code.	a comment that does not control a level of risk.



## Contract Analysis

 **Critical**  **High**  **Medium**  **Low**

Severity	Code	Description
	ST	Contract Owner is not able to stop or pause transactions
	OCTT	Contract Owner is not able to transfer tokens from specific address
	OTUT	Owner Transfer User's Tokens
	IFRL	Contract Owner is not able to increase fees more than a reasonable percent (25%)
	ULTO	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
	MNT	Contract Owner is not able to mint new tokens
	BTSW	Contract Owner is not able to burn tokens from specific wallet
	BWS	Contract Owner is not able to blacklist wallets from selling



## Contract Diagnostics



Critical



Medium



Low

Severity	Code	Description
●	S01	Public Function could be Declared External
●	S04	Conformance to Solidity Naming Conventions
●	S05	Unused State Variable
●	S07	Missing Events Arithmetic
●	S09	Dead Code Elimination
●	S13	Divide before Multiply Operation
●	S15	Local Scope Variable Shadowing



## S01 - Public Function could be Declared External

**Criticality**

low

**Location**

contract.sol#L293,633,230,334,213,256,315,642,205,275,264

### Description

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

```
allowance
approve
name
transferOwnership
increaseAllowance
transfer
symbol
decreaseAllowance
decimals
...
```

### Recommendation

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





## S04 - Conformance to Solidity Naming Conventions

**Criticality**

low

**Location**

contract.sol#L855,1000,32,903,49,907,31,991,860,905,722

### 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.

```
_devFee  
_buyBackFee  
WETH  
devWalletUpdated  
_marketingFee  
_liquidityFee  
deadAddress  
DOMAIN_SEPARATOR  
buyBackWalletUpdated  
...
```

### Recommendation

Follow the Solidity naming convention.

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



## S05 - Unused State Variable

**Criticality**

low

**Location**

contract.sol#L653

### Description

There are segments that contain unused state variables.

```
MAX_INT256
```

### Recommendation

Remove unused state variables.



## S07 - Missing Events Arithmetic

**Criticality**

low

**Location**

contract.sol#L1000,991,980

### 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.

```
swapTokensAtAmount = newAmount  
buyMarketingFee = _marketingFee  
sellMarketingFee = _marketingFee
```

### Recommendation

Emit an event for critical parameter changes.



## S09 - Dead Code Elimination

**Criticality**

low

**Location**

contract.sol#L699,712,398,705

### Description

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

```
toUint256Safe  
_burn  
toInt256Safe  
abs
```

### Recommendation

Remove unused functions.



## S13 - Divide before Multiply Operation

**Criticality**

low

**Location**

contract.sol#L1046

### Description

Performing divisions before multiplications may cause lose of prediction.

```
fees = amount.mul(buyTotalFees).div(100)
tokensForLiquidity += fees * sellLiquidityFee / sellTotalFees
tokensForMarketing += fees * sellMarketingFee / sellTotalFees
tokensForDev += fees * sellDevFee / sellTotalFees
tokensForBuyBack += fees * sellBuyBackFee / sellTotalFees
```

### Recommendation

The multiplications should be prior to the divisions.



## S15 - Local Scope Variable Shadowing

**Criticality**

low

**Location**

contract.sol#L925

### Description

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

```
totalSupply
```

### Recommendation

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



## Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
<b>Address</b>	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	



	_functionCallWithValue	Private	✓	
<b>Owable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	getUnlockTime	Public		-
	getTime	Public		-
	lock	Public	✓	onlyOwner
	unlock	Public	✓	-
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<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		-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	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>Antcoin</b>	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	minimumTokensBeforeSwapAmount	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner



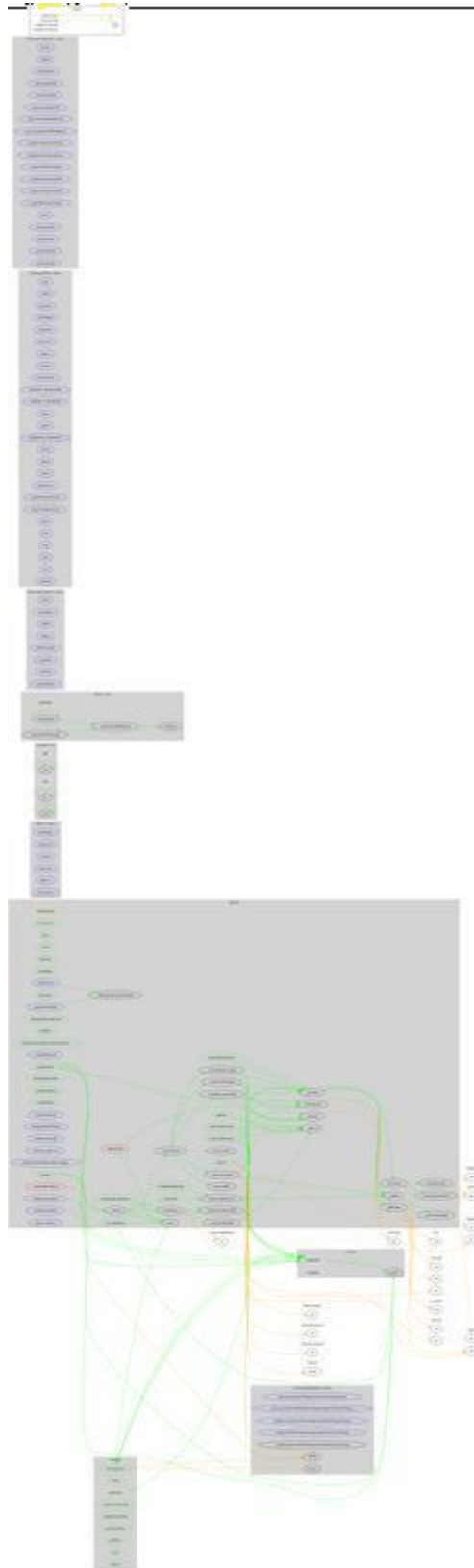
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokens	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	swapETHForTokens	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
	_transferBothExcluded	Private	✓	
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setMarketingDivisor	External	✓	onlyOwner
	setNumTokensSellToAddToLiquidity	External	✓	onlyOwner
	setMarketingAddress	External	✓	onlyOwner
	setliquidityAddress	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	prepareForPreSale	External	✓	onlyOwner
	afterPreSale	External	✓	onlyOwner



	transferToAddressETH	Public	✓	-
	recoverBalance	Public	✓	onlyOwner
	doManualSwapTokens	Public	✓	-
	<Receive Ether>	External	Payable	-



# Contract Flow





## Domain Info

<b>Domain Name</b>	bmcity.club
<b>Registry Domain ID</b>	494DOCA2C-APP
<b>Creation Date</b>	2022-07-17T20:09:16Z
<b>Updated Date</b>	2022-07-20T20:09:16Z
<b>Registry Expiry Date</b>	2023-06-17T20:09:16Z
<b>Registrar WHOIS Server</b>	whois.nic.google
<b>Registrar URL</b>	None
<b>Registrar</b>	Namecheap, LLC
<b>Registrar IANA ID</b>	1479

The domain has been created in 12 months before the creation of the audit.

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



## Summary

Baby Manchester City Fan 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 cannot be used in a malicious way to disturb the users' transactions. There is also a limit of max 10% 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.

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





## About SecureZilla

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



The SecureZilla team

<https://www.SecureZilla.io>