Cyberscope

Audit Report

Witch Baby Doge

May 2022

Type	BEP20
Network	BSC
Address	0xC24e233DD1D08aEBebA6a2729Dc0A44C2C7C1b33
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	WitchBabyDoge
Compiler Version	v0.8.6+commit.11564f7e
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0xC24e233DD1D08aEBebA6a2729Dc0A44C2C7C1b33
Symbol	WBDOGE
Decimals	9
Total Supply	1,000,000,000,000
Domain	wbdoge.co

Source Files

Filename	**SHA256**
contract.sol	3034ff104cc78f9313b7214d1c3dc4bbd083edf07d610fa90aa003e8d9814012

Audit Updates

Initial Audit	4th May 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

ELFM - Exceed Limit Fees Manipulation

Criticality	medium
Location	contract.sol#L391

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setFee` function with a high percentage value.

```
    function setFee(uint256 RedistributionFeeOnBuy, uint256
RedistributionFeeOnSell, uint256 TaxFeeOnBuy, uint256 TaxFeeOnSell) public
onlyDev {
        require(RedistributionFeeOnBuy < 15, "Redistribution cannot be more
than 15");
        require(RedistributionFeeOnSell < 15, "Redistribution cannot be more
than 15");
        require(TaxFeeOnBuy < 15, "Tax cannot be more than 15");
        require(TaxFeeOnSell < 15, "Tax cannot be more than 15");
        _RedistributionFeeOnBuy = RedistributionFeeOnBuy;
        _RedistributionFeeOnSell = RedistributionFeeOnSell;
        _TaxFeeOnBuy = TaxFeeOnBuy;
        _TaxFeeOnSell = TaxFeeOnSell;
    }
```

Recommendation

The contract could embody a check for not allowing the total fees on buy and on sell to be more than 25%.

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.

ULTW - Unlimited Liquidity to Team Wallet

Criticality	minor
Location	contract.sol#L379, 385

Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the manualswap and manualsend functions.

```
    function manualswap() external {
        require(_msgSender() == _BuybackAddress || _msgSender() ==
_MarketingAddress || _msgSender() == owner());
        uint256 contractBalance = balanceOf(address(this));
        swapTokensForEth(contractBalance);
    }
```

```
    function manualsend() external {
        require(_msgSender() == _BuybackAddress || _msgSender() ==
_MarketingAddress || _msgSender() == owner());
        uint256 contractETHBalance = address(this).balance;
        sendETHToFee(contractETHBalance);
    }
```

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
	FSA	Fixed Swap Address
	L01	Public Function could be Declared External
	L02	State Variables could be Declared Constant
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L170

Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
IUniswapV2Router02 _uniswapV2Router =
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
        uniswapV2Router = _uniswapV2Router;
        uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())
            .createPair(address(this), _uniswapV2Router.WETH());
```

Recommendation

It could be better to allow the swap address mutation in case of future swap updates.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L114,120,188,192,196,200,208,213,217,222,304,310,317,391,402,406

Description

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

```
excludeMultipleAccountsFromFees
toggleSwap
setFee
setNewMarketingAddress
setNewDevAddress
rescueForeignTokens
transferFrom
approve
allowance
...
```

Recommendation

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

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L97

Description

Constant state variables should be declared constant to save gas.

```
_previousOwner
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L38,303,309,304,391,402,136,140,141,143,144,146,147,149,150,151,153,154

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.

```
_MarketingAddress
_BuybackAddress
_decimals
_symbol
_name
_TaxFee
_RedistributionFee
_TaxFeeOnSell
_RedistributionFeeOnSell
...
```

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#L97,131

Description

There are segments that contain unused state variables.

```
_tOwned
_previousOwner
```

Recommendation

Remove unused state variables.

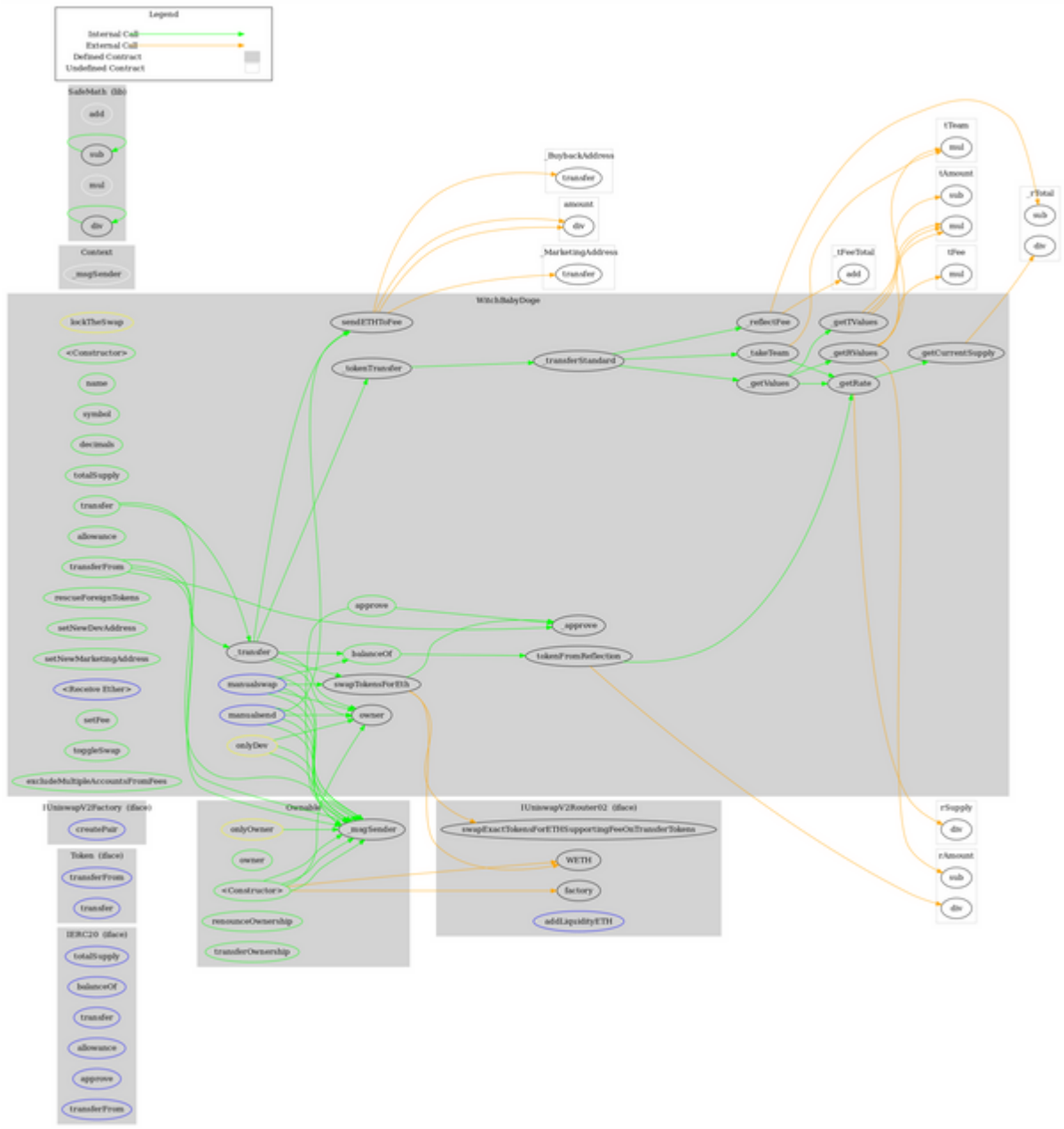
Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
Token	Interface			
	transferFrom	External	✓	-
	transfer	External	✓	-
IUniswapV2Factory	Interface			
	createPair	External	✓	-
IUniswapV2Router02	Interface			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
Context	Implementation			
	_msgSender	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		

	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
WitchBabyDoge	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	tokenFromReflection	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokensForEth	Private	✓	lockTheSwap
	sendETHToFee	Private	✓	
	_tokenTransfer	Private	✓	
	rescueForeignTokens	Public	✓	onlyDev
	setNewDevAddress	Public	✓	onlyDev
	setNewMarketingAddress	Public	✓	onlyDev
	_transferStandard	Private	✓	
	_takeTeam	Private	✓	
	_reflectFee	Private	✓	

	<Receive Ether>	External	Payable	-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	manualswap	External	✓	-
	manualsend	External	✓	-
	setFee	Public	✓	onlyDev
	toggleSwap	Public	✓	onlyDev
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	wbdoge.co
Registry Domain ID	DB86D6FEFBDFE4528B522BB76F751D751-GDREG
Creation Date	2022-04-25T14:19:26Z
Updated Date	2022-04-30T14:19:27Z
Registry Expiry Date	2023-04-25T14:19:26Z
Registrar WHOIS Server	whois.discount-domain.com
Registrar URL	whois.discount-domain.com
Registrar	GMO Internet, Inc. d/b/a Onamae.com
Registrar IANA ID	49

The domain has been created 9 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

There are some functions that can be abused by the owner like manipulating fees and transferring funds to the team’s wallet. The maximum fee percentage that can be set is 28%. 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.

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 provides all the essential tools to assist users draw their own conclusions.

The Cyberscope team

https://www.cyberscope.io