



# **RugFreeCoins Audit**



**Universal World Cup NFTsToken**

**Smart Contract Security Audit**

**August 30, 2022**

# Contents

Audit details	1
Disclaimer	2
Overview	3
Background	4
Target market and the concept	7
Potential to grow with score points	8
Total Points	8
Contract details	9
Contract code function details	10
Contract description table	12
Security issue checking status	18
Owner privileges	19
Audit conclusion	21



# Audit details



## **Audited project**

Universe World Cup NFTs Token



## **Contract Address**

0xffc4c02C6BB187cE473Fb00458EF6CF80503D189



## **Client contact**

Universe World Cup NFTs Team



## **Blockchain**

Binance smart chain



## **Project website**

# Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Rugfreecoins and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Rugfreecoins) owe no duty of care towards you or any other person, nor does Rugfreecoins make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Rugfreecoins hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Rugfreecoins hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Rugfreecoins, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

# Overview

- ✓ No mint function found; the owner cannot mint tokens after initial deploy.
- ✓ The owner can't be able to set a max transaction limit lower than 0.1% of the circulating supply.
- ✓ The owner can't pause trading.
- ✓ The owner can't set fees over 25%.
- ✓ Owner can't blacklist wallets.
- ✓ The owner can't set a max wallet limit lower than 1% of the circulating supply.
- ✓ The owner can't claim the contract's balance of its own token.

# Background

Rugfreecoins was commissioned by the Universe World Cup NFTs Team to perform an audit of the smart contract.

**<https://bscscan.com/token/0xffc4c02c6bb187ce473fb00458ef6cf80503d189>**

The focus of this audit is to verify that the smart contract is secure, resilient, and working according to the specifications.

The information in this report should be used to understand the risk exposure of the smart contract, project feasibility, and long-term sustainability, and as a guide to improving the security posture of the smart contract by remediating the issues that were identified.

# ROADMAP

## **Level 01: Development**

The project began in August, and the community and team have been consistently delivering since then.

## **Level 02: Marketing Campaign**

We've been running marketing campaigns since the KangarooWC community and old team got together to make this project dream a reality, and we won't stop until we've written history.

## **Level 03: Creating awareness**

Twitter Australian football team follow us and more influencers.

## **Level 04 – KANGWC Gram**

We're working on a photo-sharing social platform for crypto and football fans to share game predictions, experiences, and ideas, whether live from the stadium or online. We will also integrate a gamification system, allowing users to earn incentives such as match tickets, flights, and other items.

# Tokenomics

**0% fee when buying & selling**



# Target market and the concept

## Target market

- Anyone who's interested in the Crypto space with long-term investment plans.
- Anyone who's ready to earn a passive income by holding tokens.
- Anyone who's interested in trading tokens.
- Anyone who's ready to staking and receive rewards.
- Anyone who's ready to contribute to the good cause of charity.
- Anyone who's interested in taking part in the future plans of the Universe World Cup NFTs
- Anyone who's interested in making financial transactions with any other party using Universe World Cup NFTs Token as the currency.

# Potential to grow with score points

1.	Project efficiency	8/10
2.	Project uniqueness	7/10
3	Information quality	7/10
4	Service quality	9/10
5	System quality	8/10
6	Impact on the community	7/10
7	Impact on the business	9/10
8	Preparing for the future	8/10
9	Smart contract security	10/10
10	Smart contract functionality assessment	10/10
Total Points		<b>8.3/10</b>

# Contract details

## Token contract details for 30<sup>th</sup> August 2022

Contract name	Universe World Cup NFTs
Contract address	0xffc4c02C6BB187cE473Fb00458EF6CF80503D189
Token supply	1,000,000,000
Token ticker	UWC
Decimals	9
Token holders	3
Transaction count	6
Contract deployer address	0xBe2b979C39813106be1afE77a1120CCdB38400dd
Contract's current owner address	0xBe2b979C39813106be1afE77a1120CCdB38400dd











# Contract code function details

No	Category	Item	Result
1	Coding conventions	BRC20 Token standards	pass
		compile errors	pass
		Compiler version security	pass
		visibility specifiers	pass
		Gas consumption	pass
		SafeMath features	pass
		Fallback usage	pass
		tx.origin usage	pass
		deprecated items	pass
		Redundant code	pass
		Overriding variables	pass
2	Function call audit	Authorization of function call	pass
		Low level function (call/delegate call) security	pass
		Returned value security	pass
		Self-destruct function security	pass
3	Business security	Access control of owners	
		Business logics	pass
		Business implementations	pass
4	Integer overflow/underflow		pass
5	Reentrancy		pass
6	Exceptional reachable state		pass
7	Transaction ordering dependence		pass
8	Block properties dependence		pass
9	Pseudo random number generator (PRNG)		pass
10	DoS (Denial of Service)		pass
11	Token vesting implementation		pass
12	Fake deposit		pass














13	Event security		pass
----	----------------	--	------


















# Contract description table









The below table represents the summary of the contracts and methods in the token contract. We scanned the whole contract and listed down all the Interfaces, functions, and implementations with their visibility and mutability.













Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
UWC	Implementation	IERC20, Ownable		
L		Public !		NO !
L		External !		NO !
L	totalSupply	External !		NO !
L	name	Public !		NO !
L	symbol	Public !		NO !
L	decimals	Public !		NO !
L	balanceOf	Public !		NO !
L	allowance	External !		NO !
L	approve	Public !		NO !
L	_approve	Internal 		
L	approveMax	External !		NO !
L	transfer	External !		NO !
L	transferFrom	External !		NO !
L	_transferFrom	Internal 		





L	getBep20Tokens	External !		onlyOwner
L	clearStuckBalance	External !		onlyOwner
L	enableTrading	Public !		onlyOwner
L	whitelistPreSale	Public !		onlyOwner
L	isMaxTxExcluded	Public !		NO !
L	isMaxWalletExcluded	Public !		NO !
L	setMaxTxAmount	External !		onlyOwner
L	setMaxWalletToken	External !		onlyOwner
<b>Ownable</b>	<b>Implementation</b>	<b>Context</b>		
L		Public !		NO !
L	owner	Public !		NO !
L	_checkOwner	Internal 		
L	renounceOwnership	Public !		onlyOwner
L	transferOwnership	Public !		onlyOwner
L	_transferOwnership	Internal 		
<b>IERC20</b>	<b>Interface</b>			
L	totalSupply	External !		NO !
L	balanceOf	External !		NO !
L	transfer	External !		NO !
L	allowance	External !		NO !

L	approve	External !		NO !
L	transferFrom	External !		NO !
<b>SafeMath</b>	<b>Library</b>			
L	tryAdd	Internal 		
L	trySub	Internal 		
L	tryMul	Internal 		
L	tryDiv	Internal 		
L	tryMod	Internal 		
L	add	Internal 		
L	sub	Internal 		
L	mul	Internal 		
L	div	Internal 		
L	mod	Internal 		
L	sub	Internal 		
L	div	Internal 		
L	mod	Internal 		
<b>IUniswapV2 Router02</b>	<b>Interface</b>	<b>IUniswapV2 Router01</b>		
L	removeLiquidityETHSupportingFeeOnTransferTokens	External !		NO !
L	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External !		NO !

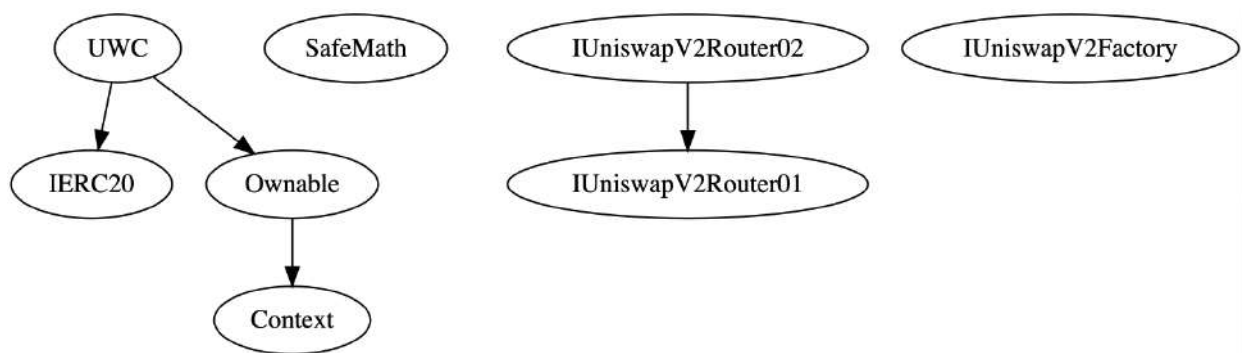
L	swapExactTokensForTokensSupportingFeeOnTransferTokens	External !		NO !
L	swapExactETHForTokensSupportingFeeOnTransferTokens	External !		NO !
L	swapExactTokensForETHSupportingFeeOnTransferTokens	External !		NO !
<b>IUniswapV2 Factory</b>	<b>Interface</b>			
L	feeTo	External !		NO !
L	feeToSetter	External !		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 !
<b>Context</b>	<b>Implementation</b>			
L	_msgSender	Internal 		
L	_msgData	Internal 		
<b>IUniswapV2 Router01</b>	<b>Interface</b>			
L	factory	External !		NO !
L	WETH	External !		NO !

L	addLiquidity	External !		NO !
L	addLiquidityETH	External !		NO !
L	removeLiquidity	External !		NO !
L	removeLiquidityETH	External !		NO !
L	removeLiquidityWithPermit	External !		NO !
L	removeLiquidityETHWithPermit	External !		NO !
L	swapExactTokensForTokens	External !		NO !
L	swapTokensForExactTokens	External !		NO !
L	swapExactETHForTokens	External !		NO !
L	swapTokensForExactETH	External !		NO !
L	swapExactTokensForETH	External !		NO !
L	swapETHForExactTokens	External !		NO !
L	quote	External !		NO !
L	getAmountOut	External !		NO !
L	getAmountIn	External !		NO !
L	getAmountsOut	External !		NO !
L	getAmountsIn	External !		NO !

## Legend

Symbol	Meaning
	Function can modify state
	Function is payable

## Inheritance Hierarchy



# Security issue checking status

## ❖ High severity issues

No High severity issues found

## ❖ Medium severity issues

No medium severity issues found

## ❖ Low severity issues

No low severity issues found

## ❖ Centralization Risk

No Centralization Risk found



# Owner privileges

- ❖ Owner can get any bep20 tokens other than native tokens to owner wallet

```
ftrace | funcSig
function getBep20Tokens(address _tokenAddress↑, uint256 amount↑)
    external
    onlyOwner
{
    require(
        _tokenAddress↑ != address(this),
        "You can not withdraw native tokens"
    );
    require(
        IERC20(_tokenAddress↑).balanceOf(address(this)) >= amount↑,
        "No Enough Tokens"
    );
    IERC20(_tokenAddress↑).transfer(msg.sender, amount↑);
}
```

- ❖ Owner can get contract bnb balance to owner wallet

```
ftrace | funcSig
function clearStuckBalance(uint256 amountPercentage↑) external onlyOwner {
    uint256 amountBNB = address(this).balance;
    payable(msg.sender).transfer((amountBNB * amountPercentage↑) / 100);
}
```

- ❖ Owner can enable trading, once enabled cannot disable again

```
// switch Trading
ftrace | funcSig
function enableTrading() public onlyOwner {
    tradingOpen = true;
}
```

- ❖ Owner can whitelist presale address

```
ftrace | funcSig
function whitelistPreSale(address _preSale↑) public onlyOwner {
    isAuthorized[_preSale↑] = true;
    isMaxTxExempt[_preSale↑] = true;
    isMaxWalletExempt[_preSale↑] = true;
}
```

- ❖ Owner can change max transaction amount minimum up to 0.1%

```
ftrace | funcSig
function setMaxTxAmount(uint256 amount↑) external onlyOwner {
    require(
        amount↑ >= 1000000,
        "Minimum wallet token amount should grater than 0.1%"
    );

    maxTxAmount = amount↑ * (10**decimals);
}
```

- ❖ Owner can change max wallet token minimum up to 1%

```
ftrace | funcSig
function setMaxWalletToken(uint256 amount↑) external onlyOwner {
    require(
        amount↑ >= 10000000,
        "Minimum wallet token amount should grater than 1%"
    );

    maxWalletTokens = amount↑ * (10**decimals);
}
```

# Audit conclusion

RugFreeCoins team has performed in-depth testings, line-by-line manual code review, and automated audit of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, manipulations, and hacks. According to the smart contract audit.

Smart contract functional Status: **PASS**

Number of risk issues: **0**

Solidity code functional issue level: **PASS**

Number of owner privileges: **6**

Centralization risk correlated to the active owner: **LOW**

Smart contract active ownership: **YES**