



Smart Contract Security Audit

Project: World Cup Inu

Oct 13, 2022



Contract Address

0xcF7CA81e6ce541D49e19C16dA6C32BC3724e1897

Table of Contents

- 1 Disclaimer**
- 2 Audit Review**
- 3 Project Review**
- 4 Smart Contract Vulnerability Checks**
- 5 Manual Code Review**
- 6 Owner Privileges**
 - 6.1 Contract Ownership
 - 6.2 Liquidity Overview
- 7 Tokenomics**
- 8 Social Media Check**
- 9 Website Review**
- 10 Audit Conclusion**

Disclaimer

The contents of this report reflect only the CRACKEN TECH audit team's understanding of the current progress and status of the security of the code audited, to verify the integrity of the code provided for the scope of this audit. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Given the size of the project, the findings detailed here are not to be considered exhaustive, and further testing and audit are recommended after the issues covered are fixed. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report.

The review does not address the compiler layer, any other areas beyond the programming language, or other programming aspects that could present security risks. If the audited source files are smart contract files, risks or issues introduced by using data feeds from off-chain sources are not extended by this review either.

Audit Review

The source code of the World Cup Inu was audited in order to acquire a clear impression of how the project was implemented. The Cracken Tech audit team conducted in-depth research, analysis, and scrutiny, resulting in a series of observations. A detailed list of each issue found, and vulnerabilities in the source code will be included in the audit report. The problems and potential solutions are given in this report, we will identify common sources for such problems and comments for improvement.

The auditing process will follow a routine as special considerations by Cracken:

- Review of the specifications, sources, and instructions provided to Cracken to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Cracken describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code is exercised when we run the test cases.
- Symbolic execution is analyzing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

Project Review

Token Summary

Parameter	Result
Token Name	World Cup Inu
Token Symbol	WOCI
Token Decimal	18
Total Supply	100,000,000,000
Platform	BSC
Buy Tax Fee	7%
Sell Tax Fee	7%
Contract Creation Date	Oct 12, 2022
Liquidity Status	Not Available
Liquidity Lockup Time	Not Available
Compiler Version	v0.7.4+commit.3f05b770
Optimization	No with 200 runs
Contract Address	0xcF7CA81e6ce541D49e19C16dA6C32BC3724e1897
Deployer Address	0xe3c242aef07ee22b6fb19a33b4dd69639053c25a
Owner Address	0x6eb16956cbf1275e482a1e3cbecfecb669273e7

Source Code

CRACKEN was commissioned by World Cup Inu to perform an audit based on the following smart contract:

<https://bscscan.com/address/0xcF7CA81e6ce541D49e19C16dA6C32BC3724e1897>





Smart Contract Vulnerability Checks

Vulnerability	Auto-Scan	Manual-Scan	Result
Unencrypted Private Data On-Chain	Complete	Complete	Low / No Risk
Code With No Effects	Complete	Complete	Low / No Risk
Message call with hardcoded gas amount	Complete	Complete	Low / No Risk
Hash Collisions with Multiple Variable Length Arguments	Complete	Complete	Low / No Risk
Unexpected Ether balance	Complete	Complete	Low / No Risk
Presence of unused variables	Complete	Complete	Low / No Risk
Right-To-Left-Override control character (U+202E)	Complete	Complete	Low / No Risk
Typographical Error	Complete	Complete	Low / No Risk
DoS With Block Gas Limit	Complete	Complete	Low / No Risk
Arbitrary Jump with Function Type Variable	Complete	Complete	Low / No Risk
Insufficient Gas Grieving	Complete	Complete	Low / No Risk
Incorrect Inheritance Order	Complete	Complete	Low / No Risk
Write to Arbitrary Storage Location	Complete	Complete	Low / No Risk
Requirement Violation	Complete	Complete	Low / No Risk
Missing Protection against Signature Replay Attacks	Complete	Complete	Low / No Risk
Weak Sources of Randomness from Chain Attributes	Complete	Complete	Low / No Risk
Authorization through tx. origin	Complete	Complete	Low / No Risk
Delegate call to Untrusted Callee	Complete	Complete	Low / No Risk





Vulnerability	Auto-Scan	Manual-Scan	Result
Use of Deprecated Solidity Functions	Complete	Complete	Low / No Risk
Assert Violation	Complete	Complete	Low / No Risk
Reentrancy	Complete	Complete	Low / No Risk
Unprotected SELF-DESTRUCT Instruction	Complete	Complete	Low / No Risk
Unprotected Ether Withdrawal	Complete	Complete	Low / No Risk
Outdated Compiler Version	Complete	Complete	Low / No Risk
Integer Overflow and Underflow	Complete	Complete	Low / No Risk
Function Default Visibility	Complete	Complete	Low / No Risk

Manual Code Review

Classification of Issues

Severity	Description
 High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
 Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
 Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
 Informational	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
 High-Risk	3
 Medium-Risk	1
 Low-Risk	0
 Informational	1
Total	5

● High-Risk: functions make cause the rug or scam project. **Must be fixed.**

Set max buy / sell tax fee

Description:

The owner can change the buy & sell fees up to 50%.

[HIGH-RISK]

```
function setFees(uint256 _liquidityFee, uint256 _reflectionFee, uint256
_marketingFee, uint256 _ecosystemfee, uint256 _burnFee, uint256
_feeDenominator) external authorized {
    liquidityFee = _liquidityFee;
    reflectionFee = _reflectionFee;
    marketingFee = _marketingFee;
    ecosystemfee = _ecosystemfee;
    burnFee = _burnFee;
    totalFee =
    _liquidityFee.add(_reflectionFee).add(_marketingFee).add(_ecosystemfee).ad
d(_burnFee);
    feeDenominator = _feeDenominator;
    require(totalFee < feeDenominator/2, "Fees cannot be more than
50%");
}
```

Recommendation:

We recommend adding a requirement to lower the max fee amount.

● High-Risk: functions make cause the rug or scam project. **Must be fixed.**

The blacklist function is enabled

Description:

The owner can add blacklist wallets.

[HIGH RISK]

```
function setMaxWalletPercent_base1000(uint256 maxWallPercent_base1000)
external onlyOwner() {
    _maxWalletToken = (_totalSupply * maxWallPercent_base1000 ) /
1000;
}

function setMaxTxPercent_base1000(uint256
maxTXPercentage_base1000) external onlyOwner() {
    _maxTxAmount = (_totalSupply * maxTXPercentage_base1000 ) /
1000;
}

function setTxLimit(uint256 amount) external authorized {
    _maxTxAmount = amount;
}
```

Recommendation:

We recommend that the owner should disable the blacklist function.

● **Medium-Risk:** functions make cause a few bugs of the project. Should be fixed.

Set wallet max limit

Description:

The owner can set max tx amount without limit

[MEDIUM-RISK]

```
function setMaxWalletPercent_base1000(uint256 maxWallPercent_base1000)
external onlyOwner() {
    _maxWalletToken = (_totalSupply * maxWallPercent_base1000 ) /
1000;
}

function setMaxTxPercent_base1000(uint256
maxTXPercentage_base1000) external onlyOwner() {
    _maxTxAmount = (_totalSupply * maxTXPercentage_base1000 ) /
1000;
}

function setTxLimit(uint256 amount) external authorized {
    _maxTxAmount = amount;
}
```

Recommendation:

We recommend that the owner should disable the blacklist function.

● High-Risk: functions make cause the rug or scam project. **Must be fixed.**

The trading function is enabled to be paused

Description:

The owner can pause the trading.

[HIGH RISK]

```
function tradingStatus(bool _status) public onlyOwner {  
    tradingOpen = _status;  
}
```

Recommendation:

We recommend the owner disable this function.

- **Informational:** Implementation of certain corrective actions or accepting the risk.

Set cooldown when the trading function is enabled

Description:

The owner can set cooldown time when trading.

// enable cooldown between trades

```
function cooldownEnabled(bool _status, uint8 _interval) public onlyOwner  
{  
  
    buyCooldownEnabled = _status;  
  
    cooldownTimerInterval = _interval;  
  
}
```

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	External
approveMax	address spender	External
authorize	address adr	Public
clearStuckBalance	uint256 amountPercentage	External
clearStuckBalance_sender	uint256 amountPercentage	External
cooldownEnabled	bool _status, uint8 _interval	External
manage_blacklist	address[] calldata addresses, bool status	External
multiTransfer	address from, address[] calldata addresses, uint256[] calldata tokens	External
multiTransfer_fixed	address from, address[] calldata addresses, uint256 tokens	External
setDistributionCriteria	uint256 _minPeriod, uint256 _minDistribution	External
setDistributorSettings	uint256 gas	External
setFeeReceivers	address _autoLiquidityReceiver, address _marketingFeeReceiver, address _ecosystemfeeReceiver, address _burnFeeReceiver	External
setFees	uint256 _liquidityFee, uint256 _reflectionFee, uint256 _marketingFee, uint256 _ecosystemfee, uint256 _burnFee, uint256 _feeDenominator	External
setIsDividendExempt	address holder, bool exempt	External
setIsFeeExempt	address holder, bool exempt	External
setIsTimelockExempt	address holder, bool exempt	External

setIsTxLimitExempt	address holder, bool exempt	External
setMaxTxPercent_base1000	uint256 maxTXPercentage_base1000	External
setMaxWalletPercent_base1000	uint256 maxWallPercent_base1000	External
setSwapBackSettings	bool _enabled, uint256 _amount	External
setTargetLiquidity	uint256 _target, uint256 _denominator	External
setTxLimit	uint256 amount	External
set_sell_multiplier	uint256 Multiplier	External
tradingStatus	bool _status	Public
transfer	address recipient, uint256 amount	External
transferFrom	address sender, address recipient, uint256 amount	Public
transferOwnership	address newOwner	Public
unauthorize	address adr	Public

Contract Ownership

The contract ownership of World Cup Inu is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

The current owner is the address 0x6eb16956cbf1275e482a1e3cbecfecb669273e7 which can be viewed: [HERE](#)

The owner wallet has the power to call the functions displayed on the privileged functions list above, if the owner wallet is compromised these privileges could be exploited.

We recommend the team renounce ownership at the right timing if possible, or gradually migrate to a time lock with governing functionalities in respect of transparency and safety considerations.

Liquidity Overview

Liquidity Information

Parameter	Result
Pair Address	0xb3b52b01453eaa2225ecda2ef67e7ad86f701faf
WOCI Reserves	0.00 WOCI
BNB Reserves	0.00 BNB
Liquidity Value	\$0 USD
Liquidity Ownership	The token does not have liquidity at the moment of the audit

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x6eb16956cbf1275e482a1e3cbecfecb669273e7	100,000,000,000	100.0000%

Social Media Check

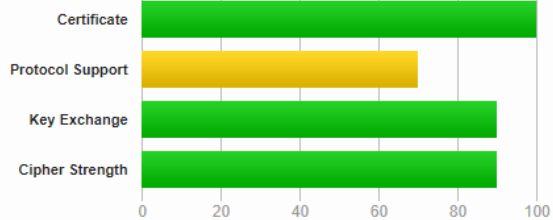
Social Media Type	Link	Result
Website	https://www.worldcupinubsc.com/	Checked
Twitter	https://twitter.com/worldcupinu_inu/	Checked
Telegram	https://t.me/WorldCupInu_GLO/	Checked

Website Review



Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports TLS 1.1. Grade capped to B. [MORE INFO »](#)

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	www.worldcupinubsc.com Fingerprint SHA256: ad0b0dbaab373b6799dad815b113406aecf8ceabedd674f3615a9fb35dodb481 Pin SHA256: yzCXOkXd+ZlIJQT5sGgiqgkA9XQ7765fRk81buvpGw=
Common names	www.worldcupinubsc.com
Alternative names	worldcupinubsc.com www.worldcupinubsc.com
Serial Number	033e3bca20b6de6d7cb00cb535cb27f34fea
Valid from	Tue, 11 Oct 2022 15:10:39 UTC
Valid until	Mon, 09 Jan 2023 15:10:38 UTC (expires in 2 months and 27 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencor.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	OCS OCSP: http://r3.o.lencor.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile version is quite Friendly
- Contains no code errors
- SSL is Secured
- No spelling errors

Audit Conclusion

- The owner cannot mint new tokens
- The owner can set cooldown time when trading.
- **The owner cannot pause trading [High-Risk]**
- **The owner can blacklist users [High-Risk]**
- **The owner can change the max tx amount without limit [High-Risk]**
- **The owner can change buy/sell fees up to 50% [High-Risk].**

(The fees cannot be changed if the owner renounced the ownership)