



# Smart Contract Security Audit

**Project: Panda Coin**

Oct 31, 2022



**Contract Address**

0x8c86e5A942386d10aF72879779dED335c9C634eE

# 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 Panda Coin 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	Panda Coin
Token Symbol	Panda
Token Decimal	18
Total Supply	1,000,000
Platform	BSC
Buy Tax Fee	4%
Sell Tax Fee	4%
Contract Creation Date	Jul 17, 2022
Liquidity Status	Not Available
Liquidity Lockup Time	Not Available
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	Yes with 200 runs
Contract Address	0x8c86e5A942386d10aF72879779dED335c9C634eE
Deployer Address	0xb10717a41930091b6B9D7fDaa261FA06c40A2a41
Owner Address	0xb10717a41930091b6B9D7fDaa261FA06c40A2a41

### Source Code

CRACKEN was commissioned by Panda Coin to perform an audit based on the following smart contract:

<https://bscscan.com/address/0x8c86e5A942386d10aF72879779dED335c9C634eE>





## 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	0
 Medium-Risk	1
 Low-Risk	1
 Informational	0
Total	2



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

## Set blacklist users

Description:

### The owner can set blacklist users

#### [MEDIUM-RISK]

```
function multipleBotlistAddress(address[] calldata accounts, bool excluded) public  
onlyOwner {  
    for (uint256 i = 0; i < accounts.length; i++) {  
        _isBlacklisted[accounts[i]] = excluded;  
    }  
}
```

#### Recommendation:

We recommend that the owner should disable the blacklist function.

● **Low-Risk:** Implementation of certain corrective actions or accepting the risk.

## Set Buy / Sell Fees

Description:

Total fees can be changed up to 25%.

```
function setBuyTaxes(uint256 liquidity, uint256 rewardsFee, uint256 marketingFee,
uint256 deadFee) external onlyOwner {
    require(rewardsFee.add(liquidity).add(marketingFee).add(deadFee) <= 25, "Total
buy fee is over 25%");
    buyTokenRewardsFee = rewardsFee;
    buyLiquidityFee = liquidity;
    buyMarketingFee = marketingFee;
    buyDeadFee = deadFee;
}
```

```
function setSelTaxes(uint256 liquidity, uint256 rewardsFee, uint256 marketingFee,
uint256 deadFee) external onlyOwner {
    require(rewardsFee.add(liquidity).add(marketingFee).add(deadFee) <= 25, "Total
sel fee is over 25%");
    sellTokenRewardsFee = rewardsFee;
    sellLiquidityFee = liquidity;
    sellMarketingFee = marketingFee;
    sellDeadFee = deadFee;
}
```

## Recommendation:

**Total buy and sell fees should be less than 25%.**

## Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
decreaseAllowance	address spender, uint256 subtractedValue	Public
excludeFromDividends	address account	External
excludeFromFees	address account, bool excluded	Public
excludeMultipleAccountsFromFees	address[] calldata accounts, bool excluded	Public
increaseAllowance	address account, bool excluded	Public
processDividendTracker	Unit256 gas	External
setAutomatedMarketMakerPair	address pair, bool value	Public
renounceOwnership	Unit256 _amount	Public
setBuyTaxes	int256 liquidity, uint256 rewardsFee, uint256 marketingFee, uint256 deadFee	External
setMarketingFee	uint256 value	External
setDeadWallet	address addr	Public
setSellTaxes	int256 liquidity, uint256 rewardsFee, uint256 marketingFee, uint256 deadFee	External
transferOwnership	address newOwner	Public
setSwapTokensAmount	uint256 amount	Public
updateClaimWait	uint256 newClaimWait	External
updateDividendTracker	address newAddress	Public
updateGasForProcessing	uint256 newValue	Public
updateMinimumTokenBalanceForDividends	uint256 amount	External

## Contract Ownership

The contract ownership of Panda Coin 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 0xb10717a41930091b6B9D7fDaa261FA06c40A2a41 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 time 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	0xf81d200f2aa309bf5f62e1963e8c2dd66d54e1e4
Panda Reserves	0.00 Panda
BNB Reserves	0.00 BNB
Liquidity Value	\$0 USD
Liquidity Ownership	The token does not have liquidity at the moment of the audit

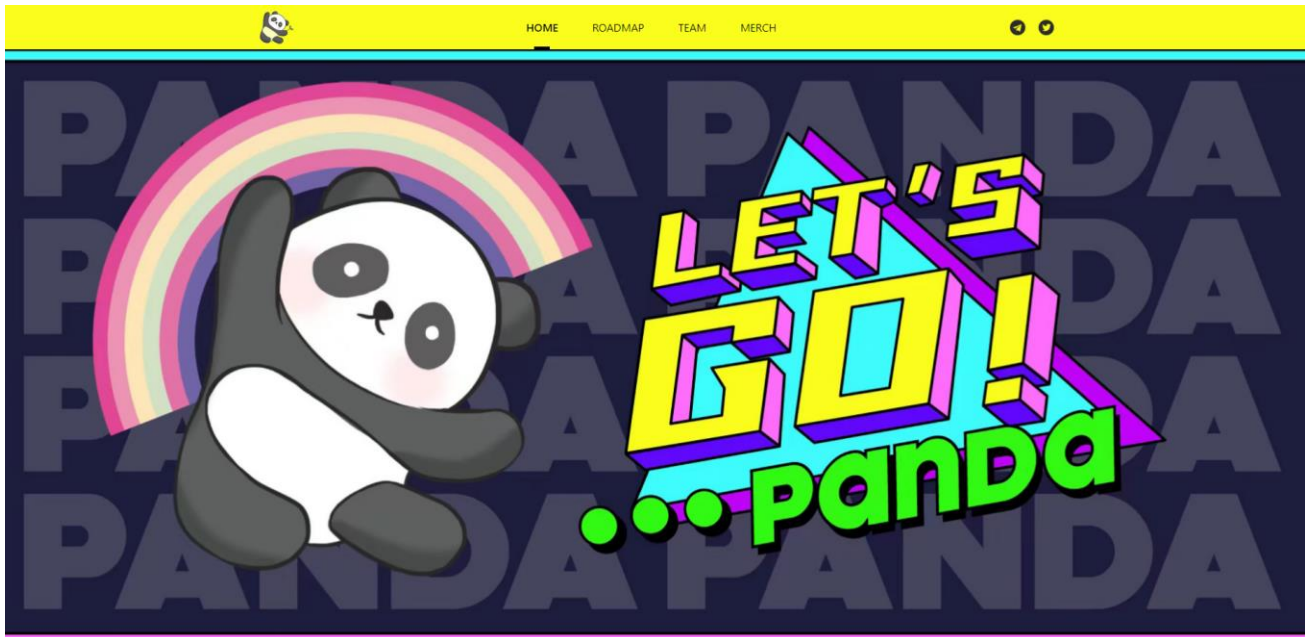
## Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x3ae7022bb6ee3222f8d7e9143b762d41b0888888	1,000,000	100.0000%

## Social Media Check

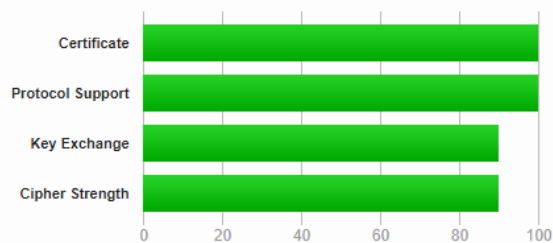
Social Media Type	Link	Result
Website	<a href="https://pandacion.club/">https://pandacion.club/</a>	Checked
Twitter	<a href="https://twitter.com/PandacoinCN/">https://twitter.com/PandacoinCN/</a>	Checked
Telegram	<a href="https://t.me/PandacoinCN/">https://t.me/PandacoinCN/</a>	Checked

## Website Review



### Summary

Overall Rating



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

This site works only in browsers with SNI support.

## Certificate #1: RSA 2048 bits (SHA256withRSA)



### Server Key and Certificate #1



<b>Subject</b>	pandacion.club Fingerprint SHA256: 19160dad827cb4c6527d8df07172d2627a9d495bb3f090e32d7e6653909ec4d0 Pin SHA256: FOsUPnVgQvxlNkOGBvtJyhcoKL565r7WXeGUHTqt2Ug=
<b>Common names</b>	pandacion.club
<b>Alternative names</b>	pandacion.club www.pandacion.club
<b>Serial Number</b>	09d9dd6520fc199bf0e128f4ab134561
<b>Valid from</b>	Mon, 10 Oct 2022 00:00:00 UTC
<b>Valid until</b>	Tue, 10 Oct 2023 23:59:59 UTC (expires in 11 months and 10 days)
<b>Key</b>	RSA 2048 bits (e 65537)
<b>Weak key (Debian)</b>	No
<b>Issuer</b>	Encryption Everywhere DV TLS CA - G1 AIA: <a href="http://cacerts.digicert.com/EncryptionEverywhereDVTLSCA-G1.crt">http://cacerts.digicert.com/EncryptionEverywhereDVTLSCA-G1.crt</a>
<b>Signature algorithm</b>	SHA256withRSA
<b>Extended Validation</b>	No
<b>Certificate Transparency</b>	Yes (certificate)
<b>OCSP Must Staple</b>	No
<b>Revocation information</b>	OCSP OCSP: <a href="http://ocsp.digicert.com">http://ocsp.digicert.com</a>
<b>Revocation status</b>	Good (not revoked)
<b>DNS CAA</b>	No ( <a href="#">more info</a> )
<b>Trusted</b>	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL Secured
- No spelling errors

## Audit Conclusion

- The owner cannot pause trading
- The owner cannot mint new tokens
- **The owner can blacklist users [Medium-Risk]**
- The owner cannot change the max tx amount
- The owner can change buy/sell fees up to 25%.  
(The fees cannot be changed if the owner renounced the ownership)

**AUDIT IS PASSED**