



Smart Contract Security Audit

Project: CryptoDNF

Oct 31, 2022



Contract Address

0x7B9F4E67B0a087D47e79AC35c96016BD7232E339

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 CryptoDNF 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	CryptoDNF
Token Symbol	CDNF
Token Decimal	9
Total Supply	50,000,000,000
Platform	BSC
Buy Tax Fee	3%
Sell Tax Fee	3%
Contract Creation Date	Oct 30, 2022
Liquidity Status	Not available when audit
Liquidity Lockup Time	Not available when audit
Compiler Version	v0.8.14+commit.80d49f37
Optimization	Yes with 200 runs
Contract Address	0x7B9F4E67B0a087D47e79AC35c96016BD7232E339
Deployer Address	0x252d483e081b73B1f10812350381e49514Fbb771
Owner Address	0x252d483e081b73B1f10812350381e49514Fbb771

Source Code

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

<https://bscscan.com/address/0x7B9F4E67B0a087D47e79AC35c96016BD7232E339>





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	4
---	---

 Medium-Risk	0
---	---

 Low-Risk	0
--	---

 Informational	0
---	---

Total	4
-------	---

● 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 100%

[HIGH-RISK]

```
function setBuyFundFee(uint256 fundFee) external onlyOwner {  
    _buyFundFee = fundFee;  
}  
  
function setSellLPDividendFee(uint256 dividendFee) external onlyOwner {  
    _sellLPDividendFee = dividendFee;  
}  
  
function setSellFundFee(uint256 fundFee) external onlyOwner {  
    _sellFundFee = fundFee;  
}  
  
function setSellLPFee(uint256 lpFee) external onlyOwner {  
    _sellLPFee = lpFee;  
}
```

Recommendation:

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

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

Set trading function is enabled

Description:

The owner can set close trading [HIGH-RISK]

```
function returnMoon() external onlyOwner {  
  
    goMoonBlock = 0;  
  
}
```

Recommendation:

We recommend removing the trading function for safety.

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

The blacklist function is enabled

Description:

The owner can add blacklist users

[HIGH-RISK]

```
function multiCheater(address[] calldata addresses, bool value) public onlyOwner{  
  
    require(addresses.length < 201);  
  
    for (uint256 i; i < addresses.length; ++i) {  
  
        _gameCheater[addresses[i]] = value;  
  
    }  
}
```

Recommendation:

We recommend that the owner should disable the blacklist function.

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

Set max Tx Amount function

Description:

The owner can set max Tx amount without a limit.

[HIGH-RISK]

```
function setMaxTxAmount(uint256 max) public onlyOwner {  
  
    maxTXAmount = max;  
  
}
```

Recommendation:

We recommend that the owner should limit the max tx amount.

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	Public
claimToken	address token, uint256 amount, address to	External
claimBalance	None	External
goMoon	None	External
renounceOwnership	None	Public
multiCheater	address[] calldata addresses, bool value	External
returnMoon	None	External
setBuyFundFee	uint256 fundFee	External
setBuyLPDividendFee	uint256 dividendFee	External
setCheater	address addr, bool enable	External
setFeeWhiteList	address addr, bool enable	External
setFundAddress	address addr	External
setMaxTxAmount	uint256 max	Public
setSellFundFee	uint256 fundFee	External
setSellLPDividendFee	uint256 lpFee	External
setSellLPFee	uint256 dividendFee	External
transfer	address recipient, uint256 amount	External
transferFrom	address sender, address recipient, uint256 amount	Public
transferOwnership	address newOwner	Public

Contract Ownership

The contract ownership of CryptoDNF is not currently being 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 0x252d483e081b73B1f10812350381e49514Fbb771 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	0xe635b6a9c1be212477bb8f8c2f776366a5600931
CDNF Reserves	0.00 CDNF
BNB Reserves	0.00 BNB
Liquidity Value	\$0.00 USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit

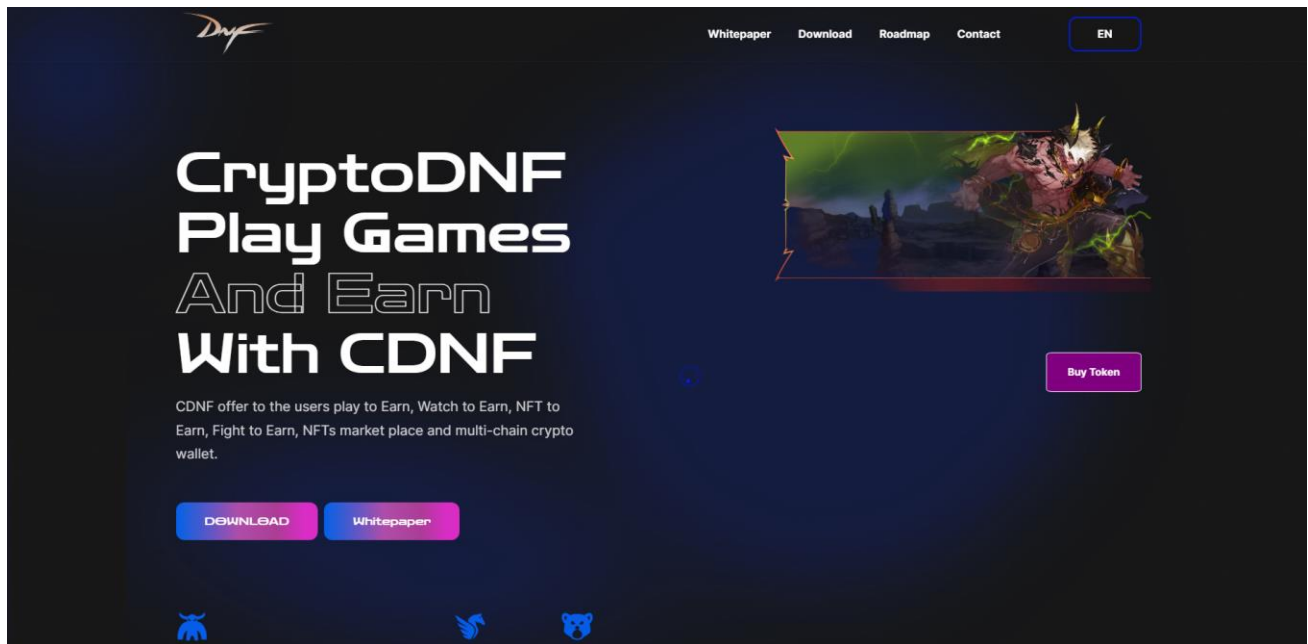
Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	Pinksale: PinkLock V2	34,800,000,000	69.6000%
2	0x28c4ce19373ece8de7b93db7af8443d3e3031945	14,472,000,000	28.9440%
3	0x7e442e01d64e690dc9cd94a9d9aa414b61820181	728,000,000	1.4560%

Social Media Check

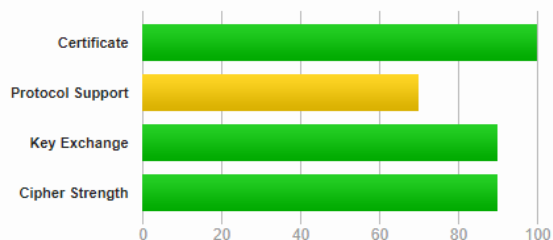
Social Media Type	Link	Result
Website	https://www.cryptodnf.net/	Checked
Twitter	https://twitter.com/CryptoDNF/	Checked
Telegram	https://t.me/CryptoDNF_BSC/	Checked

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 »](#)

DNS Certification Authority Authorization (CAA) Policy found for this domain. [MORE INFO »](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1



Subject	www.cryptodnf.net Fingerprint SHA256: 5db5de5f419c3885a16bfb017a1fbf7ca13b302fba8b8ff243f39cc42d18d2a9 Pin SHA256: TmAeapN+hj1m7PczUIBzWnw84HC0GfxSBIMRR3iyi9U=
Common names	www.cryptodnf.net
Alternative names	www.cryptodnf.net
Serial Number	04ab29d328138878e568381a235dac8b80cf
Valid from	Thu, 27 Oct 2022 05:04:42 UTC
Valid until	Wed, 25 Jan 2023 05:04:41 UTC (expires in 2 months and 25 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	OCSP OCSP: http://r3.o.lencor.org
Revocation status	Good (not revoked)
DNS CAA	Yes policy host: www.cryptodnf.net issue: letsencrypt.org flags:1 issue: trust-provider.com flags:0
Trusted	Yes Mozilla Apple Android Java Windows

- Mobile Friendly
- Contains no code errors
- SSL is secured
- No spelling errors

Audit Conclusion

- The owner cannot pause trading.
- The owner cannot mint new tokens.
- **The owner can disable trading function [High-Risk].**
- **The owner can add blacklist users [High-Risk].**
- **The owner can set the max transaction amount without a limit [High-Risk].**
- **The owner can change the buy/sell fee up to 100% [High-Risk].**

(All functions cannot be used if the ownership is renounced)