CRACKEN

Smart Contract Security Audit

Project: Newpoliton Dog

Oct 28, 2022

Contract Address

0x8d4333986d5e81027Fcd38c296D0B793D7128B60

Table of Contents

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 Newpoliton Dog 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	NewpolitonDog
Token Symbol	NewpolitonDog
Token Decimal	9
Total Supply	100,000,000
Platform	BSC
Buy Tax Fee	0%
Sell Tax Fee	1%
Contract Creation Date	Oct 27, 2022
Liquidity Status	Not available when audit
Liquidity Lockup Time	Not available when audit
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	Yes with 200 runs
Contract Address	0x8d4333986d5e81027Fcd38c296D0B793D7128B60
Deployer Address	0x8590498c29c5f1f88be2aa17b40B2f25b27953Cc
Owner Address	0x8590498c29c5f1f88be2aa17b40B2f25b27953Cc

Source Code

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

https://bscscan.com/address/0x8d4333986d5e81027Fcd38c296D0B793D7128B60

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 setBuyTaxes(uint256 newLiquidityTax, uint256 newMarketingTax, uint256
newburnedTax) external onlyOwner() {
        _buyLiquidityFee = newLiquidityTax;
        _buyMarketingFee = newMarketingTax;
        _buyburnedFee = newburnedTax;

        _totalTaxIfBuying =
_buyLiquidityFee.add(_buyMarketingFee).add(_buyburnedFee);
    }

    function setSellTaxes(uint256 newLiquidityTax, uint256 newMarketingTax, uint256
newburnedTax) external onlyOwner() {
        _sellLiquidityFee = newLiquidityTax;
        _sellMarketingFee = newMarketingTax;
        _sellburnedFee = newburnedTax;

        _totalTaxIfSelling =
_sellLiquidityFee.add(_sellMarketingFee).add(_sellburnedFee);
    }
```

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 max tx amount

Description:

The owner can change Max Transaction Amount without limit

[HIGH-RISK]

```
function setMaxTxAmount(uint256 maxTxAmount) external onlyOwner() {

        _maxTxAmount = maxTxAmount;

    }
```

Recommendation:

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

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

Set max Wallet Limit

Description:

The owner can set Wallet Max Amount without limit [HIGH-RISK]

```
function setWalletLimit(uint256 newLimit) external onlyOwner {

        _walletMax    = newLimit;

    }
```

Recommendation:

We recommend adding a requirement to limit the max transaction 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 users

[HIGH-RISK]

```
function setblocklist(address _account) external onlyOwner {

        if (isbotBlackList[_account]) {

            isbotBlackList[_account] = false;

        } else {

            isbotBlackList[_account] = true;

        }

    }
```

Recommendation:

We recommend that the owner should disable the blacklist function.

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
UPendtime	uint256 _endtime	External
UPfeeTXtime	uint256 _feeTXtime	External
approve	address spender, uint256 amount	Public
changeRouterVersion	address newRouterAddress	Public
decreaseAllowance	address spender, uint256 subtractedValue	Public
enableDisableWalletLimit	bool newValue	External
increaseAllowance	address spender, uint256 addedValue	Public
setBuyTaxes	uint256 newLiquidityTax, uint256 newMarketingTax, uint256 newburnedTax	External
setDistributionSettings	uint256 newLiquidityShare, uint256 newMarketingShare, uint256 newburnedShare	External
setIsExcludedFromFee	address account, bool newValue	Public
setIsTxLimitExempt	address holder, bool exempt	External
setIsWalletLimitExempt	address holder, bool exempt	External
setMarketPairStatus	address account, bool newValue	Public
setMarketingWalletAddress	address newAddress	External
setMaxTxAmount	uint256 maxTxAmount	External
setNumTokensBeforeSwap	uint256 newLimit	External
setSellTaxes	int256 newLiquidityTax, uint256 newMarketingTax, uint256 newburnedTax	External
setSwapAndLiquifyByLimitOnly	bool newValue	Public

Function Name	Parameters	Visibility
setSwapAndLiquifyEnabled	bool _enabled	Public
setWalletLimit	uint256 newLimit	External
setblocklist	address _account	External
setburnedWalletAddress	address newAddress	External
transfer	address recipient, uint256 amount	External
transferFrom	address sender,address recipient,uint256 amount	Public
transferOwnership	address newOwner	Public
waiveOwnership	None	Public

Contract Ownership

The contract ownership of Newpoliton Dog 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 0x8590498c29c5f1f88be2aa17b40B2f25b27953Cc 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	0x8bdcfcd5778fd83250f065394b37789ce5af6328
NewpolitonDog Reserves	0.00 NewpolitonDog
BNB Reserves	0.00 BNB
Liquidity Value	$0.00 USDT
Liquidity Ownership	The token does not have liquidity at the moment of the audit

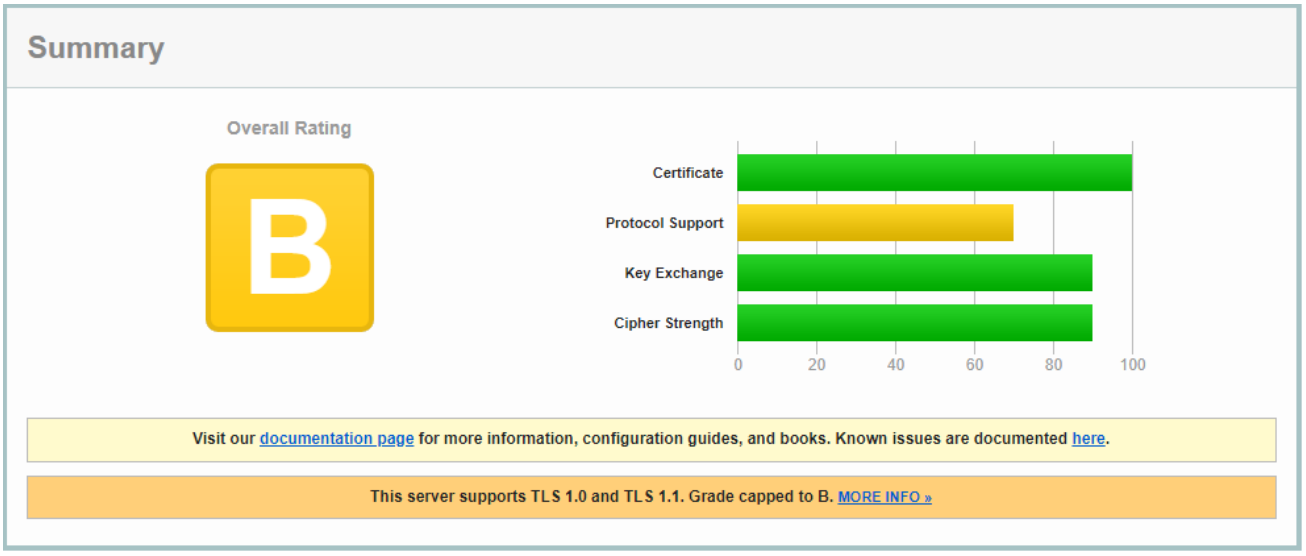
Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	0x8590498c29c5f1f88be2aa17b40b2f25b27953cc	100,000,000	100.0000%

Social Media Check

Social Media Type	Link	Result
Website	https://newpoliton.xyz/	Checked
Telegram	https://t.me/newpolitondog/	Checked

Website Review



Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	newpoliton.xyz Fingerprint SHA256: 932f4780078723a6f61f0e5c84081dd2e14b7a045e36a48cabebd40829d74485 Pin SHA256: T1uWKfDsb9xVtaLst8RNwOEh8Qvj/sLBh9M+liHqFLI=
Common names	newpoliton.xyz
Alternative names	newpoliton.xyz www.newpoliton.xyz
Serial Number	03581c4ec2b7ab7456c8c915c01c67e26481
Valid from	Wed, 26 Oct 2022 12:18:10 UTC
Valid until	Tue, 24 Jan 2023 12:18:09 UTC (expires in 2 months and 26 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
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 add blacklist users [High-Risk].**
- **The owner can set the max wallet amount without limit [High-Risk].**
- **The owner can set the max transaction amount without 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)