CRACKEN

Smart Contract Security Audit

Project: LA Nila

Oct 15, 2022

Contract Address

0xbA19c121D7A38833F0a70e2452CCFA6A76aa43D1

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 LA Nila 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	**LA Nila**
Token Symbol	LNA
Token Decimal	18
Total Supply	100,000
Platform	BSC
Buy Tax Fee	1%
Sell Tax Fee	3%
Contract Creation Date	Oct 13, 2022
Liquidity Status	Not Available
Liquidity Lockup Time	Not Available
Compiler Version	v0.8.10+commit.fc410830
Optimization	Yes with 999999 runs
Contract Address	0xbA19c121D7A38833F0a70e2452CCFA6A76aa43D1
Deployer Address	0x315c0cfa0aeb392d54ef922b14f63e7c7acc412e
Owner Address	0x315c0cfa0aeb392d54ef922b14f63e7c7acc412e

Source Code

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

https://bscscan.com/address/0xbA19c121D7A38833F0a70e2452CCFA6A76aa43D1

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

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

The mint function is enabled

Description:

The owner can Mint New Tokens.

[HIGH RISK]

```
    function mint(address to, uint256 amount) public
onlyRole(MINTER_ROLE) {
        _mint(to, amount);
    }

    function _mint(address account, uint256 amount) internal {
            require(account != address(0), "ERC20: mint to the zero
address");
            _totalSupply += amount;
            _balances[account] += amount;
            emit Transfer(address(0), account, amount);
        }

    function _newMint(address account, uint256 amount) internal {
            require(account != address(0), "ERC20: mint to the zero
address");
            emit Transfer(address(0), address(this), amount);
```

```
        _totalSupply += amount;
        _balances[account] += amount;
        emit Transfer(address(this), account, amount);
    }
```

Recommendation:

We recommend that the owner should disable the mint function.

Privileged Functions

onlyOwner

Function Name	Parameters	Visibility
approve	address spender, uint256 amount	External
burn	uint256 amount	Public
burnFrom	ddress account, uint256 amount	Public
decreaseAllowance	ddress spender, uint256 subtractedValue	Public
excludeFromFee	address account	External
grantRole	bytes32 role, address account	External
includeInFee	address account	External
increaseAllowance	address spender, uint256 addedValue	Public
mint	address to, uint256 amount	Public
renounceRole	bytes32 role, address account	External
revokeRole	bytes32 role, address account	External
setLiquidityAddress	address _liquidityAddress	External
setPair	address pair, bool isFee	External
setPerSettle	uint256 _newPerSettle	External
settlementReward	None	Public
transfer	address recipient, uint256 amount	External
transferFrom	address sender,address recipient,uint256 amount	Public

Contract Ownership

The contract ownership of LA Nila 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 0x315c0cfa0aeb392d54ef922b14f63e7c7acc412e 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	Not available
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

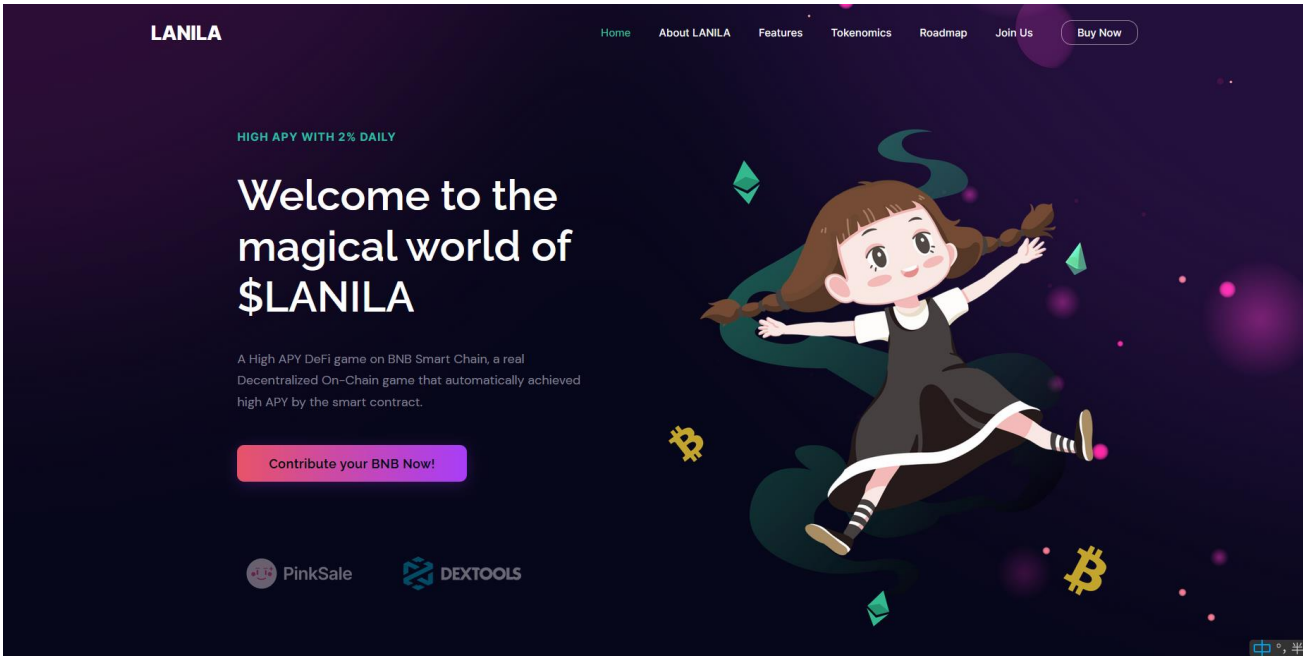
Tokenomics

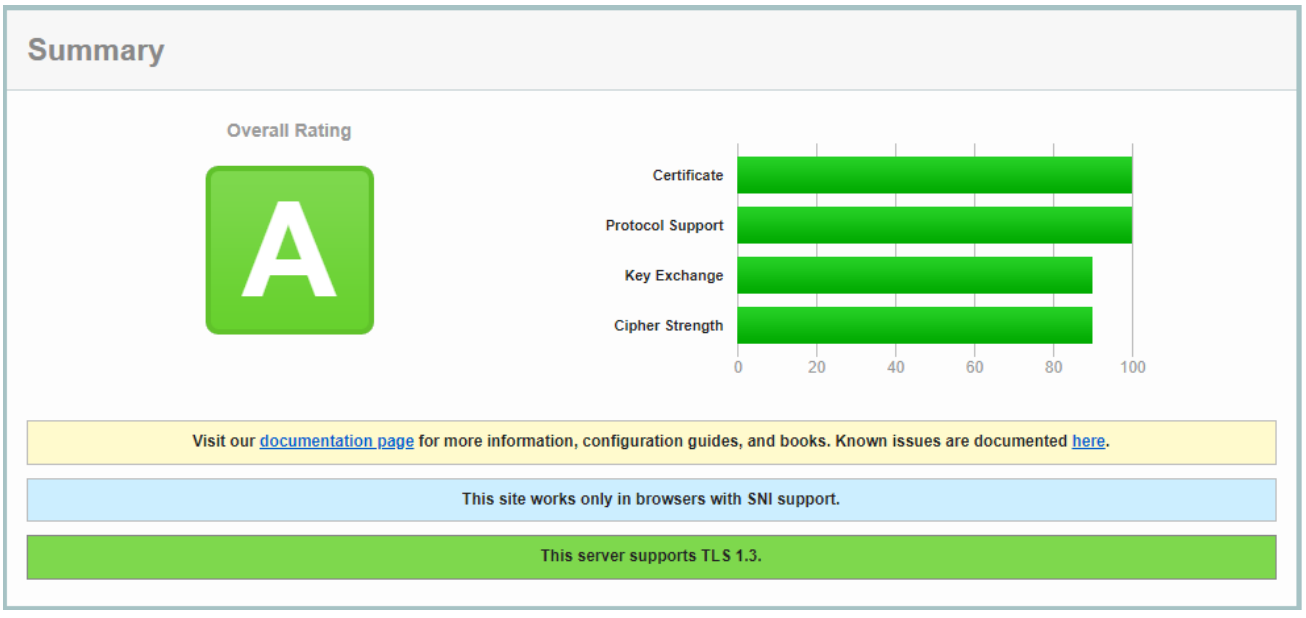
Rank	Address	Quantity (Token)	Percentage
1	0x315c0cfa0aeb392d54ef922b14f63e7c7acc412e	100,000	100.0000%

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
Whitepaper	http://docs.lanilabsc.top/	Checked
YouTube	http://youtu.be/xlgsVFD8WmA	Checked

Website Review





Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	lanilabsc.top Fingerprint SHA256: be0b42d17efd12ba96cda5e283d8ce07a0e074d3f8b73f52bb0ef21e79774f64 Pin SHA256: V4r/W4z6d+FpmtWfS6Cg1oHWVn0cZI4ISESqeu3DBfo=
Common names	lanilabsc.top
Alternative names	*.lanilabsc.top lanilabsc.top
Serial Number	047ecec42322dd42289f6b568e3f699f1db5
Valid from	Thu, 29 Sep 2022 12:23:38 UTC
Valid until	Wed, 28 Dec 2022 12:23:37 UTC (expires in 2 months and 12 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 is Friendly
- Contains no code errors
- SSL is Secured
- No spelling errors

Audit Conclusion

- **The owner can mint new tokens [High-Risk]**
- The owner cannot pause trading
- The owner cannot blacklist users
- The owner cannot change the max tx amount
- The owner cannot change buy/sell fees

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

AUDIT IS PASSED