



# AUDIT REPORT

---

May , 2025

For

**WAVE**

# Table of Content

Table of Content	02
Executive Summary	03
Number of Issues per Severity	05
Checked Vulnerabilities	06
Techniques & Methods	08
Types of Severity	10
Types of Issues	11
 <b>Low Severity Issues</b>	12
1. Local Variables being shadowed	12
 <b>Informational Severity Issues</b>	13
1. Unused interface ERC721	13
Closing Summary & Disclaimer	14

# Executive Summary

**Project name** One Wave

**Project URL** <https://www.onewave.app/>

**Overview** OneWave is a multi-chain, multi-utility Web3 ecosystem designed to unify various blockchain services across multiple networks, including Binance Smart Chain, Polygon, Lycan, and Ethereum.

One Wave is a token contract that implements a comprehensive token management system. It includes standard token functionalities such as transfer, minting, and burning, with a total supply of 1 billion and 25 million tokens on each chain(BSC,Polygon,ethereum and lycan). A unique feature is its ability to interact with other contracts, allowing the owner to transfer tokens or Ether to specified addresses

**Audit Scope** The scope of this Audit was to analyze the One Wave Token Smart Contracts for quality, security, and correctness.

**Source Code link** <https://bsc-scan.com/token/0xd41b1c813ad0873a68dfa6dc9e64beb9a30d9253>

**Contracts in Scope** Wave

**Branch** NA

**Commit Hash** NA

**Language** Solidity



<b>Blockchain</b>	Binance smart chain Ethereum Chain Polygon Chain Lycan Chain
<b>Method</b>	Manual Analysis, Functional Testing, Automated Testing
<b>Review 1</b>	28th April 2025
<b>Updated Code Received</b>	NA
<b>Review 2</b>	NA
<b>Fixed In</b>	NA

# Number of Issues per Severity



High	0 (0.00%)
Medium	0 (0.00%)
Low	1(50.00%)
Informational	1(50.00%)

Issues	Severity			
	High	Medium	Low	Informational
Open	0	0	0	0
Resolved	0	0	0	0
Acknowledged	0	0	1	1
Partially Resolved	0	0	0	0

# Checked Vulnerabilities

<input checked="" type="checkbox"/> Access Management	<input checked="" type="checkbox"/> Compiler version not fixed
<input checked="" type="checkbox"/> Arbitrary write to storage	<input checked="" type="checkbox"/> Address hardcoded
<input checked="" type="checkbox"/> Centralization of control	<input checked="" type="checkbox"/> Divide before multiply
<input checked="" type="checkbox"/> Ether theft	<input checked="" type="checkbox"/> Integer overflow/underflow
<input checked="" type="checkbox"/> Improper or missing events	<input checked="" type="checkbox"/> ERC's conformance
<input checked="" type="checkbox"/> Logical issues and flaws	<input checked="" type="checkbox"/> Dangerous strict equalities
<input checked="" type="checkbox"/> Arithmetic Computations Correctness	<input checked="" type="checkbox"/> Tautology or contradiction
<input checked="" type="checkbox"/> Race conditions/front running	<input checked="" type="checkbox"/> Return values of low-level calls
<input checked="" type="checkbox"/> SWC Registry	<input checked="" type="checkbox"/> Missing Zero Address Validation
<input checked="" type="checkbox"/> Re-entrancy	<input checked="" type="checkbox"/> Private modifier
<input checked="" type="checkbox"/> Timestamp Dependence	<input checked="" type="checkbox"/> Revert/require functions
<input checked="" type="checkbox"/> Gas Limit and Loops	<input checked="" type="checkbox"/> Multiple Sends
<input checked="" type="checkbox"/> Exception Disorder	<input checked="" type="checkbox"/> Using suicide
<input checked="" type="checkbox"/> Gasless Send	<input checked="" type="checkbox"/> Using delegatecall
<input checked="" type="checkbox"/> Use of tx.origin	<input checked="" type="checkbox"/> Upgradeable safety
<input checked="" type="checkbox"/> Malicious libraries	<input checked="" type="checkbox"/> Using throw

Using inline assembly Unsafe type inference Style guide violation Implicit visibility level

# Techniques and Methods

Throughout the audit of smart contracts, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments, match logic and expected behavior.
- Token distribution and calculations are as per the intended behavior mentioned in the whitepaper.
- Implementation of ERC standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

**The following techniques, methods, and tools were used to review all the smart contracts.**

## Structural Analysis

In this step, we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

## Static Analysis

A static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

**Code Review / Manual Analysis**

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

**Gas Consumption**

In this step, we have checked the behavior of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

**Tools And Platforms Used For Audit**

Remix IDE, Foundry, Solhint, Mythril, Slither, Solidity statistical analysis.

# Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below

## ● High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

## ■ Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

## ● Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

## ■ Informational Issues

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

# Types of Issues

<b>Open</b>  Security vulnerabilities identified that must be resolved and are currently unresolved.	<b>Resolved</b>  Security vulnerabilities identified that must be resolved and are currently unresolved.
<b>Acknowledged</b>  Vulnerabilities which have been acknowledged but are yet to be resolved.	<b>Partially Resolved</b>  Considerable efforts have been invested to reduce the risk/ impact of the security issue, but are not completely resolved.

# Low Severity Issues

## Local Variables being shadowed

Acknowledged

### Path

<https://bscscan.com/token/0xd41b1c813ad0873a68dfa6dc9e64beb9a30d9253#code>

### Function

\_approve()

### Description

The issue reported is a variable/function shadowing problem. In the 'WAVE' contract, the `\_approve()` function has a parameter named `owner`, which shadows the `owner()` function from the `Ownable` contract. This can lead to confusion and potential errors in the code, as the `owner` parameter in `\_approve` is a local variable and not the `owner()` function that returns the contract owner address.

```
function _approve(address owner, address spender, uint256 amount) internal {
    require(owner != address(0), "BEP20: approve from the zero address");
    require(spender != address(0), "BEP20: approve to the zero address");

    _allowances[owner][spender] = amount;
    emit Approval(owner, spender, amount);
}
```

### Recommendation

Change the owner param to \_owner in the \_approve() internal function.

# Informational Severity Issues

## Unused interface ERC721

Acknowledged

### Path

<https://bscscan.com/token/0xd41b1c813ad0873a68dfa6dc9e64beb9a30d9253#code>

### Function

-

### Description

The contract declares that it implements the ERC721 interface, but no functions or functionalities from this interface are utilized within the contract's code. This unnecessary declaration increases the contract's size and could lead to potential confusion regarding its intended behavior. Removing this unused interface will optimize the contract's bytecode and improve its clarity.

### Recommendation

Remove the interface for the ERC721.



# Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

# Closing Summary

In this report, we have considered the security of One Wave. We performed our audit according to the procedure described above.

Low and informational severity issues were found. One Wave team acknowledge them all.

The code is of good quality, with no critical issues identified. The issues noted are minor in nature and do not impact the overall functionality of the project.

# Disclaimer

At QuillAudits, we have spent years helping projects strengthen their smart contract security. However, security is not a one-time event—threats evolve, and so do attack vectors. Our audit provides a security assessment based on the best industry practices at the time of review, identifying known vulnerabilities in the received smart contract source code.

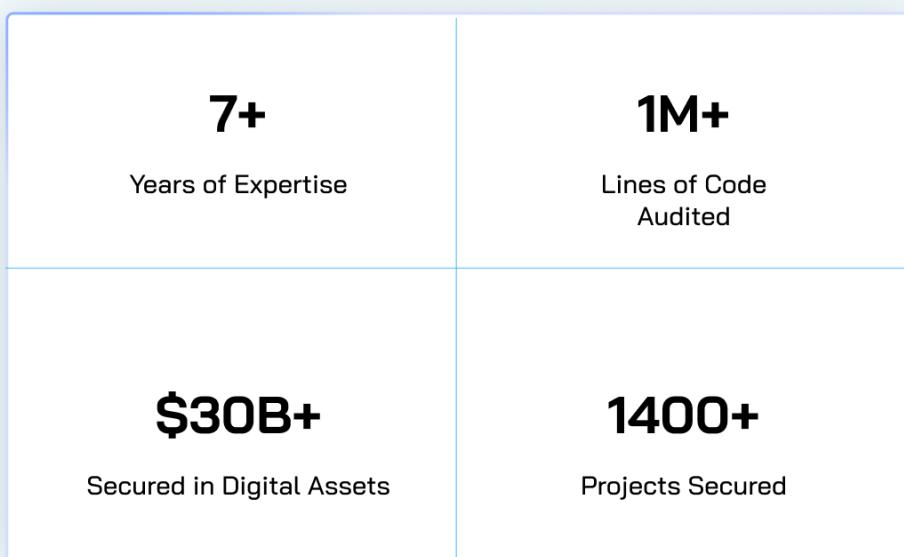
This report does not serve as a security guarantee, investment advice, or an endorsement of any platform. It reflects our findings based on the provided code at the time of analysis and may no longer be relevant after any modifications. The presence of an audit does not imply that the contract is free of vulnerabilities or fully secure.

While we have conducted a thorough review, security is an ongoing process. We strongly recommend multiple independent audits, continuous monitoring, and a public bug bounty program to enhance resilience against emerging threats.

Stay proactive. Stay secure.

# About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem



Follow Our Journey



# AUDIT REPORT

---

May , 2025

For

**WAVE**



QuillAudits

Canada, India, Singapore, UAE, UK

[www.quillaudits.com](http://www.quillaudits.com)    [audits@quillaudits.com](mailto:audits@quillaudits.com)