



SECURE BE.

BUILD TRUST IN YOUR  
PROJECT WITH  
OUR AUDIT



19 OCTOBER 2023

SECUREBE.COM



# Table Of Content

---

- 1 Summary**
- 2 Overview**
- 3 — 4 Vulnerability Check**
- 5 Owner Privileges**



# Summary

---

**This report has been prepared for botifi.ai to discover issues and vulnerabilities in the source code of the botifi.ai project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilising Static Analysis and Manual Review techniques.**

**The auditing process pays special attention to the following considerations:**

- **Testing the smart contracts against both common and uncommon attack vectors.**
- **Assessing the codebase to ensure compliance with current best practices and industry standards.**
- **Ensuring contract logic meets the specifications and intentions of the client.**
- **Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.**
- **Thorough line-by-line manual review of the entire codebase by industry experts.**

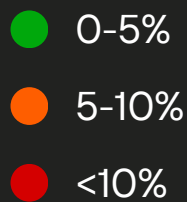
**The security assessment resulted in findings that ranged from Medium to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:**

- **Enhance general coding practices for better structures of source codes;**
- **Add enough unit tests to cover the possible use cases;**
- **Provide more comments per each function for readability, especially contracts that are verified in public;**
- **Provide more transparency on privileged activities once the protocol is live.**



## Overview

PROJECT NAME	BOTiFi.Ai (BOTIFI)
ADDRESS	0xb1bf223d00a0c0086ee0ae6c8b1fcb1c2e4a479c
NETWORK	BSC
TOTAL SUPPLY	100,000,000 BOTIFI
COMPILER VER.	v0.8.17+commit.8df45f5f
LANGUAGE	Solidity



☒ Optimization With 200 Runs

## Wallets

OWNER	0xBc329F8352c3a3cB918Cd4dc3392C65C6Cf1Dd83
CREATOR	0xBc329F8352c3a3cB918Cd4dc3392C65C6Cf1Dd83

## Vulnerability Summary

SECURITY SCORING: 100 / 100



# Vulnerability Check

## Code Review

DESIGN LOGIC	PASSED
COMPILER WARNINGS	PASSED
PRIVATE USER DATA LEAKS	PASSED
TIMESTAMP DEPENDENCE	PASSED
INTEGER OVERFLOW AND UNDERFLOW	PASSED
RACE CONDITION REENTRANCY	PASSED
POSSIBLE DELAYS IN DATA DELIVERY	PASSED
ORACLE CALLS	PASSED
FRONT RUNNING	PASSED
DOS WITH BLOCK GAS LIMIT	PASSED
DOS WITH REVERT	PASSED
METHODS EXECUTION PERMISSIONS	PASSED
ECONOMY MODEL	PASSED
IMPACT OF THE EXCHANGE RATE	PASSED
MALICIOUS EVENT LOG	PASSED
SCOPING AND DECLARATIONS	PASSED
UNINITIALIZED STORAGE POINTERS	PASSED
ARITHMETIC ACCURACY	PASSED
CROSS FUNCTION RACE CONDITIONS	PASSED
SAFE ZEPPELIN MODULE	PASSED
FALLBACK FUNCTION SECURITY	PASSED



# Vulnerability Check

---

## Function Review

BUSINESS LOGICS REVIEW FUNCTIONALITY CHECKS	PASSED
ACCESS CONTROL & AUTHORIZATION	PASSED
ESCROW MANIPULATION	PASSED
TOKEN SUPPLY MANIPULATION	PASSED
ASSETS INTEGRITY	PASSED
USER BALANCES MANIPULATION	PASSED
DATA CONSISTENCY MANIPULATION	PASSED
KILL - SWITCH MECHANISM OPERATION TRAILS & EVENT GENERATION	PASSED



# Owner Privileges

---

```
function enableTax() public onlyOwner {
    require(!taxStatus, "CoinToken: Tax is already enabled");
    taxStatus = true;
}

function disableTax() public onlyOwner {
    require(taxStatus, "CoinToken: Tax is already disabled");
    taxStatus = false;
}

function setBuyTax(uint256 dev, uint256 marketing, uint256
liquidity, uint256 charity) public onlyOwner {
    buyTaxes["dev"] = dev;
    buyTaxes["marketing"] = marketing;
    buyTaxes["liquidity"] = liquidity;
    buyTaxes["charity"] = charity;
}

function setSellTax(uint256 dev, uint256 marketing, uint256
liquidity, uint256 charity) public onlyOwner {
    sellTaxes["dev"] = dev;
    sellTaxes["marketing"] = marketing;
    sellTaxes["liquidity"] = liquidity;
    sellTaxes["charity"] = charity;
}
```



## Owner Privileges

---

# CONCLUSION

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Owner can't mint tokens        | <input checked="" type="checkbox"/> Owner can't stop the contract |
| <input checked="" type="checkbox"/> Owner can't limit transactions | <input checked="" type="checkbox"/> Owner can't stop trading      |
| <input checked="" type="checkbox"/> Owner can't set fees <25%      | <input checked="" type="checkbox"/> Owner can't block wallets     |