

SMART CONTRACT SECURITY AUDIT WENPUMP



AUDITED ON SEPTEMBER 05, 2021

USING INTERFI AUDITING ARCHITECTURE

Summary

Audit:

Auditing Firm	InterFi Network
Architecture	InterFi Auditing Architecture
Smart Contract Audit Approved By	Chris Blockchain Specialist at InterFi
Project Overview Approved BY	Albert Project Specialist at InterFi
Platform	Solidity
Audit Check (Mandatory)	Vulnerability Check, Source Code Review, Functional Test
Project Check (Optional)	Website Review, Socials Review, Token Review (Not Applicable)
Consultation Request Date	September 03, 2021
Report Date	September 05, 2021

Risk profile:

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit, **WENPUMP's smart contract source code has Low Risk Severity.**

For the detailed understanding of risk severity, source code vulnerability, and functional test, kindly refer to the audit. **At the time of the audit, the contract is not deployed on any blockchain. Note, the owner/developer can change/modify contract before blockchain deployment. Please proceed with caution.**

Table Of Contents

Project Overview	4
Audit Scope & Methodology	6
InterFi's Risk Classification.....	8
Smart Contract Overview	9
Smart Contract Risk Assessment.....	13
Auditor's Verdict	15
Important Disclaimer	16
About InterFi Network.....	17

InterFi
Blockchain Security
.....
Confidential Audit

Project Overview

InterFi was consulted by WENPUMP on September 03, 2021 to conduct a smart contract security audit of their solidity source code.

Public information

WENPUMP is a yield-generating smart contract on the Binance Smart Chain that allows the holder to passively build a long-term portfolio of the 5 largest cryptocurrencies in the world: BTC, ETH, BNB, ADA and USDT.

Summary: Holders automatically build a long-term investment portfolio just by holding WENPUMP.

Information	WENPUMP
Blockchain	No deployment info at the time of audit
Language	Solidity
Contract	https://github.com/interfinetwork/smart-contract-audits/blob/main/WenPump.sol
Website	https://wenspump.io/
Twitter	https://twitter.com/wenspumpbsc
Telegram	https://t.me/wenspump_bsc

Public logo



Solidity Source Code & Extras

<https://github.com/interfinetwork/smart-contract-audits/blob/main/WenPump.sol>

<https://github.com/interfinetwork/smart-contract-audits/blob/main/WenPump%20Libraries.sol>

GitHub Commits

Solidity source code committed at: d80ebec6206197008eac81847d39294679be7422

Audit Scope & Methodology

The scope of this report is to audit the smart contract source code of WENPUMP. The source code can be viewed in its entirety on

<https://github.com/interfinetwork/smart-contract-audits/blob/main/WenPump.sol>

InterFi has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities

- ❖ Re-entrancy (RE)
- ❖ Unhandled Exceptions (UE)
- ❖ Transaction Order Dependency (TO)
- ❖ Integer Overflow (IO)
- ❖ Unrestricted Action (UA)

Source Code Review

- ❖ Ownership Takeover
- ❖ Gas Limit and Loops
- ❖ Deployment Consistency
- ❖ Repository Consistency
- ❖ Data Consistency
- ❖ Code Typo Error
- ❖ Token Supply Manipulation
- ❖ Access Control and Authorization
- ❖ Operations Trail and Event Generation

Functional Assessment

- ❖ Assets Manipulation
- ❖ Liquidity Access

ECHELON-1 Analysis

The aim of “InterFi’s ECHELON-1 Analysis” is to analyze the smart contract and identify the vulnerabilities and the hacks in the smart contract. Mentioned are the steps used by ECHELON-1 to assess the smart contract:

1. Code review that includes the following
 - ❖ Review of the specifications, sources, and instructions provided to InterFi to make sure we understand the size, scope, and functionality of the smart contract.
 - ❖ Manual review of code, which is the process of reading source code line-byline to identify potential vulnerabilities.
2. Testing and automated analysis that includes the following
 - ❖ Test coverage analysis, which is the process of determining whether the test cases are covering the code and how much code is exercised when we run those test cases.
 - ❖ Symbolic execution, which is analysing a program to determine what inputs causes each part of a program to execute.
3. Best practices review, which is a review of the smart contracts to improve efficiency, effectiveness, clarify, maintainability, security, and control based on the established industry and academic practices, recommendations, and research.
4. Specific, itemized, actionable recommendations to help you take steps to secure your smart contracts

Automated 3P frameworks used to assess the smart contract vulnerabilities

- ❖ Slither
- ❖ MythX
- ❖ Consensys Mythril
- ❖ Open Zeppelin
- ❖ Solidity Code Compiler

InterFi's Risk Classification

Smart contracts are generally designed to manipulate and hold funds denominated in Ether. This makes them very tempting attack targets, as a successful attack may allow the attacker to directly steal funds from the contract. Below are the typical risk levels of a smart contract:

Vulnerable: A contract is vulnerable if it has been flagged by a static analysis tool as such. As we will see later, this means that some contracts may be vulnerable because of a false-positive.

Exploitable: A contract is exploitable if it is vulnerable and the vulnerability could be exploited by an external attacker. For example, if the "vulnerability" flagged by a tool is in a function which requires to own the contract, it would be vulnerable but not exploitable.

Exploited: A contract is exploited if it received a transaction on the main network which triggered one of its vulnerabilities. Therefore, a contract can be vulnerable or even exploitable without having been exploited.

Risk severity	Meaning
! Critical	This level vulnerabilities could be exploited easily, and can lead to asset loss, data loss, asset manipulation, or data manipulation. They should be fixed right away.
! High	This level vulnerabilities are hard to exploit but very important to fix, they carry an elevated risk of smart contract manipulation, which can lead to critical risk severity
! Medium	This level vulnerabilities are should be fixed, as they carry an inherent risk of future exploits, and hacks which may or may not impact the smart contract execution.
! Low	This level vulnerabilities can be ignored. They are code style violations, and informational statements in the code. They may not affect the smart contract execution

Smart Contract Overview

Knick-knacks in the smart contract

Query	Result
_name	WenPump
_symbol	WPUMP
_decimals	9
InitialSupply	1,200,000,000
MarketingWallets	0xDaA7dd8f8dED51eeb26392907aF60896846300A4
	0xf430fd172a3d9738fdA5B5356addBa719164befc,
	0xIAAf19570DAAA82748097A2f77E3796D91F56ead,
	0x02f9DF96eaaFc9d3dE4faF14792b29fDB0505AF3,
	0xFIC6e2254351bd3A7E6599F011026E29344C0542
Maxtax	20
_buyTax	17
_sellTx	17
PayoutTokens Bitcoin	0x7130d2A12B9BCbFAe4f2634d864A1Ee1Ce3Ead9c
PayoutTokens Ethereum	0x2170Ed0880ac9A755fd29B2688956BD959F933F8
PayoutTokens ADA	0x3EE2200Efb3400fAbB9AacF31297cBdD1d435D47
PayoutTokens USDT	0x55d398326f99059fF775485246999027B3197955

Vulnerability**Status**

Compiler errors	! Low
Re-entrancy. Race conditions and cross function race conditions (RE)	Passed
Possible delays in data delivery	Passed
Gas optimization	! Low
Integer Underflow and overflow	Passed
Oracle Calls	Passed
Call stack depth attack	Passed
Parity Multisig Bug	Passed
Tx ordering dependency (TO)	Passed
DOS with revert and block gas limit	Passed
Private user data leaks	Passed
Malicious event log	Passed
Safe open zeppelin contract implementation and usage	Passed
The impact of exchange rate on the logic	Passed
Functions that are not used (dead-code)	! Low
Typographical Errors	Passed
Signature Malleability	Passed
Floating Pragma	! Low
Scoping and declarations	! Medium

Verifying token functions

Function	Description	Tested	Verdict
TotalSupply	provides information about the total token supply	Yes	Passed
BalanceOf	provides account balance of the owner's account	NA	NA
Transfer	executes transfers of a specified number of tokens to a specified address	Yes	Passed
TransferFrom	executes transfers of a specified number of tokens from a specified address	Yes	Passed
Approve	allow a spender to withdraw a set number of tokens from a specified account	Yes	Passed
Allowance	returns a set number of tokens from a spender to the owner	Yes	Passed

Verified

- ❖ Owner can mint tokens at token launch.
- ❖ Owner can not pause the contract.

Note

- ❖ At the time of the audit, the contract is not deployed on any blockchain. Note, the owner/developer can change/modify contract before blockchain deployment.
- ❖ Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.

Points To Note

The Wenpump.sol smart contract utilizes the “SafeMath” to prevent Integer Overflow.

```
Library SafeMath {
    ftrace | funcSig
    function add(uint256 a!, uint256 b!) internal pure returns (uint256) {
        uint256 c = a! + b!;
        require(c >= a!, "SafeMath: addition overflow");
        return c;
    }
}
```

The Wenpump.sol smart contract has a low severity issue which may not create any functional vulnerability.

```
{
  "resource": "/d:/staticanalysis/contracts/WenPump.sol",
  "owner": "_generated_diagnostic_collection_name_#0",
  "severity": 8,
  "message": "Expected identifier, got 'LParen'",
  "source": "solc",
  "startLineNumber": 105,
  "startColumn": 17,
  "endLineNumber": 105,
  "endColumn": 18
}
```

Smart Contract Risk Assessment

SWC Errors	Issue	Severity
Error	LParen	! Low

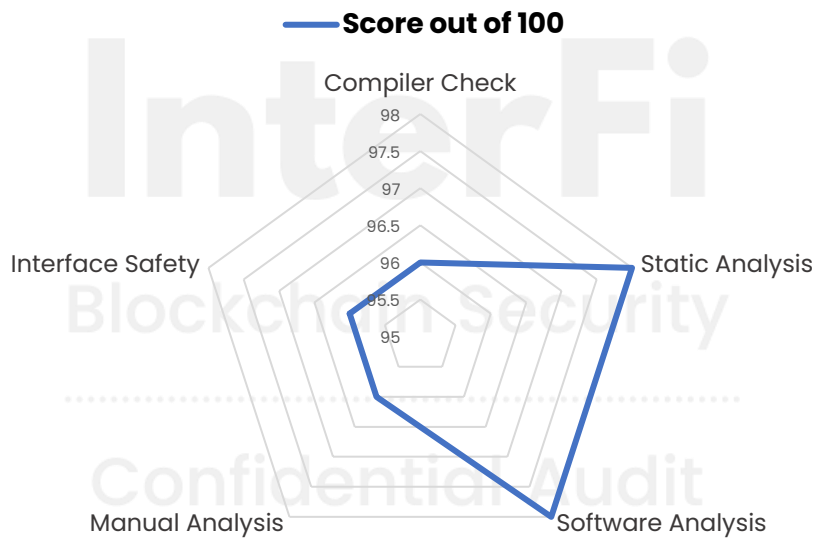
Expected identifier, got 'LParen'

Solution: Dynamic imports should be able to be used as bare expressions, or to be chained as promises without being assigned to an identifier.

InterFi
Blockchain Security
.....
Confidential Audit

Risk Severity Status

! Critical	None critical severity issues identified
! High	None high severity issues identified
! Medium	1 Medium severity issues identified
! Low	4 Low severity issues identified
Passed	19 functions and instances verified and passed



Compiler Check	96
Static Analysis	98
Software Analysis	98
Manual Analysis	96
Interface Safety	96

Auditor's Verdict

InterFi team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks.

WENPUMP's smart contract source code has LOW RISK SEVERITY.

WENPUMP has PASSED the InterFi's ECHELON-1 standard smart contract audit.



Auditor's Footnote:

- ❖ At the time of the audit, the contract is not deployed on any blockchain. Note, the owner/developer can change/modify contract before deployment. Please proceed with caution.
- ❖ Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security.
- ❖ Project's liquidity pair isn't checked and verified due to out of scope.
- ❖ Project website is not checked due to out of scope. The website hasn't been reviewed for SSL and lighthouse report.
- ❖ Project team KYC, and the project's social channels are not checked due to out of scope.

Important Disclaimer

InterFi Network provides contract auditing and project verification services for blockchain projects. The purpose of the audit is to analyse the on-chain smart contract source code, and to provide basic overview of the project. **This report should not be transmitted, disclosed, referred to, or relied upon by any person for any purposes without InterFi's prior written consent.**

InterFi provides the easy-to-understand assessment of the project, and the smart contract (otherwise known as the source code). The audit makes no statements or warranties on the security of the code. It also cannot be considered as an enough assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have used all the data at our disposal to provide the transparent analysis, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. **Be aware that smart contracts deployed on a blockchain aren't resistant from external vulnerability, or a hack. Be aware that active smart contract owner privileges constitute an elevated impact to smart contract's safety and security. Therefore, InterFi does not guarantee the explicit security of the audited smart contract.**

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report should not be considered as an endorsement or disapproval of any project or team.

The information provided on this report does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. Do conduct your own due diligence and consult your financial advisor before making any investment decisions.

About InterFi Network

InterFi Network provides intelligent blockchain solutions. InterFi is developing an ecosystem that is seamless and responsive. Some of our services: Blockchain Security, Token Launchpad, NFT Marketplace, etc. **InterFi's mission is to interconnect multiple services like Blockchain Security, DeFi, Gaming, and Marketplace under one ecosystem that is seamless, multi-chain compatible, scalable, secure, fast, responsive, and easy-to-use.**

InterFi is built by a decentralized team of UI experts, contributors, engineers, and enthusiasts from all over the world. Our team currently consists of 6+ core team members, and 10+ casual contributors. **InterFi provides manual, static, and automatic smart contract analysis, to ensure that project is checked against known attacks and potential vulnerabilities.**

For more information, visit <https://interfi.network>

To book an audit, message <https://t.me/interfiaudits>

InterFi
Blockchain Security
.....
Confidential Audit