# CONTRACT WOLF

*Security Assessment*

# What AI Dapp

Verified on 11/02/2024

## SUMMARY

| Project | CHAIN | METHODOLOGY |
|---|---|---|
| What AI Dapp | - | Manual & Automatic Analysis |

| FILES | DELIVERY | TYPE |
|---|---|---|
| Single | 11/02/2024 | Standard Audit |

| | 0 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|
| | Total Findings | Critical | Major | Medium | Minor | Informational |

🟥 **0 Critical** — An exposure that can affect the contract functions in several events that can risk and disrupt the contract

🟧 **0 Major** — An exposure that can affect the outcome when using the contract that can serve as an opening in manipulating the contract in an unwanted manner

🟧 **0 Medium** — An opening that could affect the outcome in executing the contract in a specific situation

⬜ **0 Minor** — An opening but doesn't have an impact on the functionality of the contract

🟦 **0 Informational** — An opening that consists information but will not risk or affect the contract

**STATUS** ✔️**AUDIT PASSED**

## TABLE OF CONTENTS | What AI

# DISCLAIMER | What AI

**ContractWolf** audits and reports should not be considered as a form of project's "Advertisement" and does not cover any interaction and assessment from "Project Contract" to "External Contracts" such as PancakeSwap, UniSwap, SushiSwap or similar.

**ContractWolf** does not provide any warranty on its released report and should not be used as a decision to invest into audited projects.

**ContractWolf** provides a transparent report to all its "Clients" and to its "Clients Participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

**ContractWolf**'s presence is to analyze, audit and assess the Client's Smart Contract to find any underlying risk and to eliminate any logic and flow errors within its code.

*Each company or project should be liable to its security flaws and functionalities.*

# SCOPE OF WORK | What AI

**What AI** team has agreed and provided us with the files that need to be tested (*Github, BSCscan, Etherscan, Local files etc*). The scope of audit is the main contract.

The goal of this engagement is to identify if there is a possibility of security flaws in the implementation of smart contract and its systems.

ContractWolf will be focusing on contract issues and functionalities along with the project claims from smart contract to their website, whitepaper, repository which has been provided by **What AI.**
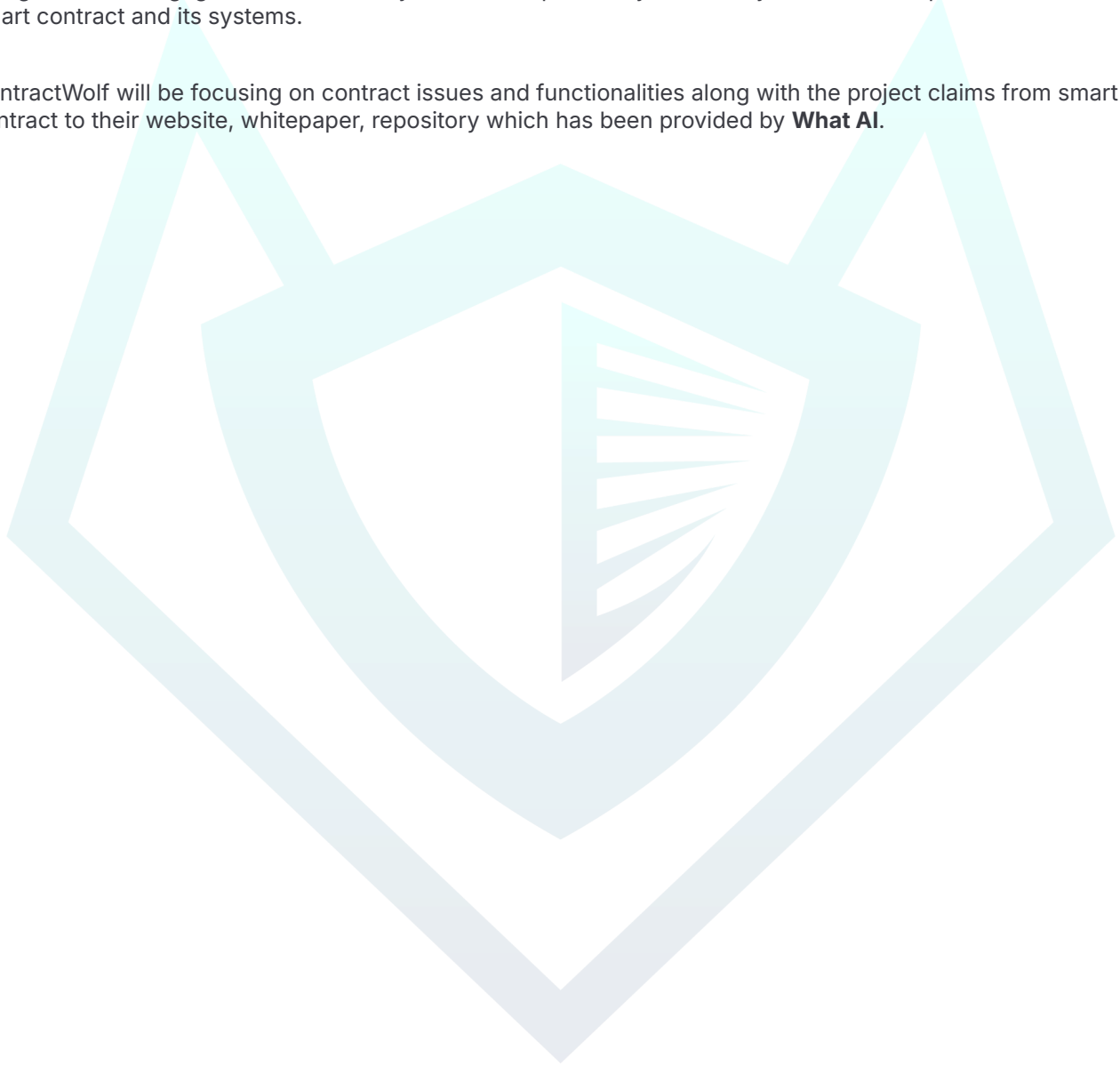
# AUDITING APPROACH | What AI

Every line of code along with its functionalities will undergo manual review to check for security issues, quality of logic and contract scope of inheritance. The manual review will be done by our team that will document any issues that they discovered.

### METHODOLOGY

The auditing process follows a routine series of steps :

1. Code review that includes the following :
   - Review of the specifications, sources and instructions provided to ContractWolf to make sure we understand the size, scope and functionality of the smart contract.
   - Manual review of code. Our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities, underlying and hidden security flaws.

2. Testing and automated analysis that includes :
   - Testing the smart contract function with common test cases and scenarios to ensure that it returns the expected results.

3. Best practices and ethical review. The team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security and control within the smart contract.

4. Recommendations to help the project take steps to eliminate or minimize threats and secure the smart contract.

# TOKEN DETAILS | What AI

First AI-Driven Trading & Sniping Bot on Whatsapp, Discord & Telegram.

## SOURCE

Source                    *Sent Via local-files*

# FINDINGS | What AI

| 0 | 0 | 0 | 0 | 0 | 0 |
|---|---|---|---|---|---|
| Total Findings | Critical | Major | Medium | Minor | Informational |

This report has been prepared to state the issues and vulnerabilities for What AI Dapp through this audit. The goal of this report findings is to identify specifically and fix any underlying issues and errors

| ID | Title | File & Line # | Severity | Status |
|----|-------|---------------|----------|--------|
| NO ISSUES FOUND | - | - | - | - |

# PENETRATION ATTACKS | What AI

Dapp Weakness Classification and Test Cases

| ID | Description | Status |
|---|---|---|
| DCW-001 | Malware Scan | ● Passed |
| DCW-002 | Phishing | ● Passed |
| DCW-003 | Missing HTTP Headers | ● Passed |
| DCW-004 | Valid SSL Certificate | ● Passed |
| DCW-005 | Firewalls(Drop & Deny) | ● Passed |
| DCW-006 | SQL Injection | ● Passed |
| DCW-007 | Framework Version | ● Passed |
| DCW-008 | Gas Limit | ● Passed |
| DCW-009 | Address Approval | ● Passed |
| DCW-010 | Address Draining | ● Passed |

**FIXES & RECOMMENDATION**

## NO ISSUES FOUND | SAFE TO INTERACT

This dapp from What AI has been audited by ContractWolf and has been marked safe to interact with. Please proceed with due diligence.

# AUDIT COMMENTS | What AI

Dapp audit comment for a non-technical perspective

- 🟢 What AI has been marked as SAFE to be interacted with by any EVM wallets *(11–02-2024)*
- 🟢 DAPP has no backdoors
- 🟢 DAPP cannot drain wallets via approval

# CONTRACTWOLF

Blockchain Security - Smart Contract Audits