OFFSIDE LABS

Mind Network AgenticWorld

Smart Contract Security Assessment

April 2025

Prepared for:

Mind Network

Prepared by:

Offside Labs

Yao Li

Tim Li

Contents

1 About Offside Labs

Offside Labs stands as a pre-eminent security research team, comprising highly skilled hackers with top - tier talent from both academia and industry.

The team demonstrates extensive and diverse expertise in modern software systems, which encompasses yet are not restricted to *browsers*, *operating systems*, *IoT devices*, and *hypervisors*. Offside Labs is at the forefront of innovative domains such as *cryptocurrencies* and *blockchain technologies*. The team achieved notable accomplishments including the successful execution of remote jailbreaks on devices like the **iPhone** and **PlayStation 4**, as well as the identification and resolution of critical vulnerabilities within the **Tron Network**.

Offside Labs actively involves in and keeps contributing to the security community. The team was the winner and co-organizer for the *DEFCON CTF*, the most renowned CTF competition in Web2. The team also triumphed in the **Paradigm CTF 2023** in Web3. Meanwhile, the team has been conducting responsible disclosure of numerous vulnerabilities to leading technology companies, including *Apple*, *Google*, and *Microsoft*, safeguarding digital assets with an estimated value exceeding **$300 million**.

During the transition to Web3, Offside Labs has attained remarkable success. The team has earned over **$9 million** in bug bounties, and **three** of its innovative techniques were acknowledged as being among the **top 10 blockchain hacking techniques of 2022** by the Web3 security community.

2 Executive Summary

Introduction

Offside Labs completed a security audit of *AgenticWorld* smart contracts, starting on April 3, 2025, and concluding on April 8, 2025.

Project Overview

AgenticWorld is a decentralized AI ecosystem designed to power secure and autonomous AI agents. Utilizing Fully Homomorphic Encryption (FHE), it enables encrypted computations, ensuring robust data privacy within multi-agent systems (MAS). With integrated security layers and interoperability hubs, AgenticWorld facilitates trustless AI collaboration, decentralized identity management, and confidential machine learning across Web3 and DeFi ecosystems. As part of the AgenticWorld ecosystem, this project empowers users to own AI agents and interact with interoperability hubs. Through these interactions and staking mechanisms, users can participate in reward distribution, fostering engagement and incentivizing collaboration in the decentralized network.

Audit Scope

The assessment scope contains mainly the smart contracts of the agentic-world program for the *AgenticWorld* project. The audit is based on the following specific branches and commit hashes of the codebase repositories:

- AgenticWorld
  - Codebase: `https://github.com/mind-network/mind-agent-contracts`
  - Commit Hash: c813e93e2c565176756f4d1abc158566bea36a40

We listed the files we have audited below:

- AgenticWorld
  - contracts/**/*.sol

Findings

The security audit revealed:

- 0 critical issue
- 0 high issue
- 1 medium issues
- 0 low issue
- 2 informational issues

Further details, including the nature of these issues and recommendations for their remediation, are detailed in the subsequent sections of this report.

3 Summary of Findings

ID	Title	Severity	Status
01	Lack of Non-Decreasing Property for Exchange Rate of Reward to Asset	Medium	Fixed
02	Inconsistent Constructor for Contracts with Initialize Function	Informational	Fixed
03	Unchecked Return Value for Functions of EnumerableSet	Informational	Fixed

4 Key Findings and Recommendations

4.1 Lack of Non-Decreasing Property for Exchange Rate of Reward to Asset

Severity: Medium	Status: Fixed
Target: Smart Contract	Category: Precision

Description

In the `MemberPool` contract, the exchange rate of reward to asset is calculated and reward debt is recorded for each user to maintain the accounting of reward distribution. However, the current implementation uses floor division when calculating the exchange rate in both the deposit and withdrawal processes. This approach fails to maintain the non-decreasing property of the exchange rate for reward to asset.

Impact

A decreasing exchange rate can lead to:

1. Reward shortages: User rewards may fall below their recorded reward debt, potentially causing a DoS (Denial of Service) attack.
2. Reward reduction: All users may receive fewer rewards than expected, leading to unfair distribution.

Proof of Concept

Below is an illustrative scenario:

1. Initial state:
   - `hubReward = 100`
   - `hubAsset = 99`
2. User A deposits 100 assets, and the exchange rate is calculated as:

   `100 * (101 / 100) = 101`

   New state:
   - `hubReward = 201`
   - `hubAsset = 199`
3. User B deposits 10 assets, and the exchange rate is calculated as:

   `10 * (202 / 200) = 10`

   New state:

- `hubReward = 211`
- `hubAsset = 209`

4. User A withdraws 100 assets, and the exchange rate is calculated as:

   `100 * (212 / 210) = 100`

   Due to rounding errors caused by floor division, rewards might decrease, violating the non-decreasing property.

Recommendation

Consider using ceiling division for deposit.

Mitigation Review Log

Fixed in commit abb561d55f8c2aee5397d43defbd75c84a776353.

4.2 Informational and Undetermined Issues

Inconsistent Constructor for Contracts with Initialize Function

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Logic Error

Out of six contracts implementing a proxy-style `initialize` function, only three include a constructor that calls the `_disableInitializers` function.

Unchecked Return Value for Functions of EnumerableSet

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Data Validation

In the Agent and Vesting contracts, the `EnumerableSet` library is utilized to track corresponding IDs for users. However, the functions provided by `EnumerableSet` return a boolean value to indicate whether the operation was successful, which is currently unchecked.

5 Disclaimer

This report reflects the security status of the project as of the date of the audit. It is intended solely for informational purposes and should not be used as investment advice. Despite carrying out a comprehensive review and analysis of the relevant smart contracts, it is important to note that Offside Labs' services do not encompass an exhaustive security assessment. The primary objective of the audit is to identify potential security vulnerabilities to the best of the team's ability; however, this audit does not guarantee that the project is entirely immune to future risks.

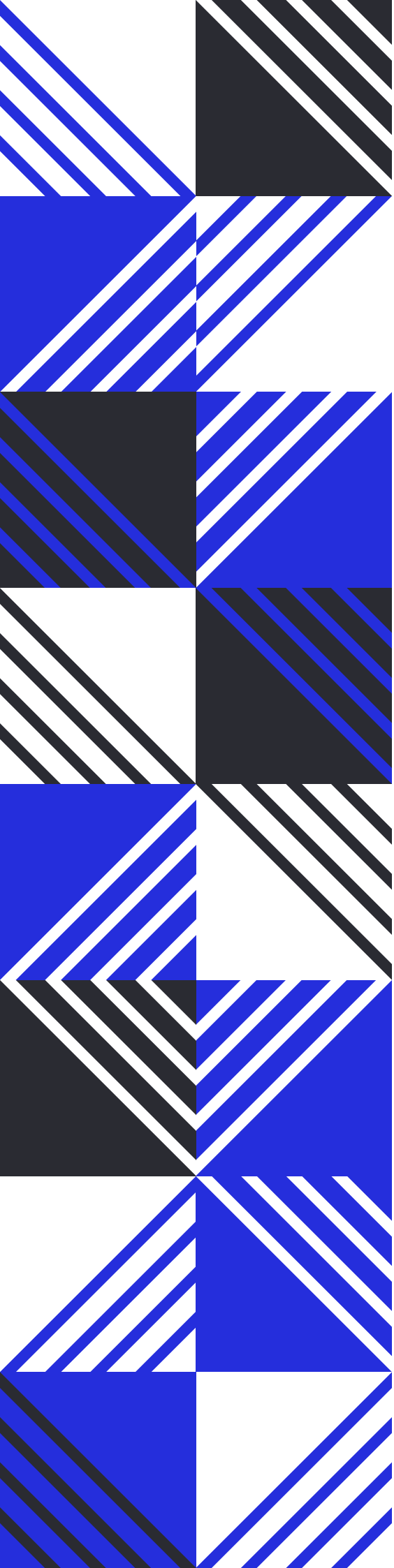
Offside Labs disclaims any liability for losses or damages resulting from the use of this report or from any future security breaches. The team strongly recommends that clients undertake multiple independent audits and implement a public bug bounty program to enhance the security of their smart contracts.

The audit is limited to the specific areas defined in Offside Labs' engagement and does not cover all potential risks or vulnerabilities. Security is an ongoing process, regular audits and monitoring are advised.

Please note: Offside Labs is not responsible for security issues stemming from developer errors or misconfigurations during contract deployment and does not assume liability for centralized governance risks within the project. The team is not accountable for any impact on the project's security or availability due to significant damage to the underlying blockchain infrastructure.

By utilizing this report, the client acknowledges the inherent limitations of the audit process and agrees that the firm shall not be held liable for any incidents that may occur after the completion of this audit.

This report should be considered null and void in case of any alteration.



OFFSIDE LABS

https://offside.io/

https://github.com/offsidelabs

https://twitter.com/offside_labs