OFFSIDE LABS

Meteora DAMM v2

Smart Contract Security Assessment

June 2025

Prepared for:

Meteora

Prepared by:

Offside Labs

Sirius Xie

Ronny Xing

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 *DAMM v2* smart contracts, starting on May 7th, 2025, and concluding on May 27th, 2025.

Project Overview

DAMM v2 is a next-generation AMM with enhanced flexibility and efficiency. It supports concentrated liquidity within a custom price range, allowing better capital use. It also expands token support to both SPL and Token 2022 standards.

Its fee structures are highly customizable, with options for fixed or dynamic fees. It also provides an anti-sniper fee scheduler that gradually reduces swap fees over time. LP fees in DAMM v2 are not auto-compounded and can be claimed independently, with flexible collection modes.

Liquidity can be locked permanently or with vesting, while still allowing fee claims. DAMM v2 also includes built-in farming, and pools can be scheduled to activate at a custom start time for planned launches.

Audit Scope

The assessment scope contains mainly the smart contracts of the cp-amm program for the *DAMM v2* project.

The audit is based on the following specific branches and commit hashes of the codebase repositories:

- DAMM v2
  - Codebase: `https://github.com/MeteoraAg/damm-v2`
  - Commit Hash: 6d8349071063d2e68ad7aff935dd9d42b3c53fc4

We listed the files we have audited below:

- DAMM v2
  - programs/cp-amm/src/**/*.rs

Findings

The security audit revealed:

- 0 critical issue
- 0 high issue
- 0 medium issue
- 0 low issue
- 3 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	Inconsisent Slippage Checks between Swap and remove_liquidity	Informational	Fixed
02	Improper add operation	Informational	Fixed
03	Dust Rewards Permanently Locked Due to Precision Loss	Informational	Acknowledged

4 Key Findings and Recommendations

4.1 Informational and Undetermined Issues

Inconsisent Slippage Checks between Swap and remove_liquidity

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

In the `swap` IX, the value compared against the input parameter `minimum_amount_out` is the `transfer_fee_excluded_amount_out` , which excludes the Token-2022 transfer fee.

In the `remove_liquidity` IX, the value compared against the input parameter `token_X_amount_threshold` includes the Token-2022 transfer fee, i.e., it uses the raw `token_X_amount` .

The inconsistent interpretation of thresholds between `swap` and `remove_liquidity` may cause confusion for users.

It is recommended to maintain a consistent design for the amounts used in slippage checks for both instructions: either always include the Token-2022 transfer fee, or always exclude it.

Improper add operation

Severity: Informational	Status: Fixed
Target: Smart Contract	Category: Code QA

In `Position.accumulate_total_claimed_rewards` , `wrapping_add` is used to accumulate new rewards into `RewardInfo.total_claimed_rewards` . In Rust, `wrapping_add` does not raise an error when an overflow occurs during the calculation. It is recommended to replace `wrapping_add` with `safe_add` .

Dust Rewards Permanently Locked Due to Precision Loss

Severity: Informational	Status: Acknowledged
Target: Smart Contract	Category: Precision

Senario 1:

In the Pool, users receive rewards for providing liquidity, which are distributed based on the amount of liquidity in their positions.

Each time a user claims rewards, the Pool updates the `UserRewardInfo.reward_per_token_checkpoint` in their Position. However, since the calculation of `reward_per_token_stored` in `Pool.update_rewards` uses integer division, there is an inherent precision loss.

As a result, the more frequently `UserRewardInfo.reward_per_token_checkpoint` is updated, the more this precision loss accumulates.

Frequent operations like `claim_reward` , `add_liquidity` , and `remove_liquidity` may lead to users receiving less rewards than expected.

Moreover, the unclaimed dust rewards due to these precision loss remain permanently in the `reward_vault` , as the program does not provide any IX to withdraw these leftover rewards.

Senario 2:

If the Pool still has rewards that haven't reached `reward_duration_end` , and the funder or admin invokes a new `fund_reward` IX, the program will merge the `carry_forward_ineligible_reward` and `leftover` amount from the previous, unfinished reward into the new reward and calculate a new `reward_rate` based on the combined amount.

However, due to precision loss in the calculation involving `reward_rate` and the remaining seconds, the computed `carry_forward_ineligible_reward` and `leftover` amount may end up slightly less than the actual leftover.

The portion of the leftover reward that was undercounted due to precision will become permanently locked in the `reward_vault` , with no IX to withdraw it.

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