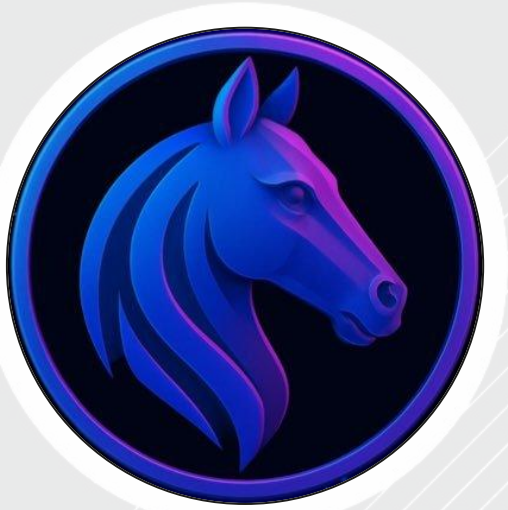
SPYWOLF

Security Audit Report



Audit prepared for

SuiDex

Completed on

Aug 5, 2025

OVERVIEW

This goal of this report is to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a a summarized review of the following key points:

- Contract's source code
- Owners' wallets
- Tokenomics
- Team transparency and goals
- Website's age, code, security and UX
- Whitepaper and roadmap
- Social media & online presence

The results of this audit are purely based on the team’s evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

TABLE OF CONTENTS

PROJECT INFORMATION

SuiDex is a decentralized exchange (DEX) and yield farming platform designed to offer rewards through token staking and liquidity provision.

Key Features

- **Yield Farming (SuiFarm):** The central feature of the platform, where users can stake both single assets and Liquidity Provider (LP) tokens into various pools to earn the native reward token, Victory.
- **Token Locking (Victory Token Locker):** A mechanism for users to lock their Victory tokens for various durations. In return, they receive a larger share of ongoing Victory emissions and a portion of the protocol's fee revenue, paid in SUI.
- **Dual Token System:** The ecosystem utilizes two primary tokens:
  - **Victory Token:** The primary reward token generated and distributed by the platform to incentivize user participation.
  - **$SUITRUMP Token:** A "mascot" token that is integrated into the farm's fee structure. A portion of farm fees is used to buy and burn $SUITRUMP, creating a deflationary mechanism.
- **Decentralized Exchange (DEX):** The platform includes a built-in Automated Market Maker (AMM) that allows users to swap between various tokens on the Sui network.

Tokenomics & Emission Model

- **Emission Schedule:** The Victory token is distributed on a 156-week (3-year) emission schedule. This begins with a 4-week "bootstrap" phase with high rewards, followed by a consistent 1% weekly decay in the rate of emissions.
- **Farm Fee Distribution:** Deposit and withdrawal fees from the SuiFarm are split three ways: 40% is used to buy and burn the $SUITRUMP token, 40% is distributed to users who have locked their Victory tokens, and 20% is sent to the project's treasury.

Technical Details

- **Smart Contract Language:** The protocol is built using the Move language (2024.beta edition).
- **Framework Dependency:** The contracts are developed and built against a testnet revision of the official Sui framework, as specified in the project's configuration files.
- **Administrative Controls:** The protocol's critical functions—such as creating new farming pools, setting reward allocations, and managing fees—are controlled by on-chain AdminCap objects, which are managed by the development team.

SCOPE OF AUDIT

This security audit was conducted by the SpyWolf Team between August 1 and August 4, 2025, at the request of the SuiDex project team.

The primary focus of this audit was the **SuiDex Yield Farm and Token Locker** smart contracts and their associated ecosystem. The analysis covered the following core components:

- suifarm.move
- token_locker.move
- global_emission_controller.move
- victorytoken.move

The scope also included a thorough review of all dependent utility contracts (such as fixed_point_math.move), deployment scripts, and provided documentation to ensure a holistic understanding of the system's functionality and on-chain configuration.

During the analysis, it was determined that the security of the core Decentralized Exchange (DEX) contracts is inextricably linked to the function and value of the LP tokens staked in the suifarm.move contract. A critical vulnerability in the DEX's pair.move contract has a direct and severe financial impact on users of the farm. Consequently, **critical vulnerabilities discovered in the core DEX contracts are included within the scope of this report.**

The audit was limited to the provided smart contract code and documentation. Off-chain components, front-end security, and the underlying security of the Sui blockchain itself were considered out of scope.

AUDIT METHODOLOGY

The security audit of the SuiDex Yield Farm and Token Locker smart contracts was conducted using a holistic and multi-layered approach to ensure comprehensive coverage. The methodology involved the following key processes:

- **Static Code Analysis:** A manual, line-by-line review of **all Move source code relevant to the farm and locker ecosystem** was performed. This included the primary business logic contracts (suifarm.move, token_locker.move, global_emission_controller.move), the victorytoken.move implementation, and all underlying dependencies such as the fixed_point_math.move library. The analysis focused on identifying logical errors, potential race conditions, incorrect access control, and arithmetic vulnerabilities.
- **Economic Model & Logic Review:** The smart contracts' implementation was systematically compared against the logic and economic principles described in the SuiDex Whitepaper.pdf, README.md, and tokenomics.csv. This was done to detect any discrepancies that could be exploited or lead to unintended economic behavior.
- **Independent Adversarial Testing:** We developed and executed a custom suite of independent test cases written in Move. This process involved:
  - **Developing Custom Scenarios:** Writing new test modules that specifically targeted the high-risk areas identified during static analysis.
  - **Simulating Economic Exploits:** Creating tests that actively simulated malicious user behavior, such as flash loan-assisted reward farming against the suifarm.move contract.
  - **Proof-of-Concept Validation:** Independently reproducing the exploit detailed in the poc.move file within our own test environment to confirm its viability and impact.
  - **Fuzzing and Edge Case Analysis:** Testing the system's behavior under extreme or unexpected conditions not covered in the provided test suite.
- **Test Coverage Assessment:** The provided test files (farm_tests.move, token_locker_tests.move, etc.) were reviewed to evaluate the depth and breadth of the project's existing testing strategy.
- **Deployment Script Analysis:** The complete_dex_setup.sh and related scripts were analyzed to understand the initialization process, default parameters, and the handling of administrative privileges for the farm and locker contracts.

FILES REVIEWED

Core Farm & Locker Contracts

- **suifarm.move**: The primary yield farming contract that manages staking pools and calculates user rewards.
- **token_locker.move**: Enables users to lock Victory tokens to earn a share of protocol fees and enhanced rewards.
- **global_emission_controller.move**: Governs the 156-week master schedule for releasing Victory token rewards.
- **victorytoken.move**: Defines the Victory token, the native reward asset of the platform.

Library & Dependency Contracts

- **fixed_point_math.move**: A utility contract providing a library for high-precision mathematical operations to prevent rounding errors.
- **library.move**: Contains helper functions, primarily for the DEX, but its utilities could be leveraged by other ecosystem contracts.

Deployment & Configuration Scripts

- **complete_dex_setup.sh**: The main deployment script for the initial on-chain setup and configuration of the farm, locker, and reward vaults.
- **create_single_pool.sh**: A script used to create individual single-asset staking pools on the farm after initial deployment.
- **create_wallet_pools.sh**: A script used to create LP token staking pools on the farm. Note: The filename suggests "wallet" but the content specifies "LP_PAIRS", indicating it's for LP pools.

Testing & Proof-of-Concept Files

- **farm_tests.move** / **token_locker_tests.move**: The unit and integration tests for the farm and locker contracts, used to verify their intended functionality.
- **poc.move**: A specific proof-of-concept file that demonstrates a known exploit, used to validate the vulnerability and test potential fixes.
- **test_coins.move**: Defines mock (fake) tokens used only within the test environment to simulate real assets like WBTC and ETH.

Documentation & Specifications

- **SuiDex Whitepaper.pdf** / **README.md**: The primary documentation outlining the project's architecture, features, and economic model.
- **tokenomics.csv**: A data file specifying the weekly emission rates and allocation percentages for the entire 156-week reward schedule.
- **SUBMISSIONS.md**: A document outlining the guidelines for bug reports, which also provides insight into the team's known areas of concern.

FOUND THREATS

Medium Risk

FARM-ME-02: Precision Loss via Integer Division Leading to Locked "Dust" Rewards

Component(s): suifarm.move, token_locker.move

Description: The formulas used to calculate rewards-per-share involve integer division, which truncates any remainder. In every calculation, a tiny fraction of a Victory token is lost due to this rounding down. These small, lost "dust" amounts are not credited to any user and will accumulate inside the contract over time. There is no mechanism to withdraw these accumulated funds.

Vulnerable Code Snippet (suifarm.move): The division by pool.total_staked is an integer division. If the remainder is non-zero, it is discarded, and that value becomes trapped in the contract.

```
// From suifarm.move's update_pool function
pool.acc_victory_per_share = pool.acc_victory_per_share + (victory_reward * 1_000_000_000_000) / pool.total_staked;
```

Attack Scenario:

1. Over several months, thousands of staking, unstaking, and reward-claiming transactions occur on the farm.
2. In each reward calculation, the formula rounds down, leaving a tiny fraction of a Victory token behind.
3. These fractions accumulate inside the suifarm contract. After a long period, this "dust" could add up to a significant number of tokens that are permanently locked and inaccessible to the team or users.

FOUND THREATS

Low Risk

FARM-LO-01: Risk of Fund Loss from Hardcoded Addresses in Deployment Script

Component(s): complete_dex_setup.sh

Description: The main deployment script, complete_dex_setup.sh, uses hardcoded addresses for critical fee distribution destinations, including the LOCKER_ADDRESS, TEAM_ADDRESS, DEV_ADDRESS, and BURN_ADDRESS. While these need to be defined for deployment, the practice of hardcoding them in a script makes the process susceptible to human error, such as a typo during a copy-paste operation or a modification.

Impact: An incorrect address in the deployment script would cause a portion of the farm's fee revenue to be permanently and irrevocably sent to an unintended destination. This would result in a direct financial loss for the intended recipients (e.g., Victory lockers or the treasury) and could impair certain protocol functions like the buy-and-burn mechanism.

FOUND THREATS

Informational

FARM-IN-01: Lack of Event Emission for Critical Admin Actions

Description: The smart contracts, particularly suifarm.move, lack on-chain events for significant administrative actions such as creating new farming pools. This reduces transparency and makes it more difficult for users, off-chain monitoring tools, and analytics platforms to track important changes to the protocol's configuration in real-time. It is recommended to implement and emit dedicated events for all critical state changes.

FARM-IN-02: Inconsistent Farm Fee Documentation

Description: There is a minor inconsistency between the implemented default fees in the deployment scripts and the user-facing documentation. The complete_dex_setup.sh script sets default fees for single-asset pools at 0.5%, whereas the README.md only states that fees are configurable without mentioning a default value. To improve clarity and transparency, it is recommended to unify all documentation to reflect the on-chain default configurations.

Dual Token Model with Deflationary Mechanism

Description: The ecosystem utilizes a two-token model: the Victory token as the primary yield-farming reward and the $SUITRUMP token as the platform's mascot. A key feature of the farm's design is that 40% of all deposit and withdrawal fees are used to systematically buy and burn $SUITRUMP tokens. This mechanism creates deflationary pressure on $SUITRUMP and directly links its value proposition to the overall transaction volume on the farm.

CONCLUSION

This security audit of the SuiDex Yield Farm and Token Locker has been completed. The process was collaborative, and we acknowledge the team's proactive approach to security, including the swift remediation of a critical vulnerability that was identified during the review.

We also acknowledge the team's trusted reputation and that operational security improvements regarding administrative controls have been noted. The remaining findings in this report are of Medium and Low severity, focusing on enhancing the protocol's long-term robustness and operational security.

While the most critical threats have been addressed, we recommend the team review and remediate these remaining medium and low-risk items to further harden the platform and ensure the highest standard of security and transparency for its users before launch.

SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- **OVER 700 SUCCESSFUL CLIENTS**
- **MORE THAN 1000 SCAMS EXPOSED**
- **MILLIONS SAVED IN POTENTIAL FRAUD**
- **PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS**
- **CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH**

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.
While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:
By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.
No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.
The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.
No applications were reviewed for security. No product code has been reviewed.