SPYWOLF

Security Audit Report

Audit prepared for

SuiRewards.Me

Completed on

April 27, 2025

SPYWOLF.CO

@SPYWOLFNETWORK

@SPYWOLFNETWORK

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

SuiRewards.Me

PROJECT DESCRIPTION

SuiRewards.me is the world's first rewards-based decentralized exchange (DEX) built on the SUI blockchain using the Move programming language. It operates as an automated market maker (AMM) with a unique rewards system, allowing users to swap tokens, provide liquidity, and earn fees while incentivizing creators and liquidity providers through a multi-tiered fee structure. This report evaluates the security of its smart contracts, focusing on potential vulnerabilities and operational considerations.

Release Date: TBD

Category: DEX

AUDIT METHODOLOGY

To provide a transparent and credible evaluation of the SuiRewards.me DEX, we employed a rigorous audit methodology using industry-standard tools and processes. The **Move CLI** was utilized to compile and test the smart contracts, ensuring seamless compatibility with the SUI blockchain environment. We leveraged the **SUI Testnet** to deploy and interact with the contracts in a controlled setting, simulating real-world conditions to validate their performance across diverse scenarios. A detailed **manual code review** was conducted to uncover potential vulnerabilities, logic errors, and ensure adherence to best practices. This was paired with **simulated tests**, incorporating edge cases, maximum input overflows, and unauthorized access attempts, to rigorously assess the contracts' resilience. Together, these tools and processes delivered a thorough and dependable analysis of the platform's security, offering the client clear insights into its robustness.

SUIREWARDS.ME FEATURES

This report provides a security audit of the decentralized exchange (DEX) implemented in the Move programming language for the SUI blockchain, specifically for SuiRewards.me. The audit is based on the provided code files: `sui_rewards_me.move`, `quote.move`, `Move.toml`, and `Move.lock`.

- **Comprehensive DEX Functionality:** The code implements a full-featured automated market maker (AMM) with:
  - Pool creation (`create_pool, create_pool_and_lock_lp`).
  - Liquidity provision (`add_liquidity, remove_liquidity`).
  - Token swapping (`swap_a_for_b, swap_b_for_a`).
  - Fee management (swap fees, burn fees, creator royalties, rewards fees, LP builder fees).
  - Event emissions for transparency (`PoolCreated`, `Swapped`, etc.).
  - Coin-based wrappers for user convenience.
- **Advanced Fee Structure:** The DEX supports multiple fee types (LP builder, burn, creator royalty, rewards, and swap fees), each with configurable maximums (e.g., 3%, 5%, 1%, 5%, 1%) and distribution thresholds (e.g., 0.1 SUI). Fee calculations involve precise mathematical operations to prevent precision loss.
- **Access Control:** The code includes a `Config` struct for managing admin privileges and a `CreatePoolLock` struct with an allowlist to restrict pool creation, adding layers of administrative logic.
- **Math Operations:** Custom math helper functions (`muldiv, ceil_muldiv, mulsqrt, ceil_div_u128`) handle multiplication, division, and square root operations with rounding to ensure accuracy and prevent overflows in a 64-bit and 128-bit integer environment.
- **Quote Calculations:** The `quote.move` module provides functions (`get_swap_quote_by_sell, get_swap_quote_by_buy`) for estimating swap outputs and required inputs, mirroring the main swap logic for consistency.
- **Event-Driven Transparency:** Extensive use of events ensures all significant actions (e.g., swaps, fee distributions) are logged, enhancing auditability.

CORE DEX CONTRACT

INFORMATION

- **File:**
  - **sui_rewards_me.move**
- **Purpose:**
  - Primary contract for the SuiRewards.me DEX, implementing the core functionality for pool creation, liquidity management, token swapping, fee handling, and access controls.
- **Logic:**
  - **Pool Creation:** Enables users to create liquidity pools with customizable fees (e.g., LP builder, burn, creator royalty, rewards).
  - **Liquidity Management:** Includes functions to add/remove liquidity, minting and burning LP tokens.
  - **Swapping:** Executes constant product AMM swaps with multi-tiered fees.
  - **Fee Handling:** Distributes fees to specific balances (e.g., swap, burn, creator, rewards) and triggers payouts when thresholds are met.
  - **Access Controls:** Manages admin privileges for updating fees, wallets, and settings.
  - **Events:** Emits events (e.g., `PoolCreated`, `Swapped`, `RewardsProcessing`) for transparency.

Tests Performed:

- Edge Case: Zero/Near-Zero Balances, Maximum Input Overflow, Front-Running Simulation, Fee Distribution Threshold, Unauthorized Access.

- **Tools Used**
  - **Move CLI:** For compiling and running unit tests.
  - **SUI Testnet:** For deploying and interacting with the contracts.
  - **Custom Scripts:** Written in Move to simulate edge cases.

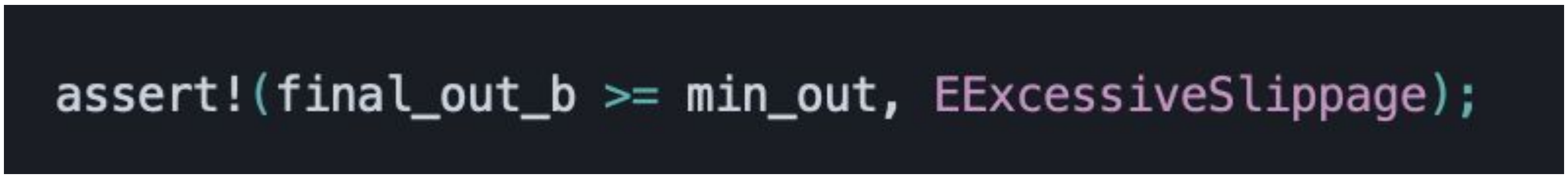
CORE DEX CONTRACT

FOUND THREATS

⚠ Medium Risk

Front-Running Susceptibility

Description: Large trades can be front-run, causing slippage losses. The min_out parameter mitigates this but relies on user settings.



```
assert!(final_out_b >= min_out, EExcessiveSlippage);
```

- Recommendation:
  - Introduce slippage tolerance settings in the UI and educate users on setting appropriate min_out values.

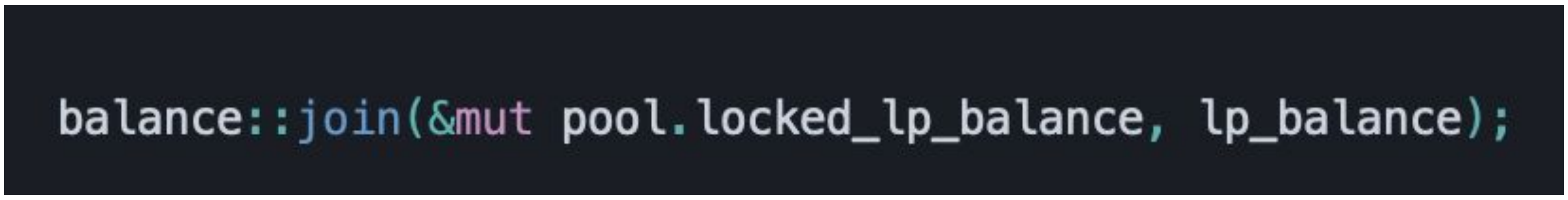
CORE DEX CONTRACT

FOUND THREATS

⚠️ Low Risk

Locked LP Tokens with No Withdrawal

Description: LP tokens locked via `create_pool_and_lock_lp` are permanently locked.
Impact: Users may misunderstand the permanent nature of locked LP tokens.



```
balance::join(&mut pool.locked_lp_balance, lp_balance);
```

- Recommendation:
  - Add clear documentation and user prompts explaining that locked LP tokens are irretrievable.

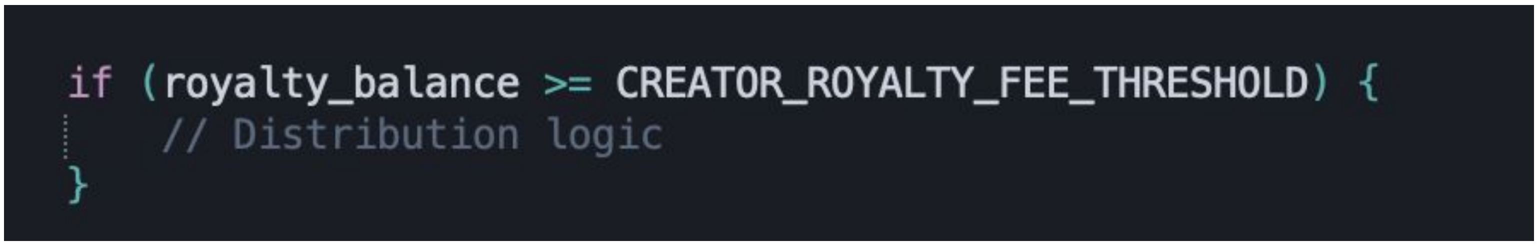
CORE DEX CONTRACT

FOUND THREATS

⚠ Low Risk

Fee Distribution Delays

Description: Fees are distributed only when balances exceed thresholds (e.g., 0.1 SUI), potentially delaying payouts.
Impact: Minor user inconvenience; no security threat.



```
if (royalty_balance >= CREATOR_ROYALTY_FEE_THRESHOLD) {
    // Distribution logic
}
```

- Recommendation:
  - ○ Implement a manual trigger for fee distribution or dynamically adjust thresholds to balance gas efficiency and timely payouts.

CORE DEX CONTRACT

FOUND THREATS

⚠ Low Risk

Immutable Fee Structure

Description: Fees are set during pool creation and cannot be adjusted later.
Impact: Limits flexibility but not a direct vulnerability.

- Recommendation:
  - Consider adding a governance mechanism (e.g., DAO voting) to allow fee adjustments post-deployment.

SWAP QUOTE HELPER CONTRACT

INFORMATION

- **File:**
  - **quote.move**
- **Purpose:**
  - This contract provides helper functions to calculate swap quotes, enabling users to estimate swap outcomes before execution.
- **Logic:**
  - **Swap Quote Calculations:** Includes `get_swap_quote_by_sell` and `get_swap_quote_by_buy` to compute expected outputs or required inputs.
  - **Fee Considerations:** Incorporates fees (e.g., swap, LP builder, burn) into quote calculations for accuracy.
  - **Non-State Modifying:** Functions are read-only and do not alter blockchain state.

Tests Performed:

- Quote Calculation for Sell, Quote Calculation for Buy, Zero Input Quote

- **Tools Used**
  - **Move CLI:** For compiling and running unit tests.
  - **Custom Scripts:** Written in Move to simulate quote calculations.

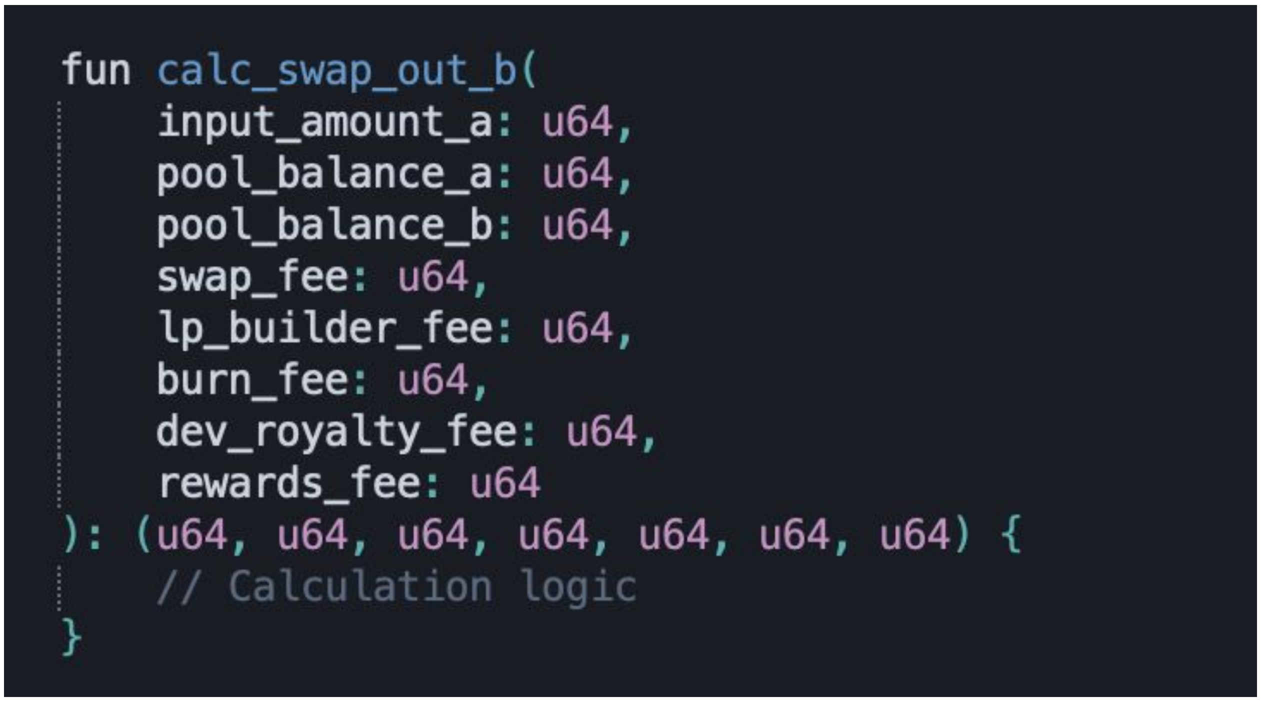
SWAP QUOTE HELPER CONTRACT

FOUND THREATS

⚠ Low Risk

Inconsistent Quote Calculations

Description: If quote logic diverges from swap logic, users could receive inaccurate estimates.
Impact: User confusion or dissatisfaction; no direct financial loss.



```
fun calc_swap_out_b(
    input_amount_a: u64,
    pool_balance_a: u64,
    pool_balance_b: u64,
    swap_fee: u64,
    lp_builder_fee: u64,
    burn_fee: u64,
    dev_royalty_fee: u64,
    rewards_fee: u64
): (u64, u64, u64, u64, u64, u64, u64) {
    // Calculation logic
}
```

- Recommendation:
  - Ensure quote calculations precisely mirror swap logic and test for consistency.

PROJECT CONFIGURATION FILE

INFORMATION

- **File:**
  - **Move.toml**
- **Purpose:**
  - Move.toml serves as the configuration file for a Move project. It defines essential metadata, dependencies, and named addresses used within the project.
- **Details:**
  - **Package Metadata:** Includes details such as the project name, edition, license, and authors, providing a clear identity for the project.
  - **Dependencies:** Lists external packages required by the project, such as the Sui framework, along with their sources (e.g., Git repositories) and specific revisions or versions.
  - **Addresses:** Specifies named addresses (e.g., sui_rewards_me = "0x0") that are referenced in the Move code, ensuring consistent address mapping.

- **Key Notes**
  - This file contains no executable logic; its role is limited to project setup and dependency management.
  - By specifying dependency versions, it helps ensure compatibility and reduces the risk of issues arising from outdated or incompatible packages.

DEPENDENCY LOCK FILE

INFORMATION

- **File:**
  - **Move.lock**
- **Purpose:**
  - Move.lock is an automatically generated file that locks the exact versions of dependencies used in the project, ensuring consistent and reproducible builds across different environments.
- **Details:**
  - **Dependency Pinning:** Records precise revisions and digests of the dependencies listed in Move.toml, guaranteeing that the same versions are used every time.
  - **Toolchain Info:** Includes details about the Move toolchain version and flavor, further ensuring build consistency.

- **Key Notes**
  - Like Move.toml, it contains no executable logic; its purpose is to enhance reproducibility and security.
  - By pinning dependency versions, it mitigates risks such as supply chain attacks, where unverified or malicious updates to dependencies could compromise the project.

CONCLUSION

The security audit of **SuiRewards.me DEX**, conducted on the SUI blockchain, reveals a technically robust decentralized exchange with **no critical vulnerabilities** identified in its smart contracts. Leveraging the inherent safety features of the **Move programming language**, the platform effectively mitigates common DeFi vulnerabilities such as reentrancy attacks and overflow errors, ensuring a secure foundation for its operations. This positions SuiRewards.me as a reliable contender in the decentralized finance (DeFi) space.

Key Findings

- **Smart Contract Security:** The audit confirms the absence of high-severity issues, underscoring the platform's resilience against exploits that have historically plagued other DeFi projects.
- **Minor Operational Risks:** While the platform is secure, minor concerns such as fee distribution delays and potential front-running were noted. These do not compromise the system's integrity but warrant proactive management to maintain user trust and operational efficiency.
- **Innovative Design:** As the first rewards-based DEX on SUI, SuiRewards.me introduces a unique fee structure that incentivizes participation and a permanent liquidity mechanism that enhances stability—key differentiators in a crowded market.

Strategic Advantages

SuiRewards.me stands out due to its pioneering approach on the SUI blockchain. The combination of a rewards-driven model and permanent liquidity not only attracts users but also fosters long-term ecosystem growth. This innovation offers investors an opportunity to back a project with significant scalability potential as the SUI ecosystem matures.

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.