SushiMaker Smart Contract Audit Report

This report summarizes the findings of a security audit conducted on the SushiMaker smart contract usin

1. Front-Running Vulnerability

- **Severity**: Medium
- **Description**: The `convert` function is vulnerable to front-running attacks. An attacker could place a t
- **Impact**: Users could receive less value for their tokens than expected if the attacker successfully ma
- **Mitigation**:
  - Implement a commit-reveal pattern to prevent front-running.
  - Utilize an off-chain matching engine for order matching.

2. Potential Reentrancy Attack (LLaMA)

- **Severity**: Medium
- **Description**: While the `SafeERC20` library is used to mitigate reentrancy risks, the contract's relianc
- **Impact**: An attacker could potentially execute a reentrancy attack, leading to the loss of funds or mar
- **Mitigation**:
  - Implement a reentrancy guard like the `ReentrancyGuard` library.
  - Develop custom reentrancy protection mechanisms within the contract.

3. Potential Overflow Attack (LLaMA)

- **Severity**: Low-Medium
- **Description**: Although the contract utilizes `SafeMath` to prevent arithmetic overflows, complex calcu
- **Impact**: An attacker could exploit overflows to manipulate the contract's logic or potentially drain func
- **Mitigation**:
  - Thoroughly review and audit all calculations involving multiple external calls for potential overflow vul
  - Employ additional safeguards and validation checks to prevent overflows.

Overall Assessment

While the SushiMaker contract appears well-structured and uses libraries like `SafeERC20` and `SafeMa

Recommendations

- Prioritize implementing the recommended mitigations for the front-running vulnerability.
- Conduct a thorough review of the contract's logic, especially calculations involving external calls, to add
- Consider implementing additional security measures like logging, monitoring, and custom reentrancy pr

Disclaimer

This report represents the findings of a security audit and should be considered as a starting point for sec