Audit

git : https://github.com/GODMuang/DEX_solidity/blob/main/src/Dex.sol

commit : `d99cfb5e97a8e3b70c1a984fb875d681677e8a51`

ID	요약	위험도
MUANG-001	`transferFrom` 함수에서 다른 사용자의 LP 토큰을 소유자가 아닌 사람이 소각할 수 있습니다.	Critical

Description

`Dex` 컨트랙트에서 `transferFrom` 함수는 `to == address(this)` 조건만 확인하고 있어서 다른 사용자의 LP 토큰을 소유자가 아닌 사람이 소각할 수 있습니다.

Impact

Critical

공격자가 `Dex` 컨트랙트 유동성 공급자 주소를 알고 있다면 해당 공급자의 모든 LP 토큰을 제거할 수 있습니다.

Recommendation

- `transferFrom` 함수의 `from` 주소가 `msg.sender` 일 때만 호출 가능하도록 하는 조건을 추가

ID	요약	위험도
MUANG-002	`mint` 함수를 누구나 호출이 가능합니다.	Critical

Description

`mint`함수가 `public` 으로 선언 되어있어 **실시간 토큰 잔액과 기존 토큰 잔액이 차이**가 있다면 `addLiquidity` 함수를 호출하지 않아도 LP 토큰을 발행할 수 있습니다.

Impact

Critical

공격자가 유동성 공급을하지 않아도 LP 토큰을 발급받을 수 있습니다.

Recommendation

- `mint` 함수를 `internal` 로 수정