Coinsult

Sherex: Decentralized Exchange (DEX) Code Audit

February 9th, 2025

https://t.me/coinsult_tg

info@coinsult_tg

Table of contents

Audit results

Code:
https://github.com/venus0311/sherex-platforom/tree/28a6fdb20e784c531444ba6c29aa89742bfe852a

masterchef-v3

sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IFarmBooster.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/ILMPool.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/ILMPoolDeployer.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IMasterChefV2.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IMasterChefV3.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/INonfungiblePositionManager.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/INonfungiblePositionManagerStruct.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IPancakeV3Pool.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IReceiver.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/interfaces/IWETH.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/keeper/MasterChefV3KeeperV1.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/keeper/MasterChefV3KeeperV2.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/libraries/SafeCast.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/receiver/MasterChefV3Receiver.sol ✅
sherex-v3-contracts/projects/masterchef-v3/contracts/receiver/MasterChefV3ReceiverV2.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/utils/Multicall.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/Enumerable.sol ✅

sherex-v3-contracts/projects/masterchef-v3/contracts/MasterChefV3.sol ✅

router

sherex-v3-contracts/projects/router/contracts/base/ApproveAndCall.sol ✅
sherex-v3-contracts/projects/router/contracts/base/ImmutableState.sol ✅
sherex-v3-contracts/projects/router/contracts/base/MulticallExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/base/OracleSlippage.sol ✅
sherex-v3-contracts/projects/router/contracts/base/PeripheryPaymentsExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/base/PeripheryPaymentsWithFeeExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/base/PeripheryValidationExtended.sol ✅

sherex-v3-contracts/projects/router/contracts/interfaces/IApproveAndCall.sol ✅

sherex-v3-contracts/projects/router/contracts/interfaces/IImmutableState.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IMixedRouteQuoterV1.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IMulticallExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IOracleSlippage.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IPeripheryPaymentsExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IPeripheryPaymentsWithFeeExtended.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IQuoter.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IQuoterV2.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/ISmartRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IStableSwap.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IStableSwapFactory.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IStableSwapInfo.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IStableSwapRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/ITokenValidator.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IV2SwapRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IV3SwapRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/interfaces/IWETH.sol ✅

sherex-v3-contracts/projects/router/contracts/lens/MixedRouteQuoterV1.sol ✅
sherex-v3-contracts/projects/router/contracts/lens/Quoter.sol ✅
sherex-v3-contracts/projects/router/contracts/lens/QuoterV2.sol ✅
sherex-v3-contracts/projects/router/contracts/lens/TokenValidator.sol ✅

sherex-v3-contracts/projects/router/contracts/libraries/Constants.sol ✅
sherex-v3-contracts/projects/router/contracts/libraries/PoolTicksCounter.sol ✅
sherex-v3-contracts/projects/router/contracts/libraries/SmartRouterHelper.sol ✅

sherex-v3-contracts/projects/router/contracts/SmartRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/StableSwapRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/V2SwapRouter.sol ✅
sherex-v3-contracts/projects/router/contracts/V3SwapRouter.sol ✅

v3-core

sherex-v3-contracts/projects/v3-core/contracts/interfaces/callback/IPancakeV3FlashCallback.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/callback/IPancakeV3MintCallback.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/callback/IPancakeV3SwapCallback.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolActions.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolDerivedState.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolEvents.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolImmutables.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolOwnerActions.sol ✅
sherex-v3-contracts/projects/v3-core/contracts/interfaces/pool/IPancakeV3PoolState.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/interfaces/IERC20Minimal.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/interfaces/IPancakeV3Factory.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/interfaces/IPancakeV3Pool.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/interfaces/IPancakeV3PoolDeployer.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/BitMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/FixedPoint128.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/FixedPoint96.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/FullMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/LiquidityMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/LowGasSafeMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/Oracle.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/Position.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/SafeCast.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/SqrtPriceMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/SwapMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/Tick.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/TickBitmap.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/TickMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/TransferHelper.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/libraries/UnsafeMath.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/PancakeV3Factory.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/PancakeV3Pool.sol ✅

sherex-v3-contracts/projects/v3-core/contracts/PancakeV3PoolDeployer.sol ✅

v3-lm-pool

sherex-v3-contracts/projects/v3-lm-pool/contracts/interfaces/IMasterChefV3.sol ✅

sherex-v3-contracts/projects/v3-lm-pool/contracts/interfaces/IPancakeV3LmPool.sol ✅

sherex-v3-contracts/projects/v3-lm-pool/contracts/interfaces/IPancakeV3LmPoolDeveloper.sol ✅

sherex-v3-contracts/projects/v3-lm-pool/contracts/libraries/LmTick.sol ✅

sherex-v3-contracts/projects/v3-lm-pool/contracts/PancakeV3LmPool.sol ✅

sherex-v3-contracts/projects/v3-lm-pool/contracts/PancakeV3LmPoolDeployer.sol ✅

v3-periphery

sherex-v3-contracts/projects/v3-periphery/contracts/base/BlockTimestamp.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/ERC721Permit.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/LiquidityManagement.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/Multicall.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/PeripheryImmutableState.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/PeripheryPayments.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/base/PeripheryPaymentsWithFee.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/base/PeripheryValidation.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/base/PoolInitializer.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/base/SelfPermit.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/external/IERC1271.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/external/IERC20PermitAllowed.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/external/IWETH9.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IERC20Metadata.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IERC721Permit.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IMulticall.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/INonfungiblePositionManager.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/INonfungibleTokenPositionDescriptor.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IPeripheryImmutableState.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IPeripheryPayments.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IPeripheryPaymentsWithFee.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IPoolInitializer.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IQuoter.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IQuoterV2.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/ISelfPermit.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/ISwapRouter.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/ITickLens.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/interfaces/IV3Migrator.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/lens ✅
– These contracts are not designed to be called on-chain. They simplify fetching on-chain data from off-chain.

sherex-v3-contracts/projects/v3-periphery/contracts/libraries/BytesLib.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/CallbackValidation.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/ChainId.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/HexStrings.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/LiquidityAmounts.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/NFTDescriptor.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/NFTSVG.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/OracleLibrary.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/Path.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/PoolAddress.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/PoolTicksCounter.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/PositionKey.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/PositionValue.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/SqrtPriceMathPartial.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/TokenRatioSortOrder.sol ✅
sherex-v3-contracts/projects/v3-periphery/contracts/libraries/TransferHelper.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/NFTDescriptorEx.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/NonfungiblePositionManager.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptor.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChain.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/NonfungibleTokenPositionDescriptorOffChainV2.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/SwapRouter.sol ✅

sherex-v3-contracts/projects/v3-periphery/contracts/V3Migrator.sol ✅

General notes

A lot of contracts use `pragma solidity ^0.8.10;` consider using a fixes pragma instead of a floating one.

Disclaimer

This audit report has been prepared by Coinsult's experts at the request of the client. It presents the results of both static analysis and manual code review. The purpose of the audit is to assess whether the functions operate as intended and to identify any potential security issues within the smart contract. The information contained in this report is intended solely to help understand the risks associated with the smart contract and to provide guidance for the development team on how the contract might be improved by addressing identified issues.

Important Notice

This audit is based on a PancakeSwap fork with some adjustments. It is assumed that the original PancakeSwap code is secure and has been well established over time. Accordingly, the focus of this audit is exclusively on the changes and adjustments made to the PancakeSwap code. The audit does not re-evaluate the security or functionality of the underlying PancakeSwap implementation.

Coinsult does not endorse, recommend, support, or suggest investing in any project based on this audit report. Nothing in this report should be construed as financial or investment advice. All decisions to use or invest in the audited project are made solely at the client's risk. Coinsult cannot be held responsible for any financial losses incurred as a result of relying on this report. Furthermore, Coinsult is not liable if a project is later found to be a scam, rug-pull, or honeypot.

Users of this audit report should perform their own due diligence and research before making any investment or development decisions.