# Protocol Audit Report

Prepared by: Bikalpa

# Table of Contents

# Protocol Summary

The `OrderBook` contract is a peer-to-peer trading system designed for `ERC20` tokens like `wETH`, `wBTC`, and `wSOL`. Sellers can list tokens at their desired price in `USDC`, and buyers can fill them directly on-chain.

# Disclaimer

Bikapa Regmi makes all effort to find as many vulnerabilities in the code in the given time period, but holds no responsibilities for the findings provided in this document. A security audit by the team is not an endorsement of the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the Solidity implementation of the contracts.

# Risk Classification

| | | **Impact** | | |
|---|---|---|---|---|
| | | High | Medium | Low |
| | High | H | H/M | M |
| Likelihood | Medium | H/M | M | M/L |
| | Low | M | M/L | L |

We use the CodeHawks severity matrix to determine severity. See the documentation for more details.

# Audit Details

## Scope

```
├── src
│   └── OrderBook.sol
```

## Roles

1. Seller - Who lists his order on the platform
2. buyer - Who buys the wrapped tokens giving usdc
3. Owner - Owner of the contract

# Executive Summary

I have spended 5 hr auditing codes and found only 2 vulnerability.

## Issues found

| Severity | Number of Issue Found |
|---|---|
| High | 0 |
| Medium | 0 |
| Low | 0 |
| gas | 1 |
| Info | 1 |
| Total | 2 |

# Findings

## Lows

### [L-1] The `_owner` shadows the state variable on `Ownable` contract.

**Description :** The constructor in `OrderBook` contract takes an argument of _owner and assigns that `_owner` to `Ownable` constructor. However, the `Ownable` contract uses `_ownable` address as a state variable. This affects the code readiability and clarity for those who reads code casually.

**Recommended Mitigation :**

```
```

```diff
-     constructor(address _weth, address _wbtc, address _wsol, address _usdc, address _owner) Ownable(_owner) { }

+     constructor(address _weth, address _wbtc, address _wsol, address _usdc, address _initialOwner) Ownable   (_initialOwner) { }
```

## Gas

### [G-1] Public variable not used internally.

If a function is marked public but is not used internally, consider marking it as `external`.

▶ 6 Found Instances

- Found in src/OrderBook.sol Line: 108

  ```
      function createSellOrder(
  ```

- Found in src/OrderBook.sol Line: 139

  ```
      function amendSellOrder(
  ```

- Found in src/OrderBook.sol Line: 178

  ```
      function cancelSellOrder(uint256 _orderId) public {
  ```

- Found in src/OrderBook.sol Line: 195

  ```
      function buyOrder(uint256 _orderId) public {
  ```

- Found in src/OrderBook.sol Line: 216

  ```
      function getOrder(uint256 _orderId) public view returns (Order memory orderDetails) {
  ```

- Found in src/OrderBook.sol Line: 221

  ```
      function getOrderDetailsString(uint256 _orderId) public view returns (string memory details) {
  ```