Obol SY Audit Report

Jul 18, 2025

Table of Contents

Summary

This report has been prepared for Obol SY smart contract, to discover issues and vulnerabilities in the source code of their Smart Contract as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis and Manual Review techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- Thorough line-by-line manual review of the entire codebase by industry experts.

Overview

Project Summary

Project Name	**Obol SY**
Codebase	**https://github.com/DAMM-Cap/Obol-SY**
Commit	**c13dfe2d8c976189be98c095a6ec886f904519a8**
Language	**Solidity**

Audit Summary

Delivery Date	**Jul 18, 2025**
Audit Methodology	**Static Analysis, Manual Review**
Total Isssues	**2**

[WP-H1] `_redeem` will burn the shares and transfer 0 `tokenOut` to the user

High

Issue Description

`amountTokenOut` is default to 0 and is never assigned a value.

Based on the context, the transfer amount should be `amountSharesToRedeem` instead.

```
75  function _redeem(address receiver, address tokenOut, uint256 amountSharesToRedeem)
76          internal
77          virtual
78          override
79          returns (uint256 amountTokenOut)
80      {
81          _transferOut(tokenOut, receiver, amountTokenOut);
82          return amountSharesToRedeem;
83      }
```

Recommendation

Change to:

```
75  function _redeem(address receiver, address tokenOut, uint256 amountSharesToRedeem)
76          internal
77          virtual
78          override
79          returns (uint256 amountTokenOut)
80      {
81          _transferOut(tokenOut, receiver, amountSharesToRedeem);
82          return amountSharesToRedeem;
83      }
```

Status

✓ Fixed

[WP-H2] Wrong implementation of `exchangeRate()`

High

Issue Description

- Expected: the number of asset wei corresponding to 1 wei of SY, scaled up by 1e18
- Current implementation: the number of SY wei corresponding to 1 wei of asset, scaled up by 1e18 (rounded up)

Also, according to `assetInfo()` , asset is `obol` , so in L87, "the exchange rate of stObol to rstObol" should probably be changed to "the exchange rate of stObol to obol" for better consistency and clarity (to avoid confusion from introducing new concepts).

```
85      /**
86       * @notice Calculates and updates the exchange rate of shares to underlying
    asset token
87       * @dev It is the exchange rate of stObol to rstObol
88       */
89      function exchangeRate() public view virtual override returns (uint256) {
90          return IRstObol(rstObol).sharesForStake(1 ether) / shareScaleFactor;
91      }
```

```
362   /// @notice Returns the number of shares that are valued at a given amount of
    stake token. Note that shares have a
363   /// scale factor of `SHARE_SCALE_FACTOR` applied to minimize precision loss due
    to truncation.
364   /// @param _amount The quantity of stake token that will be converted to a
    number of shares.
365   /// @return The quantity of shares that is worth the requested quantity of stake
    token.
366   function sharesForStake(uint256 _amount) external view virtual returns (uint256)
    {
367       Totals memory _totals = totals;
368       return _calcSharesForStakeUp(_amount, _totals);
369   }
```

```
1023    /// @notice Internal helper method that takes an amount of stake tokens and
        metadata representing the global state of
1024    /// the LST and returns the quantity of shares that is worth the requested
        quantity of stake token. All data for the
1025    /// calculation is provided in memory and the calculation is performed there,
        making it a pure function.
1026    /// @param _amount The quantity of stake token that will be converted to a
        number of shares.
1027    /// @param _totals The metadata representing current global conditions.
1028    /// @return The quantity of shares that is worth the provided quantity of stake
        token.
1029    function _calcSharesForStake(uint256 _amount, Totals memory _totals) internal
        pure virtual returns (uint256) {
1030      if (_totals.supply == 0) {
1031        return SHARE_SCALE_FACTOR * _amount;
1032      }
1033
1034      return (_amount * _totals.shares) / _totals.supply;
1035    }
1036
1037    /// @notice Internal helper method that takes an amount of stake tokens and
        metadata representing the global state of
1038    /// the LST and returns the quantity of shares that is worth the requested
        quantity of stake token, __rounded up__.
1039    /// All data for the calculation is provided in memory and the calculation is
        performed there, making it a pure
1040    /// function.
1041    /// @param _amount The quantity of stake token that will be converted to a
        number of shares.
1042    /// @param _totals The metadata representing current global conditions.
1043    /// @return The quantity of shares that is worth the provided quantity of stake
        token, __rounded up__.
1044    function _calcSharesForStakeUp(uint256 _amount, Totals memory _totals) internal
        pure virtual returns (uint256) {
1045      uint256 _result = _calcSharesForStake(_amount, _totals);
1046
1047      if (mulmod(_amount, _totals.shares, _totals.supply) > 0) {
1048        _result += 1;
1049      }
1050
1051      return _result;
1052    }
```

Recommendation

Change to:

```
85      /**
86       * @notice Calculates and updates the exchange rate of shares to underlying
    asset token
87       * @dev It is the exchange rate of stObol to Obol
88       */
89      function exchangeRate() public view virtual override returns (uint256) {
90          return IRstObol(rstObol).stakeForShares(1 ether * shareScaleFactor);
91      }
```

Status

✓ Fixed

Appendix

Timeliness of content

The content contained in the report is current as of the date appearing on the report and is subject to change without notice, unless indicated otherwise by WatchPug; however, WatchPug does not guarantee or warrant the accuracy, timeliness, or completeness of any report you access using the internet or other means, and assumes no obligation to update any information following publication.

Disclaimer

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Smart Contract technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security. No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate. FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.