SMART CONTRACT AUDIT REPORT

for

Wombat v4

PeckShield

Prepared By: Xiaomi Huang

PeckShield
March 27, 2023

Document Properties

Client	Wombat Exchange
Title	Smart Contract Audit Report
Target	Wombat v4
Version	1.0
Author	Luck Hu
Auditors	Luck Hu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	March 27, 2023	Luck Hu	Final Release
1.0-rc	March 21, 2023	Luck Hu	Release Candidate

Contact

For more information about this document and its contents, please contact PeckShield Inc.

Name	Xiaomi Huang
Phone	+86 183 5897 7782
Email	contact@peckshield.com

Contents

1 Introduction

Given the opportunity to review the design document and related smart contract source code of the Wombat protocol, we outline in the report our systematic approach to evaluate potential security issues in the smart contract implementation, expose possible semantic inconsistencies between smart contract code and design document, and provide additional suggestions or recommendations for improvement. Our results show that the given version of smart contracts is well designed and engineered, though it can be further improved by addressing our suggestions. This document outlines our audit results.

1.1 About Wombat v4

The Wombat is a BNB-native stableswap protocol with open-liquidity pools, low slippage and single-sided staking. It brings greater capital efficiency to fuel DeFi growth and adoption. This update brings additional support for USD+ which is rebasing token, and the liquid staking tokens which does not yet have an on-chain conversion oracle on BNB such as sfrxETH. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of Wombat v4

Item	Description
Name	Wombat Exchange
Website	https://www.wombat.exchange/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	March 27, 2023

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit. Note the audit scope only covers the following files: contracts/wombat-core/asset/USD+Asset.sol, contracts/wombat-core/asset/PriceFeedAsset.sol and contracts/wombat-core/libraries/GovernedPriceFeed.sol.

- https://github.com/wombat-exchange/wombat.git (48128c3)

And this is the commit ID after all fixes for the issues found in the audit have been checked in:

- https://github.com/wombat-exchange/wombat.git (55547ce)

1.2 About PeckShield

PeckShield Inc. [9] is a leading blockchain security company with the goal of elevating the security, privacy, and usability of current blockchain ecosystems by offering top-notch, industry-leading services and products (including the service of smart contract auditing). We are reachable at Telegram (https://t.me/peckshield), Twitter (http://twitter.com/peckshield), or Email (contact@peckshield.com).

Table 1.2: Vulnerability Severity Classification

Impact \ Likelihood	*High*	*Medium*	*Low*
High	Critical	High	Medium
Medium	High	Medium	Low
Low	Medium	Low	Low

1.3 Methodology

To standardize the evaluation, we define the following terminology based on the OWASP Risk Rating Methodology [8]:

- Likelihood represents how likely a particular vulnerability is to be uncovered and exploited in the wild;
- Impact measures the technical loss and business damage of a successful attack;
- Severity demonstrates the overall criticality of the risk.

Likelihood and impact are categorized into three ratings: *H*, *M* and *L*, i.e., *high*, *medium* and *low* respectively. Severity is determined by likelihood and impact and can be classified into four categories accordingly, i.e., *Critical*, *High*, *Medium*, *Low* shown in Table 1.2.

Table 1.3: The Full Audit Checklist

Category	Checklist Items
Basic Coding Bugs	Constructor Mismatch
	Ownership Takeover
	Redundant Fallback Function
	Overflows & Underflows
	Reentrancy
	Money-Giving Bug
	Blackhole
	Unauthorized Self-Destruct
	Revert DoS
	Unchecked External Call
	Gasless Send
	Send Instead Of Transfer
	Costly Loop
	(Unsafe) Use Of Untrusted Libraries
	(Unsafe) Use Of Predictable Variables
	Transaction Ordering Dependence
	Deprecated Uses
Semantic Consistency Checks	Semantic Consistency Checks
Advanced DeFi Scrutiny	Business Logics Review
	Functionality Checks
	Authentication Management
	Access Control & Authorization
	Oracle Security
	Digital Asset Escrow
	Kill-Switch Mechanism
	Operation Trails & Event Generation
	ERC20 Idiosyncrasies Handling
	Frontend-Contract Integration
	Deployment Consistency
	Holistic Risk Management
Additional Recommendations	Avoiding Use of Variadic Byte Array
	Using Fixed Compiler Version
	Making Visibility Level Explicit
	Making Type Inference Explicit
	Adhering To Function Declaration Strictly
	Following Other Best Practices

To evaluate the risk, we go through a checklist of items and each would be labeled with a severity category. For one check item, if our tool or analysis does not identify any issue, the contract is considered safe regarding the check item. For any discovered issue, we might further deploy contracts on our private testnet and run tests to confirm the findings. If necessary, we would additionally build a PoC to demonstrate the possibility of exploitation. The concrete list of check items is shown in Table 1.3.

In particular, we perform the audit according to the following procedure:

- Basic Coding Bugs: We first statically analyze given smart contracts with our proprietary static code analyzer for known coding bugs, and then manually verify (reject or confirm) all the issues found by our tool.
- Semantic Consistency Checks: We then manually check the logic of implemented smart contracts and compare with the description in the white paper.
- Advanced DeFi Scrutiny: We further review business logics, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.
- Additional Recommendations: We also provide additional suggestions regarding the coding and development of smart contracts from the perspective of proven programming practices.

To better describe each issue we identified, we categorize the findings with Common Weakness Enumeration (CWE-699) [7], which is a community-developed list of software weakness types to better delineate and organize weaknesses around concepts frequently encountered in software development. Though some categories used in CWE-699 may not be relevant in smart contracts, we use the CWE categories in Table 1.4 to classify our findings. Moreover, in case there is an issue that may affect an active protocol that has been deployed, the public version of this report may omit such issue, but will be amended with full details right after the affected protocol is upgraded with respective fixes.

1.4 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s) or blockchain software, i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice.

Table 1.4: Common Weakness Enumeration (CWE) Classifications Used in This Audit

Category	Summary
Configuration	Weaknesses in this category are typically introduced during the configuration of the software.
Data Processing Issues	Weaknesses in this category are typically found in functionality that processes data.
Numeric Errors	Weaknesses in this category are related to improper calculation or conversion of numbers.
Security Features	Weaknesses in this category are concerned with topics like authentication, access control, confidentiality, cryptography, and privilege management. (Software security is not security software.)
Time and State	Weaknesses in this category are related to the improper management of time and state in an environment that supports simultaneous or near-simultaneous computation by multiple systems, processes, or threads.
Error Conditions, Return Values, Status Codes	Weaknesses in this category include weaknesses that occur if a function does not generate the correct return/status code, or if the application does not handle all possible return/status codes that could be generated by a function.
Resource Management	Weaknesses in this category are related to improper management of system resources.
Behavioral Issues	Weaknesses in this category are related to unexpected behaviors from code that an application uses.
Business Logic	Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application. Errors in business logic can be devastating to an entire application.
Initialization and Cleanup	Weaknesses in this category occur in behaviors that are used for initialization and breakdown.
Arguments and Parameters	Weaknesses in this category are related to improper use of arguments or parameters within function calls.
Expression Issues	Weaknesses in this category are related to incorrectly written expressions within code.
Coding Practices	Weaknesses in this category are related to coding practices that are deemed unsafe and increase the chances that an exploitable vulnerability will be present in the application. They may not directly introduce a vulnerability, but indicate the product has not been carefully developed or maintained.

2 Findings

2.1 Summary

Here is a summary of our findings after analyzing the implementation of the `Wombat` smart contracts. During the first phase of our audit, we study the smart contract source code and run our in-house static code analyzer through the codebase. The purpose here is to statically identify known coding bugs, and then manually verify (reject or confirm) issues reported by our tool. We further manually review business logic, examine system operations, and place DeFi-related aspects under scrutiny to uncover possible pitfalls and/or bugs.

Severity	# of Findings	
Critical	0	
High	0	
Medium	1	■
Low	2	■ ■
Informational	0	
Total	3	

We have so far identified a list of potential issues: some of them involve subtle corner cases that might not be previously thought of, while others refer to unusual interactions among multiple contracts. For each uncovered issue, we have therefore developed test cases for reasoning, reproduction, and/or verification. After further analysis and internal discussion, we determined a few issues of varying severities need to be brought up and paid more attention to, which are categorized in the above table. More information can be found in the next subsection, and the detailed discussions of each of them are in Section 3.

2.2 Key Findings

Overall, these smart contracts are well-designed and engineered, though the implementation can be improved by resolving the identified issues (shown in Table 2.1), including 1 medium-severity vulnerabilities and 2 low-severity vulnerabilities.

Table 2.1: Key Wombat v4 Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Revisited Calculation of Skim Amount in _quoteSkimAmount()	Business Logic	Fixed
PVE-002	Low	Trust Issue of Admin Keys	Security Features	Mitigated
PVE-003	Low	Suggested immutable Usage for Gas Efficiency	Coding Practices	Fixed

Beside the identified issues, we emphasize that for any user-facing applications and services, it is always important to develop necessary risk-control mechanisms and make contingency plans, which may need to be exercised before the mainnet deployment. The risk-control mechanisms should kick in at the very moment when the contracts are being deployed on mainnet. Please refer to Section 3 for details.

PeckShield

3 | Detailed Results

3.1 Revisited Calculation of Skim Amount

- ID: PVE-001
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `USDPlusAsset`
- Category: Business Logic [6]
- CWE subcategory: CWE-841 [3]

Description

In the `Wombat` protocol, the `USDPlusAsset` contract is added to support `USD+` which is a rebasing token. The contract exposes a `skim()` function for the project owner to skim the extra reward in the same transaction with the payout. While reviewing the calculation of the skim amount that the owner can skim from the `USD+` pool, we notice it does not properly take the pending fee and the tip bucket into consideration.

To elaborate, we show below the code snippets of the `skim()/_quoteSkimAmount()` routines. As the name indicates, the `skim()` routine is used for the project owner to skim the `USD+` from the pool. At the beginning, it calls the `IPool(pool).mintFee()` routine to distribute current collected fee in the pool (line 43). Then it calls the `_quoteSkimAmount()` routine which calculates the skim amount by subtracting the pool cash from the `USD+` balance of the pool (line 55).

```
40      function skim(address _to) external nonReentrant returns (uint256 amount) {
41          require(hasRole(ROLE_USDPlusAdmin, msg.sender), 'not authorized');

43          IPool(pool).mintFee(underlyingToken);
44          amount = _quoteSkimAmount();
45          IERC20(underlyingToken).safeTransfer(_to, amount);

47          emit Skim(amount, _to);
48      }

50      function _quoteSkimAmount() internal view returns (uint256 amount) {
51          uint256 tokenBalance = IERC20(underlyingToken).balanceOf(address(this));
```

```
        uint256 cash_ = DSMath.fromWad(cash, underlyingTokenDecimals);

        if (tokenBalance < cash_) revert NotEnoughCash(tokenBalance, cash_);
        amount = tokenBalance - cash_;
    }
```

Listing 3.1: USDPlusAsset::skim()/_quoteSkimAmount()

However, it comes to our attention that the calculation of the skim amount does not take the pending fee and the tip bucket into consideration. Firstly, though it calls the `IPool(pool).mintFee()` routine to distribute the collected fee in advance, the current fee amount may not reach the `mintFeeThreshold` (line 988). In this case, the collected fee is still pending in the pool which needs to be subtracted from the skim amount. Secondly, the calculation does not subtract the tip bucket which is reserved from the fee as retention. As a result, the calculated skim amount may be much bigger than expectation and more `USD+` is skimmed from the pool.

```
986    function _mintFee(IAsset asset) internal {
987        uint256 feeCollected = _feeCollected[asset];
988        if (feeCollected == 0 feeCollected < mintFeeThreshold) {
989            // early return
990            return;
991        }
992        ...
993    }
```

Listing 3.2: USDPlusAsset::skim()/_quoteSkimAmount()

Recommendation Revisit the calculation of the skim amount to take the pending fee and the tip bucket into consideration.

Status The issue has been fixed by this commit: `55547ce`, and the team confirms to set both the `lpDividendRatio` and the `retentionRatio` to 50%, so no fee is sent to the tip bucket.

3.2 Trust Issue of Admin Keys

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Medium
- Target: `Multiple contracts`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [2]

Description

In the `Wombat` protocol, there is a privileged account, i.e., `owner`, that plays a critical role in governing and regulating the system-wide operations (e.g., add price operator who can set asset price). Our analysis shows that this privileged account needs to be scrutinized. In the following, we show the representative functions potentially affected by the privileges of the owner account.

Firstly, the privileged functions in GovernedPriceFeed allow for the owner to add/remove operator who can set price for the asset.

```
    function addOperator(address _operator) external onlyOwner {
        _grantRole(ROLE_OPERATOR, _operator);
    }

    function removeOperator(address _operator) external onlyOwner {
        _revokeRole(ROLE_OPERATOR, _operator);
    }

    function setLatestPrice(uint256 _newPrice) external {
        require(hasRole(ROLE_OPERATOR, msg.sender), 'not authorized');
        if (_newPrice >= _price) {
            require(_newPrice - _price <= maxDeviation, 'maxDeviation not respected');
        } else {
            require(_price - _newPrice <= maxDeviation, 'maxDeviation not respected');
        }
        _price = _newPrice;

        emit SetLatestPrice(_newPrice);
    }
```

Listing 3.3: Example Privileged Operations in the GovernedPriceFeed Contract

Secondly, the privileged function in PriceFeedAsset allows for the owner to set the priceFeed where the price is read.

```
function setPriceFeed(IPriceFeed _priceFeed) external onlyOwner {
    require(address(_priceFeed) != address(0), 'zero addr');
    priceFeed = _priceFeed;

    emit SetPriceFeed(_priceFeed);
}
```

Listing 3.4: Example Privileged Operations in the PriceFeedAsset Contract

Lastly, the privileged functions in USDPlusAsset allow for the owner to add/remove USD+ admin who can skim USD+ from the protocol.

```
    function addUSDPlusAdmin(address _admin) external onlyOwner {
        _grantRole(ROLE_USDPlusAdmin, _admin);
    }

    function removeUSDPlusAdmin(address _admin) external onlyOwner {
        _revokeRole(ROLE_USDPlusAdmin, _admin);
    }

    function skim(address _to) external nonReentrant returns (uint256 amount) {
        require(hasRole(ROLE_USDPlusAdmin, msg.sender), 'not authorized');
```

```
        IPool(pool).mintFee(underlyingToken);
        amount = _quoteSkimAmount();
        IERC20(underlyingToken).safeTransfer(_to, amount);

        emit Skim(amount, _to);
    }
```

Listing 3.5: Example Privileged Operations in the `USDPlusAsset` Contract

We understand the need of the privileged functions for contract maintenance, but at the same time the extra power to the `owner` may also be a counter-party risk to the protocol users. It is worrisome if the privileged `owner` account is a plain EOA account. Note that a multi-sig account could greatly alleviate this concern, though it is still far from perfect. Specifically, a better approach is to eliminate the administration key concern by transferring the role to a community-governed DAO.

Recommendation Promptly transfer the privileged account to the intended `DAO`-like governance contract. All changed to privileged operations may need to be mediated with necessary timelocks. Eventually, activate the normal on-chain community-based governance life-cycle and ensure the intended trustless nature and high-quality distributed governance.

Status This issue has been mitigated as the team confirmes they will use multi-sig for the privileged account.

3.3 Suggested immutable Usage for Gas Efficiency

- ID: PVE-003
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: `GovernedPriceFeed`
- Category: Coding Practices [5]
- CWE subcategory: CWE-1099 [1]

Description

Since version 0.6.5, `Solidity` introduces the feature of declaring a state as `immutable`. An `immutable` state variable can only be assigned during contract creation, but will remain constant throughout the life-time of a deployed contract. The main benefit of declaring a state as `immutable` is that reading the state is significantly cheaper than reading from regular storage, since it is not stored in storage anymore. Instead, an `immutable` state will be directly inserted into the runtime code.

This feature is introduced based on the observation that the reading and writing of storage-based contract states are gas-expensive. Therefore, it is always preferred if we can reduce, if not eliminate, storage reading and writing as much as possible. Those state variables that are written only once are candidates of `immutable` states under the condition that each fits the pattern, i.e., "a constant, once assigned in the constructor, is read-only during the subsequent operation."

In the following, we show the key state variable `maxDeviation` in the `GovernedPriceFeed` contract (line 19). If there is no need to dynamically update this key variable, it can be declared as either constant or `immutable` for gas efficiency. In particular, the above state variable can be defined as `immutable` as it will not be changed after its initialization in `constructor()`.

```
13 contract GovernedPriceFeed is IPriceFeed, Ownable, AccessControl {
14   bytes32 public constant ROLE_OPERATOR = keccak256('operator');

16   address public immutable token;

18   /// @notice max deviation allowed for updating oracle in case wrong parameter is supplied
19   uint256 public maxDeviation;
20   uint256 private _price;

22   event SetLatestPrice(uint256 newPrice);

24   constructor(address _token, uint256 _initialPrice, uint256 _maxDeviation) {
25       token = _token;
26       _price = _initialPrice;
27       maxDeviation = _maxDeviation;
28       _grantRole(ROLE_OPERATOR, msg.sender);
29   }
30   ...
31 }
```

Listing 3.6: `GovernedPriceFeed.sol`

Recommendation Revisit the state variable definition and make extensive use of `immutable` states for gas efficiency.

Status The issue has been fixed by this commit: `55547ce`.

4 Conclusion

In this audit, we have analyzed the design and implementation of the Wombat v4 protocol. The update brings additional support for USD+ which is rebasing token, and the liquid staking tokens which does not yet have an on-chain conversion oracle on BNB such as sfrxETH. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Moreover, we need to emphasize that Solidity-based smart contracts as a whole are still in an early, but exciting stage of development. To improve this report, we greatly appreciate any constructive feedbacks or suggestions, on our methodology, audit findings, or potential gaps in scope/coverage.

PeckShield

References

[1] MITRE. CWE-1099: Inconsistent Naming Conventions for Identifiers. https://cwe.mitre.org/data/definitions/1099.html.

[2] MITRE. CWE-287: Improper Authentication. https://cwe.mitre.org/data/definitions/287.html.

[3] MITRE. CWE-841: Improper Enforcement of Behavioral Workflow. https://cwe.mitre.org/data/definitions/841.html.

[4] MITRE. CWE CATEGORY: 7PK - Security Features. https://cwe.mitre.org/data/definitions/254.html.

[5] MITRE. CWE CATEGORY: Bad Coding Practices. https://cwe.mitre.org/data/definitions/1006.html.

[6] MITRE. CWE CATEGORY: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[7] MITRE. CWE VIEW: Development Concepts. https://cwe.mitre.org/data/definitions/699.html.

[8] OWASP. Risk Rating Methodology. https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.

[9] PeckShield. PeckShield Inc. https://www.peckshield.com.