SMART CONTRACT AUDIT REPORT

for

GumBall

Prepared By: Xiaomi Huang

PeckShield

December 23, 2022

Document Properties

Client	GumBall
Title	Smart Contract Audit Report
Target	GumBall
Version	1.0
Author	Stephen Bie
Auditors	Stephen Bie, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	December 23, 2022	Stephen Bie	Final Release
1.0-rc	November 24, 2022	Stephen Bie	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 GumBall 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 can be further improved due to the presence of several issues related to either security or performance. This document outlines our audit results.

1.1 About GumBall

GumBall protocol is a DeFi NFT creation and trading hub. When an NFT collection is launched on the GumBall protocol, a corresponding amount of ERC20 tokens (GBTs) are also created for that collection. These tokens are specific to the collection and are sold on a bonding curve, with the liquidity from these sales staying in the bonding curves to act as liquidity for the collection holders to utilize. This allows users to easily swap in and out of GumBall NFT instantly, stake their NFTs, borrow against them and much more.

Table 1.1: Basic Information of GumBall

Item	Description
Target	GumBall
Type	EVM Smart Contract
Language	Solidity
Audit Method	Whitebox
Latest Audit Report	December 23, 2022

In the following, we show the Git repository of reviewed files and the commit hash value used in this audit.

- https://github.com/Heesho/GumballV2.git (8037dbb)

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

- https://github.com/Heesho/GumballV2.git (206521f)

Please note this audit only covers the `GumBallFactory.sol` (previously `Factory.sol`), `GBTFactory.sol` (previously `ERC20BondingCurveL.sol`), `GNFTFactory.sol` (previously `Gumball.sol`), and `XGBTFactory.sol` (previously `GumbarL.sol`) contracts.

1.2 About PeckShield

PeckShield Inc. [10] 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 OWASP Risk Rating Methodology [9]:

- 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.

To evaluate the risk, we go through a list of check 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) [8], 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.

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 1.3: The Full List of Check Items

Category	Check Item
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

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 Logics	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 `GumBall` implementation. 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	1	■
Total	4	

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 that 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 vulnerability, 2 low-severity vulnerabilities, and 1 informational recommendation.

Table 2.1: Key GumBall Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Low	Incompatibility with Deflationary/Rebasing Tokens	Business Logic	Confirmed
PVE-002	Low	Accommodation of Non-ERC20-Compliant Tokens	Coding Practices	Fixed
PVE-003	Informational	Suggested Event Generation for Key Operations	Coding Practices	Fixed
PVE-004	Medium	Trust Issue of Admin Keys	Security Features	Confirmed

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.

3 | Detailed Results

3.1 Incompatibility with Deflationary/Rebasing Tokens

- ID: PVE-001
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: ERC20BondingCurveL
- Category: Business Logic [7]
- CWE subcategory: CWE-841 [4]

Description

By design, the ERC20BondingCurveL contract is one of the main entries for interaction with users. In particular, one entry routine, i.e., buy(), is designed to swap a certain amount of BASE_TOKEN to GBT. While examining its logic, we observe the transfer amount of BASE_TOKEN is directly to be used to calculate the exchanged amount of GBT. This is reasonable under the assumption that the transfer of BASE_TOKEN will always result in full transfer.

```
    function buy(uint256 _amountBASE, uint256 _minGBT, uint256 expireTimestamp) public nonReentrant {
        require(start + delay <= block.timestamp  whitelist[msg.sender], "Market Closed");
        require(expireTimestamp == 0  expireTimestamp > block.timestamp, "Expired");

        address account = msg.sender;

        syncReserves();
        uint256 feeAmountBASE = _amountBASE * PROTOCOL / DIVISOR;
        treasuryBASE += (feeAmountBASE);

        uint256 oldReserveBASE = reserveVirtualBASE + reserveRealBASE;
        uint256 newReserveBASE = oldReserveBASE + _amountBASE - feeAmountBASE;

        uint256 oldReserveGBT = reserveGBT;
        uint256 newReserveGBT = oldReserveBASE * oldReserveGBT / newReserveBASE;

        uint256 outGBT = oldReserveGBT - newReserveGBT;
```

```

        require(outGBT > _minGBT, "Less than Min");

        if (start + delay >= block.timestamp) {
            require(outGBT <= 10e18 && limit[account] <= 10e18, "Over whitelist limit");
            limit[account] += outGBT;
            require(limit[account] <= 10e18, "Whitelist amount overflow");
        }

        reserveRealBASE = newReserveBASE - reserveVirtualBASE;
        reserveGBT = newReserveGBT;

        IERC20Upgradeable(BASE_TOKEN).safeTransferFrom(account, address(this), _amountBASE);
        IERC20Upgradeable(address(this)).safeTransfer(account, outGBT);

        emit Buy(account, _amountBASE);
    }
```

Listing 3.1: `ERC20BondingCurveL::buy()`

However, there exist other ERC20 tokens that may make certain customizations to their ERC20 contracts. One type of these tokens is deflationary tokens that charge certain fee for every `transfer()` or `transferFrom()`. (Another type is rebasing tokens such as `YAM`.) As a result, this may not meet the assumption behind these routines related to token transfer.

One possible mitigation is to measure the asset change right before and after the asset-transferring routines. In other words, instead of bluntly assuming the amount parameter in `transfer()` or `transferFrom()` will always result in full transfer, we need to ensure the increased or decreased amount in the contract before and after the `transfer()` or `transferFrom()` is expected and aligned well with our operation. Though these additional checks cost additional gas usage, we consider they are necessary to deal with deflationary tokens or other customized ones if their support is deemed necessary.

Recommendation If current codebase needs to support possible deflationary tokens, it is better to check the balance before and after the `transfer()`/`transferFrom()` call to ensure the book-keeping amount is accurate. This support may bring additional gas cost. Also, keep in mind that certain tokens may not be deflationary for the time being. However, they could have a control switch that can be exercised to turn them into deflationary tokens. One example is the widely-adopted `USDT`.

Status The issue has been confirmed by the team. There is no need to support deflationary/rebasing tokens.

3.2 Accommodation of Non-ERC20-Compliant Tokens

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low
- Target: ERC20BondingCurveL
- Category: Coding Practices [6]
- CWE subcategory: CWE-1126 [1]

Description

Though there is a standardized ERC-20 specification, many token contracts may not strictly follow the specification or have additional functionalities beyond the specification. In this section, we examine the approve() routine and analyze possible idiosyncrasies from current widely-used token contracts. In particular, we use the popular stablecoin, i.e., USDT, as our example. We show the related code snippet below.

```
/**
* @dev Approve the passed address to spend the specified amount of tokens on behalf
    of msg.sender.
* @param _spender The address which will spend the funds.
* @param _value The amount of tokens to be spent.
*/
function approve(address _spender, uint _value) public onlyPayloadSize(2 * 32) {

    // To change the approve amount you first have to reduce the addresses`
    //  allowance to zero by calling `approve(_spender, 0)` if it is not
    //  already 0 to mitigate the race condition described here:
    //  https://github.com/ethereum/EIPs/issues/20#issuecomment-263524729
    require(!((_value != 0) && (allowed[msg.sender][_spender] != 0)));

    allowed[msg.sender][_spender] = _value;
    Approval(msg.sender, _spender, _value);
}
```

Listing 3.2: USDT Token Contract

It is important to note that the approve() function does not have a return value. However, the IERC20 interface has defined the following approve() interface with a bool return value: function approve(address spender, uint256 amount)external returns (bool). As a result, the call to approve() may expect a return value. With the lack of return value of USDT's approve(), the call may be unfortunately reverted.

Because of that, a normal call to approve() is suggested to use the safe version, i.e., safeApprove (). In essence, it is a wrapper around ERC20 operations that may either throw on failure or return false without reverts. Moreover, the safe version also supports tokens that return no value (and instead revert or throw on failure). Note that non-reverting calls are assumed to be successful.

In the following, we show the `treasurySkim()` routine in the `ERC20BondingCurveL` contract. If the `USDT` token is supported as `BASE_TOKEN`, the unsafe version of `IERC20Upgradeable(BASE_TOKEN).approve(gumbar, 0)` (line 256) may revert as there is no return value in the `USDT` token contract's `approve()` implementation (but the `IERC20` interface expects a return value).

```
252     function treasurySkim() external {
253         ...
254 
255         // requires here
256         IERC20Upgradeable(BASE_TOKEN).approve(gumbar, 0);
257         IERC20Upgradeable(BASE_TOKEN).approve(gumbar, _treasuryBASE * GUMBAR / DIVISOR);
258         IGumbar(gumbar).notifyRewardAmount(BASE_TOKEN, _treasuryBASE * GUMBAR / DIVISOR)
            ;
259         IERC20Upgradeable(BASE_TOKEN).safeTransfer(artist, _treasuryBASE * ARTIST /
            DIVISOR);
260         IERC20Upgradeable(BASE_TOKEN).safeTransfer(treasury, _treasuryBASE * TREASURY /
            DIVISOR);
261         IERC20Upgradeable(BASE_TOKEN).safeTransfer(msg.sender, reward);
262 
263         emit Skim(msg.sender);
264     }
```

Listing 3.3: `ERC20BondingCurveL::treasurySkim()`

Recommendation Accommodate the above-mentioned idiosyncrasy about ERC20-related `approve()`.

Status The issue has been addressed by the following commit: `c788e00`.

3.3 Suggested Event Generation for Key Operations

- ID: PVE-003
- Severity: Informational
- Likelihood: N/A
- Impact: N/A
- Target: `Multiple Contracts`
- Category: Coding Practices [6]
- CWE subcategory: CWE-563 [3]

Description

In `Ethereum`, the `event` is an indispensable part of a contract and is mainly used to record a variety of runtime dynamics. In particular, when an `event` is emitted, it stores the arguments passed in transaction logs and these logs are made accessible to external analytics and reporting tools. `Events` can be emitted in a number of scenarios. One particular case is when system-wide parameters or settings are being changed. Another case is when tokens are being minted, transferred, or burned.

While examining the events that reflect the protocol dynamics, we notice there are several key operations that lack meaningful events to reflect their changes. In the following, we show several representative routines.

```
    function _whitelist(address[] memory accounts, bool _bool) external onlyProtocol() {
        for (uint256 i = 0; i < accounts.length; i++) {
            whitelist[accounts[i]] = _bool;
        }
    }

    function setTreasury(address _treasuryAddr) external onlyProtocol() {
        treasury = _treasuryAddr;
    }

    function changeArtist(address _newArtistAddr) external onlyArtist() {
        artist = _newArtistAddr;
    }
```

Listing 3.4: `ERC20BondingCurveL`

With that, we suggest to emit meaningful events for these key operations. Also, the key event information is better `indexed`. Note each emitted event is represented as a topic that usually consists of the signature (from a `keccak256` hash) of the event name and the types (`uint256`, `string`, etc.) of its parameters. Each indexed type will be treated like an additional topic. If an argument is not indexed, it will be attached as data (instead of a separate topic). Considering that the key information is typically queried, it is better treated as a topic, hence the need of being `indexed`.

Recommendation Properly emit the above-mentioned events with accurate information to timely reflect state changes. This is very helpful for external analytics and reporting tools.

Status The issue has been addressed by the following commit: `c788e00`.

3.4 Trust Issue of Admin Keys

- ID: PVE-004
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple Contracts`
- Category: Security Features [5]
- CWE subcategory: CWE-287 [2]

Description

In the `GumBall` protocol, there are a series of privileged accounts that play a critical role in governing and regulating the protocol-wide operations (e.g., configuring various system parameters). In the following, we show the representative functions potentially affected by the privilege of the accounts.

```
    function setTreasury(address _treasury) external onlyOwner {
        treasury = _treasury;
        emit TreasurySet(_treasury);
    }

    function setGBTFactory(address _GBTFactory) external onlyOwner {
        GBTFactory = _GBTFactory;
        emit GBTFactorySet(_GBTFactory);
    }

    function setGNFTFactory(address _GNFTFactory) external onlyOwner {
        GNFTFactory = _GNFTFactory;
        emit GNFTFactorySet(_GNFTFactory);
    }

    function setXGBTFactory(address _XGBTFactory) external onlyOwner {
        XGBTFactory = _XGBTFactory;
        emit XGBTFactorySet(_XGBTFactory);
    }
```

Listing 3.5: `GumBallFactory`

```
    function setBaseURI(string memory uri) external {
        require((msg.sender == IGBT(GBT).artist()),"!AUTH");
        baseTokenURI = uri;

        emit SetBaseURI(uri);
    }

    function setContractURI(string memory uri) external {
        require((msg.sender == IGBT(GBT).artist()),"!AUTH");
        _contractURI = uri;

        emit SetContractURI(uri);
    }
```

Listing 3.6: `GNFT::setBaseURI()&&setContractURI()`

We emphasize that the privilege assignment is indeed necessary and consistent with the protocol design. However, it is worrisome if the privileged account is a plain EOA account. The `multi-sig` mechanism could greatly alleviate this concern, though it is still far from perfect. Note that a compromised privileged account would allow the attacker to modify a number of sensitive system parameters, which directly undermines the assumption of the protocol design.

Recommendation Suggest to introduce the `multi-sig` mechanism to manage all the privileged accounts to mitigate this issue. Additionally, all changes to privileged operations may need to be mediated with necessary timelocks.

Status The issue has been confirmed by the team.

4 | Conclusion

In this audit, we have analyzed the design and implementation of `GumBall`, which is a `DeFi NFT` creation and trading hub. When an `NFT` collection is launched on the `GumBall` protocol, a corresponding amount of ERC20 tokens (GBTs) are also created for that collection. These tokens are specific to the collection and are sold on a bonding curve, with the liquidity from these sales staying in the bonding curves to act as liquidity for the collection holders to utilize. After that, the user can easily swap in and out of `GumBall NFT` instantly, stake their `NFTs`, borrow against them and much more. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, we need to emphasize that 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.

References

[1] MITRE. CWE-1126: Declaration of Variable with Unnecessarily Wide Scope. https://cwe.mitre.org/data/definitions/1126.html.

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

[3] MITRE. CWE-563: Assignment to Variable without Use. https://cwe.mitre.org/data/definitions/563.html.

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

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

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

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

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

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

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