SMART CONTRACT AUDIT REPORT

for

Flashstake Protocol

Prepared By: Xiaomi Huang

PeckShield

June 24, 2022

Document Properties

Client	Blockzero Labs
Title	Smart Contract Audit Report
Target	Flashstake Protocol
Version	1.0
Author	Xiaotao Wu
Auditors	Xiaotao Wu, Xuxian Jiang
Reviewed by	Xiaomi Huang
Approved by	Xuxian Jiang
Classification	Public

Version Info

Version	Date	Author(s)	Description
1.0	June 24, 2022	Xiaotao Wu	Final Release
1.0-rc1	June 18, 2022	Xiaotao Wu	Release Candidate #1

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 `Flashstake` 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 Flashstake Protocol

The `Flashstake` protocol is designed for users to stake `principal` tokens and earn up-front yields via the supported strategy. The protocol is designed to be split into two main modules, i.e., the `FlashStake` and the `FlashStrategy`. The `FlashStake` keeps track of all accounting whilst the `FlashStrategy` is responsible for depositing the principal into the yield-earning protocols such as `AAVE`. The basic information of the audited protocol is as follows:

Table 1.1: Basic Information of The Flashstake Protocol

Item	Description
Name	Blockzero Labs
Website	https://blockzerolabs.io/
Type	EVM Smart Contract
Platform	Solidity
Audit Method	Whitebox
Latest Audit Report	June 24, 2022

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

- https://github.com/BlockzeroLabs/flashv3-contracts.git (1e720c3)

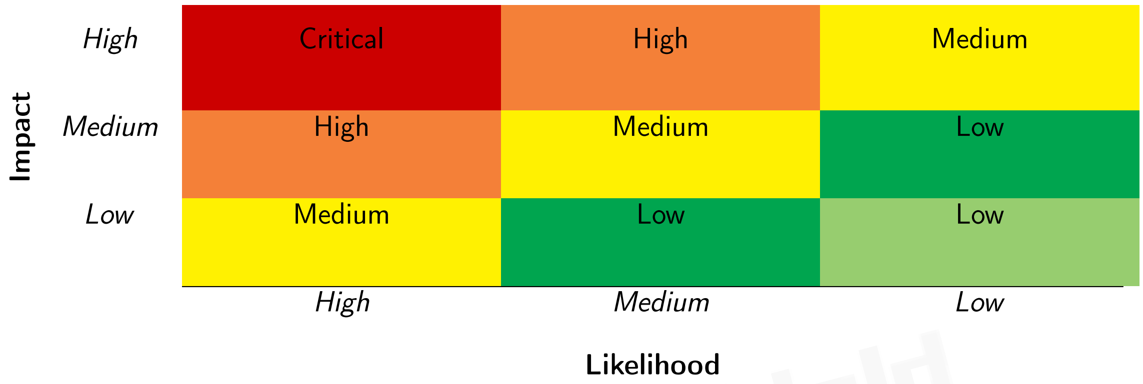
And here is the commit ID after fixes for the issues found in the audit have been checked in:

- https://github.com/BlockzeroLabs/flashv3-contracts.git (bbb40c5)

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 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.

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

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

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.

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 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 `Flashstake` protocol 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 logics, 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	2	■ ■
Low	1	■
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 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 2 medium-severity vulnerabilities and 1 low-severity vulnerability.

Table 2.1: Key Flashstake Protocol Audit Findings

ID	Severity	Title	Category	Status
PVE-001	Medium	Invalid Slippage Control in FlashProtocol::flashStake()	Time and State	Fixed
PVE-002	Low	Accommodation of Non-ERC20-Compliant Tokens	Business Logic	Fixed
PVE-003	Medium	Trust Issue of Admin Keys	Security Features	Mitigated

Besides recommending specific countermeasures to mitigate these issues, we also emphasize that 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 need to kick in at the very moment when the contracts are being deployed in mainnet. Please refer to Section 3 for details.

3 | Detailed Results

3.1 Invalid Slippage Control in FlashProtocol::flashStake()

- ID: PVE-001
- Severity: Medium
- Likelihood: Low
- Impact: High

- Target: `FlashProtocol`
- Category: Time and State [6]
- CWE subcategory: CWE-682 [2]

Description

The `FlashProtocol` contract provides a public `stake()` function for users to stake `principal` tokens and mint the corresponding amount of `fToken` to the users. The users-staked funds are transferred to the `FlashStrategy` to earn yields. The `fToken` can be burned by the stakers to claim yields earned by the `FlashStrategy`. To facilitate the yield claiming for users, the `FlashProtocol` contract also provides an external `flashStake()` function in which the acts of staking, minting `fToken` and burning all `fToken` are done in one transaction.

In the following, we examine the `FlashProtocol::flashStake()` routine that is designed to provide the staker with instant upfront yield within one transaction. We notice the actual burn `fToken` and claim yield operation `IFlashStrategy(_strategyAddress).burnFToken()` essentially specifies no restriction on possible slippage and is therefore vulnerable to possible front-running attacks, resulting in a smaller return (line 293). Note the way to use the `quotedReturn` parameter is invalid as it is eventually computed from `IFlashStrategy(_strategyAddress).quoteBurnFToken()` (line 289). In other words, the `IFlashStrategy(_strategyAddress).quoteBurnFToken()` output guarantees `tokensOwed=_minimumReturned` !

```
275     function flashStake(
276         address _strategyAddress,
277         uint256 _tokenAmount,
278         uint256 _stakeDuration,
279         address _yieldTo,
280         bool _mintNFT
```

```
    ) external nonReentrant {
        // Stake
        uint256 fTokensMinted = stake(_strategyAddress, _tokenAmount, _stakeDuration,
            _yieldTo, _mintNFT).fTokensToUser;

        IERC20C fToken = IERC20C(strategies[_strategyAddress].fTokenAddress);
        fToken.transferFrom(msg.sender, address(this), fTokensMinted);

        // Quote, approve, burn
        uint256 quotedReturn = IFlashStrategy(_strategyAddress).quoteBurnFToken(
            fTokensMinted);

        // Approve, burn and send yield to specified address
        fToken.approve(_strategyAddress, fTokensMinted);
        IFlashStrategy(_strategyAddress).burnFToken(fTokensMinted, quotedReturn,
            _yieldTo);
```

Listing 3.1: `FlashProtocol::flashStake()`

Recommendation Develop an effective mitigation to the above front-running attack to better protect the interests of users.

Status The issue has been fixed by this commit: `03000ee`.

3.2 Accommodation of Non-ERC20-Compliant Tokens

- ID: PVE-002
- Severity: Low
- Likelihood: Low
- Impact: Low

- Target: `Multiple contracts`
- Category: Business Logic [5]
- CWE subcategory: CWE-841 [3]

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 the following, we examine the `transfer()` routine and related idiosyncrasies from current widely-used token contracts.

In particular, we use the popular token, i.e., `ZRX`, as our example. We show the related code snippet below. On its entry of `transfer()`, there is a check, i.e., `if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to])`. If the check fails, it returns `false`. However, the transaction still proceeds successfully without being reverted. This is not compliant with the ERC20 standard and may cause issues if not handled properly. Specifically, the ERC20 standard specifies the following: *"Transfers _value amount of tokens to address _to, and MUST fire the Transfer event.*

The function SHOULD throw if the message caller's account balance does not have enough tokens to spend."

```
    function transfer(address _to, uint _value) returns (bool) {
        //Default assumes totalSupply can't be over max (2^256 - 1).
        if (balances[msg.sender] >= _value && balances[_to] + _value >= balances[_to]) {
            balances[msg.sender] -= _value;
            balances[_to] += _value;
            Transfer(msg.sender, _to, _value);
            return true;
        } else { return false; }
    }

    function transferFrom(address _from, address _to, uint _value) returns (bool) {
        if (balances[_from] >= _value && allowed[_from][msg.sender] >= _value &&
            balances[_to] + _value >= balances[_to]) {
            balances[_to] += _value;
            balances[_from] -= _value;
            allowed[_from][msg.sender] -= _value;
            Transfer(_from, _to, _value);
            return true;
        } else { return false; }
    }
```

Listing 3.2: ZRX.sol

Because of that, a normal call to `transfer()` is suggested to use the safe version, i.e., `safeTransfer()`, 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. Similarly, there is a safe version of `approve()/transferFrom()` as well, i.e., `safeApprove()/safeTransferFrom()`.

In current implementation, if we examine the `FlashProtocol::stake()` routine that is designed to transfer `principalToken` from the `msg.sender` to the `_strategyAddress` contract. To accommodate the specific idiosyncrasy, there is a need to user `safeTransferFrom()`, instead of `transferFrom()` (line 102).

```
89      function stake(
90          address _strategyAddress,
91          uint256 _tokenAmount,
92          uint256 _stakeDuration,
93          address _fTokensTo,
94          bool _issueNFT
95      ) public returns (StakeStruct memory _stake) {
96          require(strategies[_strategyAddress].principalTokenAddress != address(0), "
                UNREGISTERED STRATEGY");
97
98          require(_stakeDuration >= 60, "MINIMUM STAKE DURATION IS 60 SECONDS");
99          require(_stakeDuration <= IFlashStrategy(_strategyAddress).getMaxStakeDuration()
                , "EXCEEDS MAX STAKE DURATION");
100
101         // Transfer the tokens from caller to the strategy contract
```

```
        IERC20C(strategies[_strategyAddress].principalTokenAddress).transferFrom(
            msg.sender,
            address(_strategyAddress),
            _tokenAmount
        );

        ...
    }
```

Listing 3.3: `FlashProtocol::stake()`

Note this issue is also applicable to other routines, including `unstake()` from the `FlashProtocol` contract, `stake()/unstake()` from the `FlashBack` contract, and `increaseAllowance()/withdrawPrincipal()/withdrawERC20()/burnFToken()/depositReward()/addRewardTokens()/claimReward()` from the `FlashStrategyAAVEv2` contract.

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

Status This issue has been fixed in the following commit: `fbe3285`.

3.3 Trust Issue of Admin Keys

- ID: PVE-003
- Severity: Medium
- Likelihood: Medium
- Impact: Medium
- Target: `Multiple contracts`
- Category: Security Features [4]
- CWE subcategory: CWE-287 [1]

Description

In the `Flashstake` protocol, there is a privileged account, i.e., `owner`. The `owner` account plays a critical role in governing and regulating the system-wide operations (e.g., set `globalMintFee/globalMintFeeRecipient` for the `FlashProtocol` contract, set `rewardRatio/rewardLockoutTs/rewardTokenBalance/rewardTokenAddress` for the `FlashStrategyAAVEv2` contract, set `rewardRate/forfeitRewardAddress` for the `FlashBack` contract, etc.). Our analysis shows that this privileged account needs to be scrutinized. In the following, we use the `FlashStrategyAAVEv2` contract as an example and show the representative functions potentially affected by the privileges of the `owner` account.

```
    function depositReward(
        address _rewardTokenAddress,
        uint256 _tokenAmount,
        uint256 _ratio
    ) external onlyOwner {
        // Withdraw any reward tokens currently in contract and deposit new tokens
```

```
        if (rewardTokenBalance > 0) {
            // Only enforce this check if the rewardTokenBalance <= 0
            require(block.timestamp > rewardLockoutTs, "LOCKOUT IN FORCE");
            IERC20C(rewardTokenAddress).transfer(msg.sender, rewardTokenBalance);
        }
        IERC20C(_rewardTokenAddress).transferFrom(msg.sender, address(this), _tokenAmount);

        // Set Ratio and update lockout
        rewardRatio = _ratio;
        rewardLockoutTs = block.timestamp + rewardLockoutConstant;
        rewardTokenBalance = _tokenAmount;
        rewardTokenAddress = _rewardTokenAddress;
    }

    function addRewardTokens(uint256 _tokenAmount) external onlyOwner {
        IERC20C(rewardTokenAddress).transferFrom(msg.sender, address(this), _tokenAmount);
        rewardLockoutTs = block.timestamp + rewardLockoutConstant;

        // Renew the lockout period
        rewardTokenBalance = rewardTokenBalance + _tokenAmount;
    }

    function setRewardRatio(uint256 _ratio) external onlyOwner {
        // Ensure this can only be called whilst lockout is active
        require(rewardLockoutTs > block.timestamp, "LOCKOUT NOT IN FORCE");

        // Ensure the ratio can only be increased
        require(_ratio > rewardRatio, "RATIO CAN ONLY BE INCREASED");

        rewardRatio = _ratio;
    }
```

Listing 3.4: Example Privileged Operations in `FlashStrategyAAVEv2`

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 changes 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 confirms that multi-sig will be adopted for the privileged account.

4 Conclusion

In this audit, we have analyzed the `Flashstake` protocol design and implementation. The `Flashstake` protocol is designed for users to stake `principal` tokens and earn yields via the supported strategy. The current code base is well structured and neatly organized. Those identified issues are promptly confirmed and addressed.

Meanwhile, 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.

References

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

[2] MITRE. CWE-682: Incorrect Calculation. https://cwe.mitre.org/data/definitions/682.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: Business Logic Errors. https://cwe.mitre.org/data/definitions/840.html.

[6] MITRE. CWE CATEGORY: Error Conditions, Return Values, Status Codes. https://cwe.mitre.org/data/definitions/389.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.