

**HACKEN**

# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

**Customer:** Retreeb

**Date:** November 09<sup>th</sup>, 2021



This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed – upon a decision of the Customer.

## Document

<b>Name</b>	Smart Contract Code Review and Security Analysis Report for Retreeb.
<b>Approved by</b>	Andrew Matiukhin   CTO Hacken OU
<b>Type</b>	ERC20 token; Staking
<b>Platform</b>	Ethereum / Solidity
<b>Methods</b>	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
<b>Repository</b>	<a href="https://github.com/RetreebInc/staking-platform">https://github.com/RetreebInc/staking-platform</a>
<b>Commit</b>	de6c61f7559d9405ff6a764e8c0becdae8630ff7
<b>Technical Documentation</b>	NO
<b>JS tests</b>	YES
<b>Timeline</b>	06 OCTOBER 2021 - 09 NOVEMBER 2021
<b>Changelog</b>	11 OCTOBER 2021 - Initial Audit 22 OCTOBER 2021 - Second Review 09 NOVEMBER 2021 - Third Review



## Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	8
Audit overview	9
Conclusion	10
Disclaimers	12

## Introduction

Hacken OÜ (Consultant) was contracted by Retreeb (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contract and its code review conducted between October 6<sup>th</sup>, 2021 - October 11<sup>th</sup>, 2021.

Second review conducted on October 22<sup>nd</sup>, 2021.

Third review conducted on November 9<sup>th</sup>, 2021.

## Scope

The scope of the project is smart contracts in the repository:

**Repository:**

<https://github.com/RetreebInc/staking-platform>

**Commit:**

[de6c61f7559d9405ff6a764e8c0becdae8630ff7](https://github.com/RetreebInc/staking-platform/commit/de6c61f7559d9405ff6a764e8c0becdae8630ff7)

**Technical Documentation:** No

**JS tests:** Yes

**Contracts:**

[staking/StakingPlatform.sol](#)  
[staking/ISTakingPlatform.sol](#)  
[staking/TesterStakingPlatform.sol](#)  
[token/Token.sol](#)

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none"><li>▪ Reentrancy</li><li>▪ Ownership Takeover</li><li>▪ Timestamp Dependence</li><li>▪ Gas Limit and Loops</li><li>▪ DoS with (Unexpected) Throw</li><li>▪ DoS with Block Gas Limit</li><li>▪ Transaction-Ordering Dependence</li><li>▪ Style guide violation</li><li>▪ Costly Loop</li><li>▪ ERC20 API violation</li><li>▪ Unchecked external call</li><li>▪ Unchecked math</li><li>▪ Unsafe type inference</li><li>▪ Implicit visibility level</li><li>▪ Deployment Consistency</li><li>▪ Repository Consistency</li></ul>

	<ul style="list-style-type: none"> <li>▪ Data Consistency</li> </ul>
Functional review	<ul style="list-style-type: none"> <li>▪ Business Logics Review</li> <li>▪ Functionality Checks</li> <li>▪ Access Control &amp; Authorization</li> <li>▪ Escrow manipulation</li> <li>▪ Token Supply manipulation</li> <li>▪ Assets integrity</li> <li>▪ User Balances manipulation</li> <li>▪ Data Consistency manipulation</li> <li>▪ Kill-Switch Mechanism</li> <li>▪ Operation Trails &amp; Event Generation</li> </ul>

## Executive Summary

According to the assessment, the Customer's smart contracts are well-secured.



Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found 1 low severity issue.

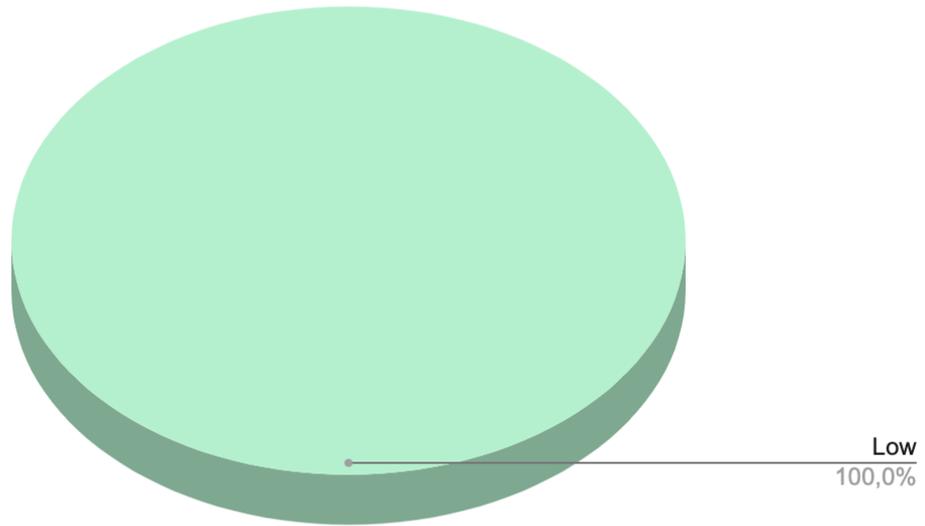
After the second review security engineers found that some contracts were slightly changed. Therefore found 3 medium and 1 low severity issues.



Hacken OÜ  
Parda 4, Kesklinn, Tallinn,  
10151 Harju Maakond, Eesti,  
Kesklinna, Estonia  
support@hacken.io

After the third review security engineers found 1 low severity issue.

*Graph 1. The distribution of vulnerabilities after the audit.*



## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
<b>High</b>	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution

## Audit overview

### ■ ■ ■ ■ Critical

No critical issues were found.

### ■ ■ ■ High

No high severity issues were found.

### ■ ■ Medium

1. All rewards for the staking period become available just after the user stakes

**Contracts:** StakingPlatform.sol

**Functions:** \_calculateRewards

**Recommendation:** Update function to return only rewards available since staking.

**Status:** fixed

2. Under some conditions, the user will be available to unstake just after stake

In case `lockupDuration < stakingDuration` and `lockupDuration` already passed since the start of staking, user will be available to withdraw just after deposit.

**Contracts:** StakingPlatform.sol

**Functions:** withdraw

**Recommendation:** Update function to prevent withdrawal before the finish of staking.

**Status:** expected behavior, not an issue

3. Unexpected remaining time calculation after the finish of staking

**Contracts:** StakingPlatform.sol

**Functions:** \_percentageTimeRemaining

**Recommendation:** Update function to return zero instead of 100% in case staking already finished, for example by changing last line to `return startPeriod == 0 ? precision : 0;`

**Status:** fixed



■ Low

**Vulnerability:** Block timestamp

Dangerous usage of `block.timestamp`. `block.timestamp` can be manipulated by miners. Contract `StakingPlatform` is fully related on the `block.timestamp`

**Recommendation:** Please consider relying on the `block.number` instead



## Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

As a result of the audit, security engineers found **1** low severity issue.

After the second review security engineers found **1** low severity issue.



## Disclaimers

### **Hacken Disclaimer**

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only – we recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts.

### **Technical Disclaimer**

Smart contracts are deployed and executed on a blockchain platform. The platform, its programming language, and other software related to the smart contract can have vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.