HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Uncut Global
Date: November 9th, 2021

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

Document

Name	Smart Contract Code Review and Security Analysis Report for Uncut Global.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	Pools; Pools Manager
Platform	Ethereum / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/bent-protocol/bent-public
Commit	e05a8890b3f39541e9cc2c267e82661ed0632d18
Technical Documentation	YES
JS tests	YES
Website	
Timeline	26 OCTOBER 2021 - 09 NOVEMBER 2021
Changelog	29 OCTOBER 2021 - INITIAL AUDIT 09 NOVEMBER 2021 - SECOND REVIEW

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

Table of contents

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

Introduction

Hacken OÜ (Consultant) was contracted by Uncut Global (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 26th, 2021 - October 29th, 2021.

Second code review conducted on November 9th, 2021.

Scope

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

Repository:
https://github.com/bent-protocol/bent-public
Commit:
e05a8890b3f39541e9cc2c267e82661ed0632d18
Technical Documentation: Yes; Bent V1.docx;
md5: e6db5ead61648cd1bec0e79e35a4efbd
JS tests: Yes; Included: "/test/"
Contracts:
interfaces\convex\IBaseRewardPool.sol
interfaces\convex\IConvexBooster.sol
interfaces\convex\IConvexToken.sol
interfaces\convex\IVirtualBalanceRewardPool.sol
interfaces\curve\curve.sol
interfaces\uniswap\IUniswapV2Factory.sol
interfaces\uniswap\IUniswapV2Pair.sol
interfaces\uniswap\IUniswapV2Router.sol
interfaces\uniswap\IWETH.sol
interfaces\IBentPool.sol
interfaces\IBentPoolManager.sol
libraries\Errors.sol
pools\BentBaseMasterchef.sol
pools\BentBasePool.sol
pools\BentPoolAlusd.sol
pools\BentPoolFrax.sol
pools\BentPoolMIM.sol
pools\BentPoolTriCrypto2.sol
pools\token\BentToken.sol
BentPoolManager.sol

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

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	▪ Reentrancy ▪ Ownership Takeover ▪ Timestamp Dependence ▪ Gas Limit and Loops ▪ DoS with (Unexpected) Throw ▪ DoS with Block Gas Limit ▪ Transaction-Ordering Dependence ▪ Style guide violation ▪ Costly Loop ▪ ERC20 API violation ▪ Unchecked external call ▪ Unchecked math ▪ Unsafe type inference ▪ Implicit visibility level ▪ Deployment Consistency ▪ Repository Consistency ▪ Data Consistency
Functional review	▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Assets integrity ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation

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

Executive Summary

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

Insecure	Poor secured	Secured	Well-secured

You are here 

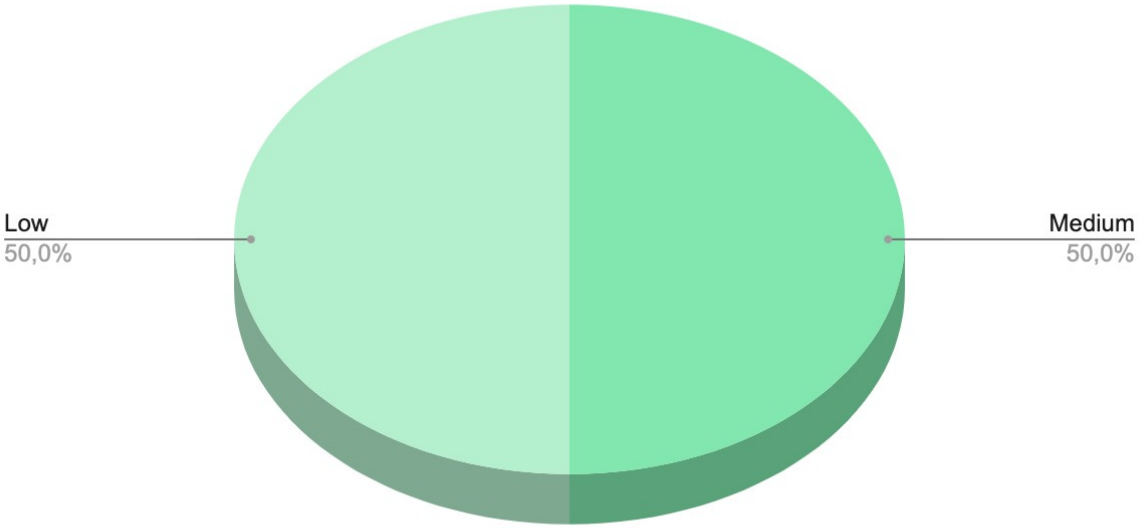
Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview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

As a result of the audit, security engineers found **1** high**,** **1** medium**,** and **2** low severity issues.

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

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

Graph 1. The distribution of vulnerabilities after the audit.



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

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	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
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution

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

Audit overview

Critical

No critical issues were found.

High

Possible rewards lost or receive more.

Changing **allocPoint** in the BentPoolManager.set method while **_withUpdate** flag set to **false** may lead to rewards lost or receiving rewards more than deserved.

Contracts: BentPoolManager.sol

Function: set

Recommendation: change.

Status: Fixed.

Medium

Provided tests not passed.

Error: ProviderError: Must be authenticated!

Recommendation: Please make sure tests are running and have at least 95% of branches covered.

Status: recommendation to set “ALCHEMY_ID” in the “.env” file didn’t change anything. Tests still cannot be run.

Low

1. Unnecessary operations.

When “allocPoint” is not changed for the pool, there is still an assignment for a new value, which just consumes gas doing nothing.

Contracts: BentPoolManager.sol

Function: set

Recommendation: Please move “totalAllocPoint” and “poolInfo[_pid].allocPoint” assignment inside the if block checking if the poolInfo[_pid].allocPoint != _allocPoint.

2. Reading state variable in the loop.

It is insufficient in a gas manner to read state variable in the loop.

Contracts: pools/BentBasePool.sol

Function: pendingReward, _updateAccPerShare, _calcAddedRewards, _updateUserRewardDebt, _harvest

Recommendation: Please store the value of the rewardPoolsCount into a local variable to save gas.

Status: Fixed.

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

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** high**,** **1** medium**,** and **2** low severity issues.

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

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

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.