

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT





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

Name	Smart Contract Code Review and Security Analysis Report for CDz Exchange-Initial Audit
Approved by	Andrew Matiukhin CTO Hacken OU
Type	BEP20 Token with Governance
Platform	Binance Smart Chain / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Git repository	https://github.com/CDzExchange/Pool/blob/master/contracts/CDzToken.sol
Commit	cc65bb8ef067872c8ced47531cd4b6a14e52f309
Timeline	29 JULY 2021 - 02 AUGUST 2021
Changelog	02 AUGUST 2021 - INITIAL AUDIT



Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	7
Audit overview	8
Conclusion	9
Disclaimers	11

Introduction

Hacken OÜ (Consultant) was contracted by CDz Exchange (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 July 29th, 2021 - August 02nd, 2021.

Scope

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

```
Repository:
  https://github.com/CDzExchange/Pool/blob/master/contracts/CDzToken.sol
Commit:
  cc65bb8ef067872c8ced47531cd4b6a14e52f309
```

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

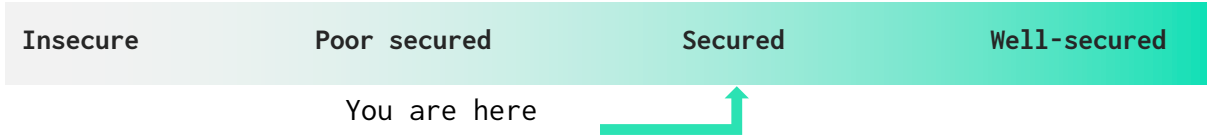
Category	Check Item
Code review	<ul style="list-style-type: none">▪ Reentrancy▪ Ownership Takeover▪ Timestamp Dependence▪ Gas Limit and Loops▪ DoS with (Unexpected) Throw▪ DoS with Block Gas Limit▪ Transaction-Ordering Dependence▪ Style guide violation▪ Costly Loop▪ BEP20 API violation▪ Unchecked external call▪ Unchecked math▪ Unsafe type inference▪ Implicit visibility level▪ Deployment Consistency▪ Repository Consistency▪ Data Consistency



Functional review	<ul style="list-style-type: none">▪ Business Logics Review▪ Functionality Checks▪ Access Control & Authorization▪ Escrow manipulation▪ Token Supply manipulation▪ Asset's integrity▪ User Balances manipulation▪ Kill-Switch Mechanism▪ Operation Trails & Event Generation
-------------------	---

Executive Summary

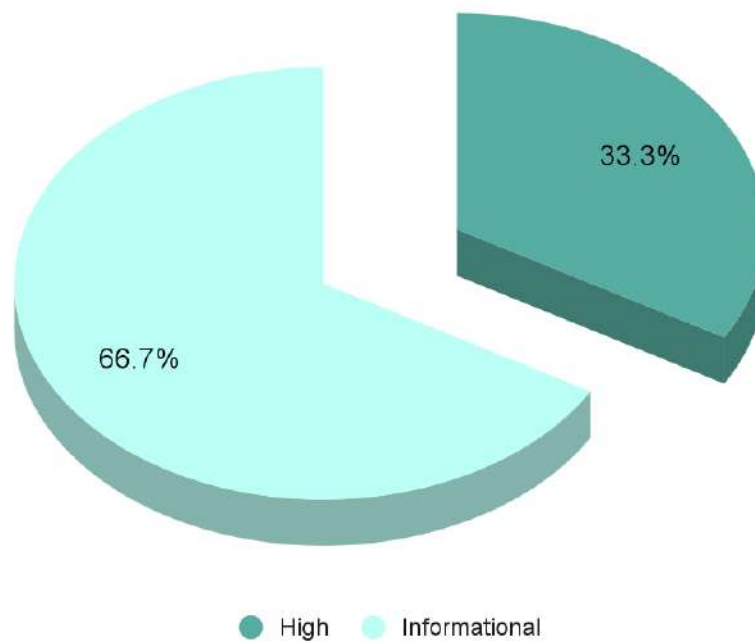
According to the assessment, the Customer's smart contracts are secured.



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.

Security engineers found 1 and 2 informational issues during the first review.

Graph 1. The distribution of vulnerabilities after the first review.



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
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Audit overview

■ ■ ■ ■ Critical

No Critical severity issues were found.

■ ■ ■ High

1. **Vulnerability:** Centralization.

The *mint* function of the *CDzToken* contract allows the owner to mint an unrestricted amount of tokens to anyone at any time.

Recommendation: If it really needs to be allowed to MasterChef to mint tokens, please make sure you're moving ownership to the MasterChef in the constructor as soon as the token is created.

Lines: #14-17

```
function mint(address _to, uint256 _amount) public onlyOwner {
    _mint(_to, _amount);
    _moveDelegates(address(0), _delegates[_to], _amount);
}
```

Customer's comment: we are going to transfer the token ownership to our masterchef contract to drive our farm and stake pools. This will be done immediately after we finalized our masterchef contract.

■ ■ Medium

No Medium severity issues were found.

■ Low

No Low severity issues were found.

■ Lowest / Code style / Best Practice

1. **Vulnerability:** Using SafeMath in solidity >0.8.

Starting solidity version 0.8 and later math is already checked and doesn't overflow and underflow. And it's not needed to check the result anymore.

Recommendation: Please consider not using SafeMath with solidity ≥ 0.8 .

2. **Vulnerability:** Public function that could be declared external **public** functions that are never called by the contract should be declared **external** to save gas.



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

Lines: #14

```
function mint(address _to, uint256 _amount) public onlyOwner {
```



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.

Security engineers found **1** high and **2** informational issues during the first review.



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 security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree 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 security of smart contracts.

Technical Disclaimer

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