HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Coinweb
Date: December 22nd, 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 Coinweb.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	ERC20 token; Vesting
Platform	Ethereum / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://gitlab.com/coinweb/coinweb-tokenomics
Commit	57700807d512ae2ea36722b450169d41f63e1df7
Deployed Contracts	https://etherscan.io/address/0x505b5eda5e25a67e1c24a2bf1a527ed9eb88bf04#code https://etherscan.io/address/0x13fe7160858f2a16b8e4429dff26c8a3a4b12b1b#code
Technical Documentation	NO
JS tests	NO
Timeline	20 SEPTEMBER 2021 - 22 DECEMBER 2021
Changelog	22 SEPTEMBER 2021 - INITIAL AUDIT 06 OCTOBER 2021 - SECOND REVIEW 02 DECEMBER 2021 - THIRD REVIEW 22 DECEMBER 2021 - FOURTH 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 Coinweb (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 September 20th, 2021 - September 22nd, 2021.

Second review conducted on October 6th, 2021.

Third review conducted on December 2nd, 2021.

Fourth review conducted on December 22nd, 2021.

Scope

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

Repository:
https://gitlab.com/coinweb/coinweb-tokenomics
Commit:
57700807d512ae2ea36722b450169d41f63e1df7
Deployed Contracts:
https://etherscan.io/address/0x505b5eda5e25a67e1c24a2bf1a527ed9eb88bf04#code
https://etherscan.io/address/0x13fe7160858f2a16b8e4429dff26c8a3a4b12b1b#code
Technical Documentation: No
JS tests: No
Contracts:
CoinwebToken.sol
TokenReleaser.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	▪ 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

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 **2** medium and **1** low severity issue.

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

After the second review security engineers found that **all** issues were addressed.

After the third review security engineers found that the token symbol was changed from CWB to CWEB, added release time, and some tokenomic changes were made. But **no security issues** were found.

After the fourth review security engineers found that TokenReleaser admin addresses were changed and also Admin was given rights to send tokens immediately to any address. Therefore **no security issues** were found.

Notice:

Admin has the rights to release any amount of tokens without using the release schedule.

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

No high severity issues were found.

Medium

1. The contract could not be compiled

   There is an issue in the code, no semicolon after the import statement line. That's why the contract could not be compiled.

   Recommendation: please check the code for all syntax errors.

   Fixed before the second review

2. Contract Releaser doesn't exist

   In the CoinwebToken smart contract, there is a state variable declaration, and Releaser is used as a type for this variable. However, there is no such smart contract name defined in the scope. Maybe it should be TokenReleaser?

   Recommendation: please double check the used smart contract names

   Fixed before the second review

3. No event on admin changed

   Changing admin in the TokenReleaser contract should emit an event for tracking off-chain

   Recommendation: please emit an event on admin changed

   Fixed before the second review

4. No event on booking tokens

   Booking tokens in the TokenReleaser contract should emit an event for tracking off-chain

   Recommendation: please emit an event on booking tokens

   Fixed before the second review

5. Test statements in the code

   There are several statements in the code which are marked as "just for testing"

   Recommendation: please remove testing statements

   Fixed before the second review

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

6. A lot of TODOs in the code

   The provided smart contracts don't look production-ready, a lot of undone TODOs appear in the code.

   Recommendation: please finish all TODOs

   Fixed before the second review

Low

1. Too many digits

   Literals with many digits are difficult to read and review.

   Recommendation: please use either ether suffix or scientific notation or even combine both (i.e. *7.68e9 ether*)

   Fixed before the second review

2. A public function that could be declared external

   public functions that are never called by the contract should be declared **external** to save gas.

   Recommendation: Use the **external** attribute for functions never called from the contract.

   Fixed before the second review

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 **2** medium and **1** low severity issue.

After the second review security engineers found that **all** issues were addressed.

After the third review security engineers found that the token symbol was changed from CWB to CWEB, added release time, and some tokenomic changes were made. But **no security issues** were found.

After the fourth review security engineers found that TokenReleaser admin addresses were changed and also Admin was given rights to send tokens immediately to any address. Therefore **no security issues** were found.

Notice:

Admin has the rights to release any amount of tokens without using the release schedule.

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.