

**HACKEN**

# SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

**Customer:** Edain Technologies AG

**Date:** March 25<sup>th</sup>, 2022

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 Edain Technologies AG.
<b>Approved By</b>	Evgeniy Bezuglyi   SC Department Head at Hacken OU
<b>Type of Contracts</b>	ERC20 token; Staking
<b>Platform</b>	EVM
<b>Language</b>	Solidity
<b>Methods</b>	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
<b>Website</b>	<a href="https://edain.ai/">https://edain.ai/</a>
<b>Timeline</b>	21.03.2022-25.03.2022
<b>Changelog</b>	25.03.2022 - Initial Review



## Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	7
Findings	8
Disclaimers	9

## Introduction

Hacken OÜ (Consultant) was contracted by Edain Technologies AG (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 contracts.

## Scope

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

**Repository:**

<https://github.com/EdainAI/edain-smartcontracts>

**Commit:** 9f0c4a5fffb97f23c7b5462420ad1f663301f69ba

**Technical Documentation:** Yes

<https://edain.ai/static/media/Edain-whitepaper.10aba7c0.pdf>

**JS tests:** Yes (in “test” directories)

**Contracts:**

EDAINStaking.sol

EDAINToken.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>▪ Transaction-Ordering Dependence</li><li>▪ Style guide violation</li><li>▪ EIP standards 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>
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</li><li>▪ Kill-Switch Mechanism</li></ul>

## Executive Summary

The score measurements details can be found in the corresponding section of the [methodology](#).

### Documentation quality

The Customer provided superficial functional requirements and technical requirements in a whitepaper. The total Documentation Quality score is **10** out of **10**.

### Code quality

The total CodeQuality score is **10** out of **10**. Code follows official style guides and uses best practices. Unit tests were provided

### Architecture quality

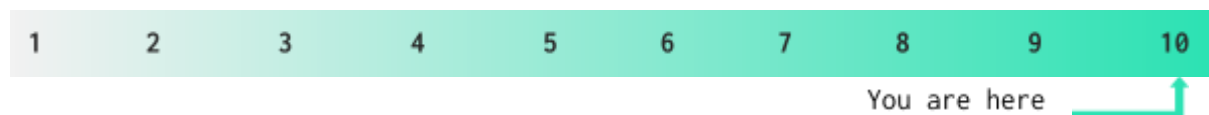
The architecture quality score is **10** out of **10**. Smart contracts of the project follow the best practices and have clean and clear architecture.

### Security score

As a result of the audit, security engineers found **1** low severity issue. The security score is **10** out of **10**. All found issues are displayed in the “Issues overview” section.

### Summary

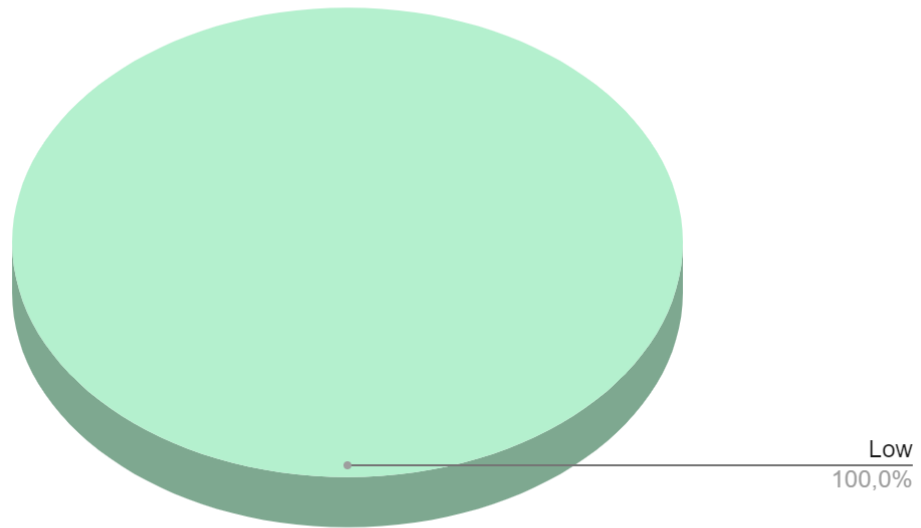
According to the assessment, the Customer's smart contract has the following score: **10.0**



### Notices

1. Owners can stop all token transfers with the *pause* function

*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 cannot lead to assets loss or data manipulations.
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that cannot have a significant impact on execution

## Findings

### ■■■■ Critical

No critical severity issues were found.

### ■■■ High

No high severity issues were found.

### ■■ Medium

No medium severity issues were found.

### ■ Low

#### 1. Floating pragma

The Staking.sol, XidenERC20.sol, EDAINStaking.sol and EDAINToken.sol contracts use floating pragma ^0.8.2 and ^0.8.7

**Contracts:** EDAINStaking.sol, EDAINToken.sol

**Recommendation:** Consider locking the pragma version whenever possible and avoid using a floating pragma in the final deployment.



## Disclaimers

### Hacken Disclaimer

The smart contracts given for audit have been analyzed by the best industry practices at the date of this report, with 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 a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements. 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 cannot guarantee the explicit security of the audited smart contracts.