HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: MooningMonkey.com
Date: February 14th, 2022

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

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 MooningMonkey.com.
Approved by	Andrew Matiukhin | CTO Hacken OU
Type	ERC721 token
Platform	BSC / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/Baushaus-io/monkey/tree/main/contracts
Commit	f566f2044aa4c340d4937ef07e97f0173a453a78
Technical Documentation	YES
JS tests	YES
Website	https://mooningmonkey.com/
Timeline	11 FEBRUARY 2022 - 14 FEBRUARY 2022
Changelog	12 FEBRUARY 2022 - Initial Audit 14 FEBRUARY 2022 - Second Audit

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 MooningMonkey.com (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 February 11th, 2022 - February 12th, 2022.

The second review was conducted on February 14th, 2022.

Scope

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

Repository:
https://github.com/Baushaus-io/monkey/tree/main/contracts
Commit:
f566f2044aa4c340d4937ef07e97f0173a453a78
Technical Documentation: Yes
JS tests: Yes
Contracts:
./contracts/contracts/interfaces/IClaimMerkle.sol
./contracts/contracts/interfaces/IMerkle.sol
./contracts/contracts/interfaces/IMMNFT.sol
./contracts/contracts/utils/ERC721A.sol
./contracts/contracts/utils/MMNFT.sol
./contracts/contracts/Merkle.sol
./contracts/contracts/MerkleClaim.sol
./contracts/contracts/MMDutchAuction.sol

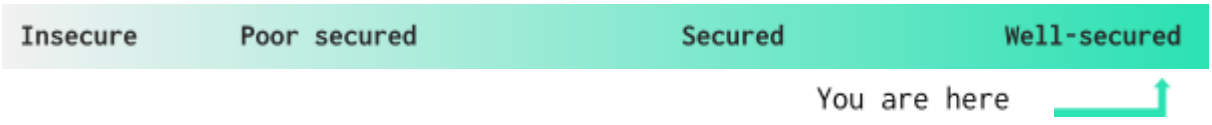
Hacken OÜ
Parda 4, Kesklinn, Tallinn,
10151 Harju Maakond, Eesti,
Kesklinna, Estonia
support@hacken.io

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

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

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

As a result of the second audit, security engineers found **no** issues. All previously reported issues have been fixed.

Notices:

The LinearDutchAuction.sol contract can mint MMNFT, but this is outside the scope of this 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

Contract owners can change the maximum supply after the contract is deployed.

Contracts: MMNFT.sol

Function: setSupply

Recommendation: remove the possibility of the supply manipulation.

Status: fixed.

High

According to the technical specifications, only whitelisted users can mint MMNFT, but the mint function allows anyone to mint.

Contracts: MMNFT.sol

Function: mint

Recommendation: restrict access to the mint function or remove it.

Status: fixed.

Medium

An outdated version of the code is being used. The new version has some gas optimizations and code improvements.

Contracts: ERC721A.sol

Recommendation: use the new version.

Status: fixed.

Low

The ‘initialized’ variable is not used.

Contracts: MerkleClaim.sol

Recommendation: remove unused variable.

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

As a result of the second audit, security engineers found **no** issues. All previously reported issues have been fixed.

Notices:

The LinearDutchAuction.sol contract can mint MMNFT, but this is outside the scope of this audit.

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.