

# 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

<b>Name</b>	Smart Contract Code Review and Security Analysis Report for Mogul - Second Review
<b>Approved by</b>	Andrew Matiukhin   CTO Hacken OU
<b>Type</b>	Voting, MasterChef
<b>Platform</b>	Ethereum / Solidity
<b>Methods</b>	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
<b>Git</b>	<a href="https://github.com/mogulproductions/smart-contracts-matic/pull/18/commits/3837d3c7af382c90f468936249c83741badae4ff">https://github.com/mogulproductions/smart-contracts-matic/pull/18/commits/3837d3c7af382c90f468936249c83741badae4ff</a>
<b>Timeline</b>	26 MAY 2021 - 30 MAY 2021
<b>Changelog</b>	27 MAY 2021 - INITIAL AUDIT 30 MAY 2021 - SECOND REVIEW



## Table of contents

Introduction	4
Scope	4
Executive Summary	6
Severity Definitions	7
Audit overview	8
Conclusion	9
Disclaimers	10

## Introduction

Hacken OÜ (Consultant) was contracted by Mogul (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on May 30<sup>th</sup>, 2021.

## Scope

The scope of the project is the smart contracts (MovieVoting and MovieVotingMasterChef) provided in the commit:

<https://github.com/mogulproductions/smart-contracts-matic/pull/18/commits/3837d3c7af382c90f468936249c83741badae4ff>

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"><li>▪ Reentrancy</li><li>▪ Ownership Takeover</li><li>▪ Timestamp Dependence</li><li>▪ Gas Limit and Loops</li><li>▪ DoS with (Unexpected) Throw</li><li>▪ DoS with Block Gas Limit</li><li>▪ Transaction-Ordering Dependence</li><li>▪ Style guide violation</li><li>▪ Costly Loop</li><li>▪ ERC20 API 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><li>▪ Data Consistency</li></ul>

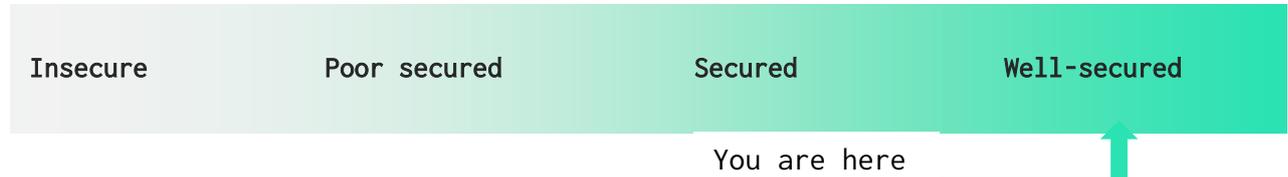


Functional review

- 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 well-secured

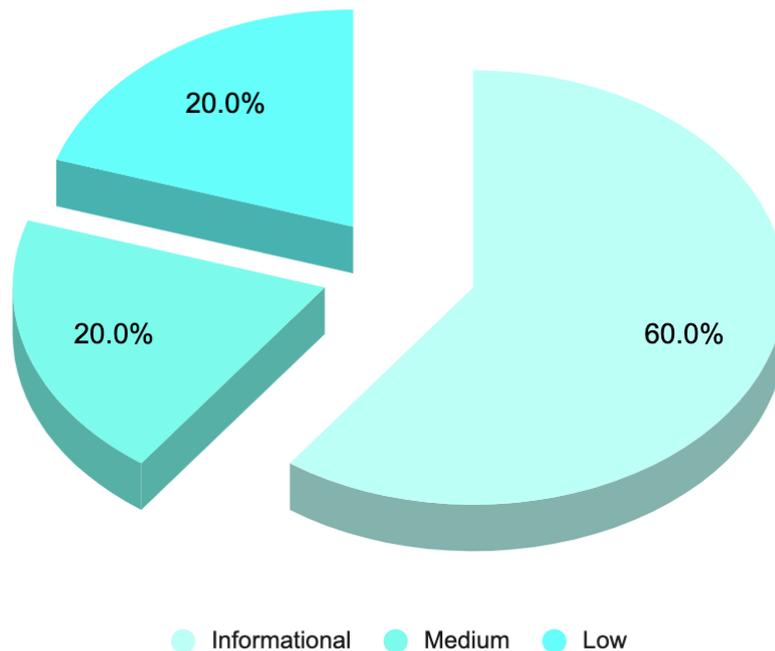


Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview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

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

Security engineers found **no issues** during the second review.

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



## 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 can't lead to assets loss or data manipulations.
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution
<b>Lowest / Code Style / Best Practice</b>	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

No High severity issues were found.

### ■ ■ Medium

#### 1. Vulnerability: Contracts that lock Ether

MovieVoting contract is BasicMetaTransaction therefore inherits the method executeMetaTransaction which is payable, so it may accept ETH. But there is no way to withdraw ETH from the MovieVoting. If someone sends ETH those would be locked on the contract forever.

Fixed before second review

### ■ Low

No Low severity issues were found

### ■ Lowest / Code style / Best Practice

#### 1. Vulnerability: Boolean equality

Boolean constants can be used directly and do not need to be compared to true or false.

Fixed before second review

#### 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.

Fixed before second review



## Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

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

Security engineers found **no issues** during the second 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.