QuillAudits

Audit Report
December, 2023

For

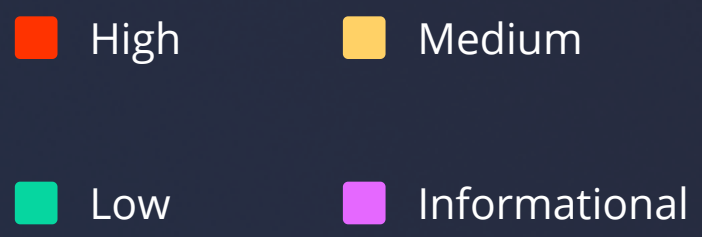
MOOLAHVERSE

Table of Content

Executive Summary

Project Name	Moolahverse
Overview	Moolahverse contract is an ERC20 token standard that mints 1 billion worth of Moolahverse token into the address of the deployer. This contract integrates the Openzeppelin standard and utilized both the ERC20Burnable and ERC20Permit extensions. While the burnable contract is an extension that allows token holders to destroy their tokens and from accounts which were given approval, the permit contract supports for approvals to be made through gasless signatures.
Timeline	4th December 2023 - 6th December 2023
Updated Code Received	10th December 2023
Second Review	11th December 2023
Method	Manual Review, Functional Testing, Automated Testing, etc. All the raised flags were manually reviewed and re-tested to identify any false positives.
Audit Scope	The scope of this audit was to analyze the Moolahverse.sol codebase for quality, security, and correctness.
Source Code	*https://github.com/moolahrick/mlh-contract/blob/master/moolahverse.sol*
Branch	master
Commit	67395ea79b6e0c53dce605a5b9b7f130c89da911
Fixed In	*https://github.com/moolahrick/mlh-contract/commit/d7dc915ffcdc9eb141057b2d640e8781ead6870b*
Mainnet Address	*https://etherscan.io/token/0xdf87270e04bc5ac140e93571d0dd0c6f4a058b41#code*

Number of Security Issues per Severity



	High	Medium	Low	Informational
Open Issues	0	0	0	0
Acknowledged Issues	0	0	0	0
Partially Resolved Issues	0	0	0	0
Resolved Issues	0	0	0	1

Checked Vulnerabilities

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contracts, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods, and tools were used to review all the smart contracts.

Structural Analysis

In this step, we have analyzed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis

A static Analysis of Smart Contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis

Manual Analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analyzed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption

In this step, we have checked the behavior of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit

Hardhat, Foundry.

Types of Severity

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

High Severity Issues

A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.

Medium Severity Issues

The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.

Low Severity Issues

Low-level severity issues can cause minor impact and are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.

Informational

These are four severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Types of Issues

Open

Security vulnerabilities identified that must be resolved and are currently unresolved.

Resolved

These are the issues identified in the initial audit and have been successfully fixed.

Acknowledged

Vulnerabilities which have been acknowledged but are yet to be resolved.

Partially Resolved

Considerable efforts have been invested to reduce the risk/impact of the security issue, but are not completely resolved.

High Severity Issues

No issues were found.

Medium Severity Issues

No issues were found.

Low Severity Issues

No issues were found.

Informational Issues

1. Floating Solidity Version

Path

Moolahverse.sol

Function

Pragma solidity ^0.8.20;

Description

Contract has a floating solidity pragma version. This is present also in inherited contracts. Locking the pragma helps to ensure that the contract does not accidentally get deployed using, for example, an outdated compiler version that might introduce bugs that affect the contract system negatively. The recent solidity pragma version also possesses its own unique bugs.

Recommendation

Making the contract use a stable solidity pragma version prevents bugs occurrence that could be ushered in by prospective versions. It is recommended, therefore, to use a fixed solidity pragma version while deploying to avoid deployment with versions that could expose the contract to attack.

Status

Resolved

Automated Tests

No major issues were found. Some false positive errors were reported by the tools. All the other issues have been categorized above according to their level of severity.

```
INFO:Detectors:
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse = (3 * denominator) ^ 2 (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#184)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#188)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#189)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#190)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#191)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#192)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - denominator = denominator / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#169)
        - inverse *= 2 - denominator * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#193)
Math.mulDiv(uint256,uint256,uint256) (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#123-202) performs a multiplication on the result of a division:
        - prod0 = prod0 / twos (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#172)
        - result = prod0 * inverse (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#199)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#divide-before-multiply
```

```
INFO:Detectors:
ERC20Permit.constructor(string).name (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/ERC20Permit.sol#39) shadows:
        - ERC20.name() (lib/openzeppelin-contracts/contracts/token/ERC20/ERC20.sol#58-60) (function)
        - IERC20Metadata.name() (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/IERC20Metadata.sol#15) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
```

```
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/interfaces/IERC5267.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/interfaces/draft-IERC6093.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/ERC20.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/IERC20.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/ERC20Burnable.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/ERC20Permit.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/IERC20Metadata.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/token/ERC20/extensions/IERC20Permit.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/Context.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/Nonces.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/ShortStrings.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/StorageSlot.sol#5) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/Strings.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/cryptography/ECDSA.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/cryptography/EIP712.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/cryptography/MessageHashUtils.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/math/Math.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (lib/openzeppelin-contracts/contracts/utils/math/SignedMath.sol#4) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.20 (src/Moolahverse.sol#2) necessitates a version too recent to be trusted. Consider deploying with 0.8.18.
Pragma version^0.8.13 (test/Moolahverse.t.sol#2) allows old versions
solc-0.8.21 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

Closing Summary

In this report, we have considered the security of the Moolahverse codebase. We performed our audit according to the procedure described above.

One informational issue was found, which the Moolahverse Team resolved.

Disclaimer

QuillAudits Smart contract security audit provides services to help identify and mitigate potential security risks in Moolahverse smart contracts. However, it is important to understand that no security audit can guarantee complete protection against all possible security threats. QuillAudits audit reports are based on the information provided to us at the time of the audit, and we cannot guarantee the accuracy or completeness of this information. Additionally, the security landscape is constantly evolving, and new security threats may emerge after the audit has been completed.

Therefore, it is recommended that multiple audits and bug bounty programs be conducted to ensure the ongoing security of Moolahverse smart contracts. One audit is not enough to guarantee complete protection against all possible security threats. It is important to implement proper risk management strategies and stay vigilant in monitoring your smart contracts for potential security risks.

QuillAudits cannot be held liable for any security breaches or losses that may occur subsequent to and despite using our audit services. It is the responsibility of the Moolahverse to implement the recommendations provided in our audit reports and to take appropriate steps to mitigate potential security risks.

About QuillAudits

QuillAudits is a secure smart contracts audit platform designed by QuillHash Technologies. We are a team of dedicated blockchain security experts and smart contract auditors determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

850+
Audits Completed

$30B
Secured

$30B
Lines of Code Audited

Follow Our Journey

Audit Report
December, 2023

For

MOOLAHVERSE

QuillAudits

Canada, India, Singapore, UAE, UK

www.quillaudits.com

audits@quillhash.com