parlour
[development]

# ROBOHERO TOKEN

## Security Assessment

March 21 2024

# SUMMARY

This report has been prepared for the RoboHero token project to identify potential issues and vulnerabilities in its ERC-20 standard smart contract deployed on the Polygon network. A detailed examination was carried out using the Manual Review technique, focusing on several key aspects to ensure the robustness and security of the smart contract. The audit process prioritized:

- Verifying the smart contract's adherence to the latest best practices and industry standards for ERC-20 tokens.
- Ensuring that the contract logic accurately reflects the intended functionalities and use cases proposed by the project stakeholders.
- Conducting an exhaustive line-by-line manual review of the entire smart contract codebase by seasoned industry experts.

**Audit Scope**

This audit reviewes the contents of an ERC-20 token called RoboHero. The smart contract's code is located in the RoboHero.sol file, which was added to the project's GitHub repository in the commit 6f4bb4b151a396ca8bf7dc3ca3190a5b5489145d.

Outside libraries utilized by the smart contract were *not* audited by Parlour Development, however they were priorly audited by independent third parties.

# OVERVIEW

## ERC-20 INFORMATION

| | |
|---|---|
| Name | RoboHero |
| Symbol | ROBO |
| Total supply | 1,000,000,000 |
| Decimals | 18 |

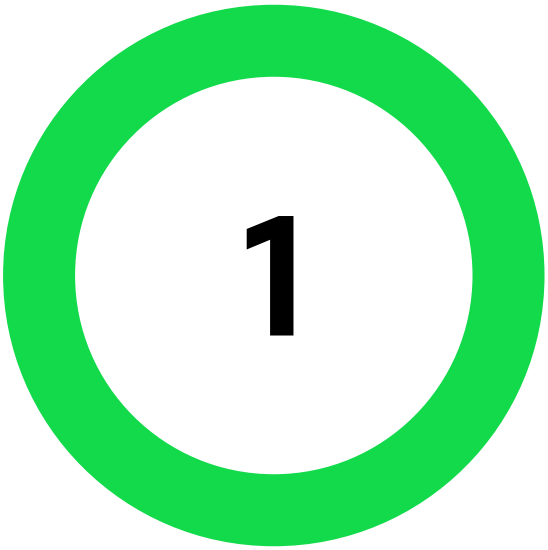
## DEPLOYMENT INFORMATION

| | |
|---|---|
| Network name | Polygon |
| Contract address | 0xb3886b3aaa6087b3d185daeb89ac113d195b5eb9 |
| Deployment date | Feb-09-2024 11:37:22 PM +UTC |
| Deployment block | 53330165 |
| Deployer address | 0xf6f120A9dd0751d71827d4E92eFE69Da6e1fF806 |

## TECHNICAL INFORMATION

| | |
|---|---|
| Technology | Solidity |
| Commit | 6f4bb4b151a396ca8bf7dc3ca3190a5b5489145d |

# FINDINGS




Total findings

- Informational
- Discussion
- Bad practice
- Minor
- Major
- Critical

| TITLE | IMPORTANCE |
| --- | --- |
| Implementation of ERC20Permit library | Informational |

# IMPLEMENTATION OF ERC20PERMIT LIBRARY

The project’s smart contract inherits from OpenZeppelin's ERC20 and ERC20Permit contracts, leveraging the OpenZeppelin library's security and reliability. The constructor mints 1 billion (1,000,000,000) tokens to the contract creator's address.

### Audit Overview

#### 1 Compliance and Functionality

The contract correctly implements the ERC20 standard functions through inheritance from the OpenZeppelin ERC20 contract. The ERC20Permit extension adds EIP-2612 permit functionality, allowing gasless transactions by permitting another address to spend tokens on the holder's behalf through a signed message.

#### 2 Code Quality and Security

Utilizing OpenZeppelin contracts for standard functionalities like ERC20 token behavior and permit features ensures high code quality and adherence to security best practices. The contracts from OpenZeppelin are widely used and audited by the community.

### 3 ERC20Permit Specific Considerations

- The ERC20Permit extension introduces a method for delegated token spending without requiring a traditional transaction. This feature is beneficial for user experience but necessitates careful handling of signatures and nonces to prevent replay attacks.

- The contract uses the ERC20Permit constructor to set the token name for the permit feature, aligning it with the token's name. This consistency is crucial for interface recognition and integration with wallets and other contracts.

## Potential Risks

### 1 Replay Attacks Prevention

Although OpenZeppelin implementation is designed to be secure against replay attacks through the use of nonces and the EIP-712 standard for structured data hashing and signing, it's crucial to ensure that these aspects are correctly implemented in any interacting systems. Regularly updating dependencies to include fixes and improvements from OpenZeppelin can mitigate risks associated with discovered vulnerabilities.

## 2 Gasless Transactions Scrutiny

While the permit feature enhances user experience by enabling gasless transactions, it also requires users to understand the implications of signing messages. Educating users on the security considerations of signing permits is advisable.

## 3 Audit of Integrations

Other contracts and external calls can cause security risks. It should be ensured that any contract interacting with RoboHero, especially those utilizing its permit feature, is thoroughly audited.

# DISCLAIMER

This audit report has been prepared by Parlour Development for informational purposes only, regarding the smart contract code of the RoboHero project, specifically focusing on its implementation of the ERC20 and ERC20Permit standards as provided in the supplied source code. It is important to note that this report does not constitute financial advice, investment advice, trading advice, or any other type of advice, and it should not be treated as such. The contents of this report are not meant to be used, nor should they be used, to make investment decisions.

The audit process involves a technical examination of the project's smart contract codebase to identify potential security vulnerabilities, design flaws, and adherence to best practices. While efforts have been made to conduct a thorough and comprehensive audit, the nature of smart contract development and the rapidly evolving landscape of blockchain technology mean that not all risks can be identified or predicted. As such, Parlour Development does not guarantee the security of the smart contract code or imply that the code is free from all possible vulnerabilities or issues.

Moreover, the findings, observations, and recommendations presented in this report are based on the state of the code at the time of the audit and the current understanding of blockchain technologies and standards as of 21/03/2024.

Future developments in blockchain technologies, smart contract design patterns, and security threats could render some of this report's findings obsolete or introduce new risks not considered during the audit.

Decisions to invest in, purchase, or use the RoboHero token or any related services should not be based solely on the information provided in this report. Potential investors and users are strongly advised to conduct their own due diligence, including consulting with professional advisors in the areas of legal, tax, financial, and other relevant disciplines, to understand the risks associated with smart contracts, cryptocurrencies, and token investments.

Parlour Development accepts no liability for any direct, indirect, or consequential loss or damage arising from the use of this report or its contents for making investment decisions. The use of the RoboHero smart contract, participation in the RoboHero token project, or any related activities is at the sole risk of the participants, without recourse to Parlour Development.

This report is confidential and intended solely for the use of stakeholders and may not be reproduced, distributed, or shared with any third parties without the express written permission of Parlour Development. By proceeding to review this report, the recipient acknowledges and agrees to the terms and limitations as outlined above.

# CONTACT

## Security Contact

support@robohero.io

## Auditor Contact


contact@parlour.dev

t.me/parlourdev

/parlourdev


parlour
[development]