



SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Monster Warriors
\$MWAR

22/01/2022

TABLE OF CONTENTS

- 1 DISCLAIMER
- 2 INTRODUCTION
- 3-4 WEBSITE DIAGNOSTIC
- 5-6 AUDIT OVERVIEW
- 7 OWNER PRIVILEGES
- 8 CONCLUSION AND ANALYSIS
- 9 TOKEN DETAILS
- 10 MONSTER WARRIORS TOKEN DISTRIBUTION &
TOP 10 TOKEN HOLDERS
- 11 TECHNICAL DISCLAIMER



DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website <https://freshcoins.io>

FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeygot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by **Monster Warriors** (Customer) to conduct a Smart Contract Code Review and Security Analysis.

0xb94BA16907D365Ff5a6D9993CDa6a32009872581

Network: **Binance Smart Chain (BSC)**

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on **22/01/2022**



WEBSITE DIAGNOSTIC

<https://monsterwarrior.net/>



0-49



50-89



90-100



Performance



Accessibility



Best
Practices



SEO



Progressive
Web App

Metrics



First Contentful Paint

2.2 s



Time to interactive

3.2 s



Speed Index

5.7 s



Total Blocking Time

570 ms



Large Contentful Paint

4.2 s



Cumulative Layout Shift

0.081

WEBSITE IMPROVEMENTS

Reduce initial server response time

Reduce unused JavaScript

Image elements do not have explicit **width** and **height**

Background and foreground colors do not have a sufficient contrast ratio.

Reduce JavaScript execution time **2.3 s**

AUDIT OVERVIEW



Security Score



Static Scan

Automatic scanning for common vulnerabilities



ERC Scan

Automatic checks for ERC's conformance



High



Medium



Low



Optimizations



Informational



No.	Issue description	Checking Status
1	Compiler Errors / Warnings	Passed
2	Reentrancy and Cross-function	Passed
3	Front running	Passed
4	Timestamp dependence	Passed
5	Integer Overflow and Underflow	Passed
6	Reverted DoS	Passed
7	DoS with block gas limit	Passed
8	Methods execution permissions	Passed
9	Exchange rate impact	Passed
10	Malicious Event	Passed
11	Scoping and Declarations	Passed
12	Uninitialized storage pointers	Passed
13	Design Logic	Passed
14	Safe Zeppelin module	Passed

OWNER PRIVILEGES

Contract owner can't mint tokens after initial contract deploy.

Contract owner can't disable trading.

Contract owner can't exclude an address from transactions.

Contract owner can't set / change buy & sell taxes.

Contract owner can't change swap settings.

Contract owner can't change tx amount.



CONCLUSION AND ANALYSIS



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



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



Found no issue during the first review.

TOKEN DETAILS

Details

Buy fees: 0%

Sell fees: 0%

Max TX: N/A

Max Sell: N/A

Honeypot Risk

Ownership: Owned

Blacklist: Not detected

Modify Max TX: Not detected

Modify Max Sell: Not detected

Disable Trading: Not detected

Rug Pull Risk

Liquidity: N/A

Holders: Clean



MONSTER WARRIORS TOKEN DISTRIBUTION & TOP 10 TOKEN HOLDERS



Rank	Address	Quantity (Token)	Percentage
1	0x37437ec15b3e342ff97269733653bec8f013bf6b	100,000,000	100.0000%

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. The audit can't guarantee the explicit security of the audited project / smart contract.

