soken

SMART CONTRACT
SECURITY AUDIT

MEDABOTS

February, 2022

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws. We took into consideration smart contract based algorithms, as well. Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it. Before making any judgments, you have to conduct your own independent research. We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report. Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills). The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
- Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
- Hashes of all transaction will be recorded
- Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
- Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
- In this phase intended behaviour of smart contract is verified.
- In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
- Gas limits of functions will be verified in this stage.

4. Automated Testing:
- Mythril
- Oyente
- Manticore
- Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Token Contract Details for 10.02.2022

Contract Name: **MedamonERC20**

Deployed address: **0xAf93908f5F8D66B50E11d7dE06f688DdE373C0cC**

Total Supply: **80,000,000**

Token Tracker: **MON**

Decimals: **18**

Token holders: **519**

Transactions count: **2079**

Top 100 holders dominance: **94.10%**

Audit Details

Project Name: **MEDABOTS**

Language: **Solidity**

Compiler Version: **v0.8.4**

Blockchain: **BSC**

Social Profiles

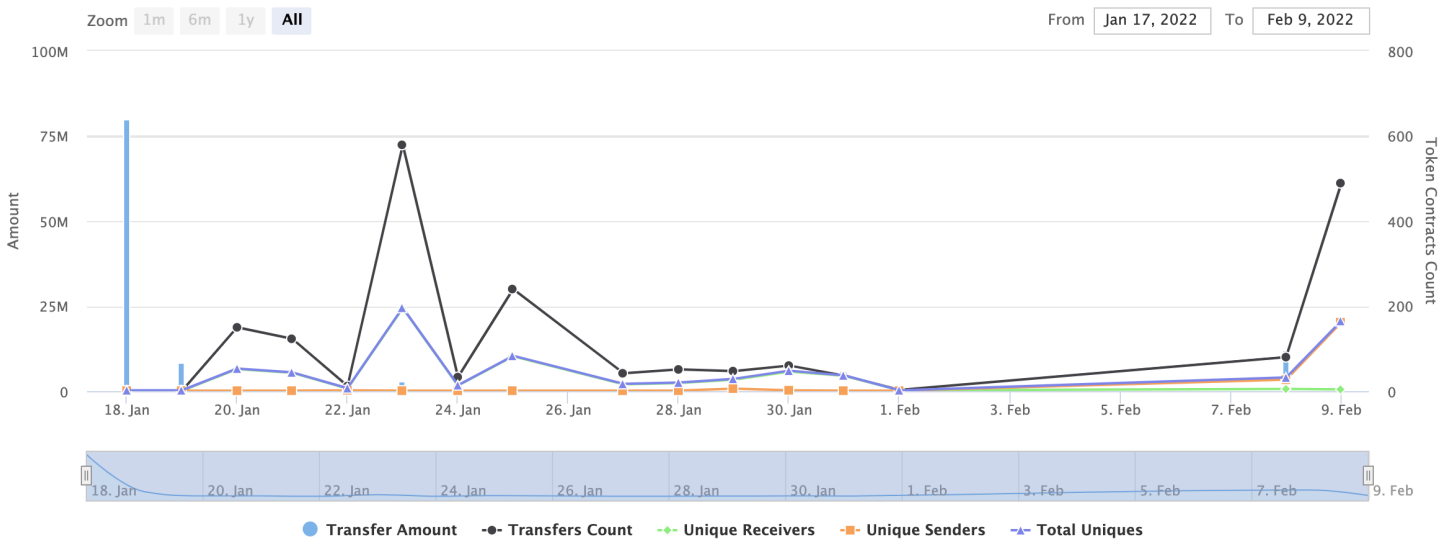
Project Website: **https://www.medabots.game/**

Project Twitter: **https://twitter.com/Medabotsworld**

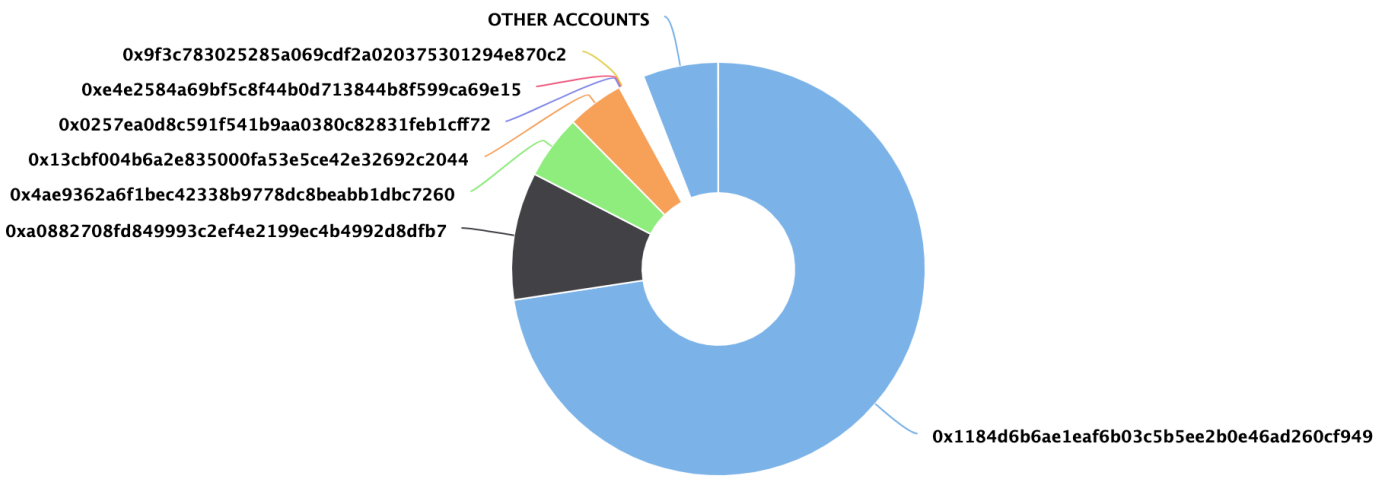
Project Telegram: **https://t.me/MedabotsOfficialChannel**

Project Instagram: **https://www.instagram.com/medabots_official/**

Contract Analytics



MON Token Distribution



MON Top Holders

Rank	Address	Quantity (Token)	Percentage
1	0x1184d6b6ae1eaf6b03c5b5ee2b0e46ad260cf949	58,081,168	72.6015%
2	0xa0882708fd849993c2ef4e2199ec4b4992d8dfb7	8,000,000	10.0000%
3	0x4ae9362a6f1bec42338b9778dc8beabb1dbc7260	4,000,000	5.0000%
4	0x13cbf004b6a2e835000fa53e5ce42e32692c2044	3,569,394.7519632	4.4617%
5	0x0257ea0d8c591f541b9aa0380c82831feb1cff72	82,469.5178984	0.1031%
6	0xe4e2584a69bf5c8f44b0d713844b8f599ca69e15	82,469.5178984	0.1031%
7	0x9f3c783025285a069cdf2a020375301294e870c2	30,723	0.0384%
8	0x76c58dd801933bb418e70359fc911a9b8902f02a	15,400	0.0193%
9	0xa49f2cc0638fdeaf3012c4c92b3997f95eda5cc6	15,400	0.0193%
10	0xa323829471ff0ccb74b0159684912ea264d30981	15,400	0.0193%

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Owner Privileges

The contract contains ownership functionality and ownership is not renounced which allows the creator or current owner to modify contract behaviour (for example, disable selling or mint new tokens)

Conclusion

Low-severity issues exist within smart contracts. Smart contracts are free from any critical or high-severity issues.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability.

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team