OXSCANS

Request

AI Generated at 04:37 PM, UTC

February 10, 2024

OVERVIEW

This audit has been perpared for 'Request' to review the main aspects of the project to help investors make an informative decision during their research process

You will find a summarized review of the following key points:

- Contract's source code
- Owner wallets
- Tokenomics
- Team transparency and goals
- Website's age, code, security and UX
- Whitepaper and roadmap
- Social media and online presence

Table of Content

General Information

Request

A decentralized network built on top of Ethereum, which allows anyone, anywhere to request a payment.

Name	**Request**
Direction	**Business Services** **Polygon Ecosystem** **Gnosis Chain Ecosystem** **Ethereum Ecosystem**
Info	Website Telegram Bot Docs Twitter

General Information

Tokenomics

Ticker	REQ
Deployed	October 07, 2017
Network	ethereum
Contract Address	0x8f8221afbb33998d8584a2b05749ba73c37a938a

General Analysis

Audit Review Process

1. Testing the smart contracts against both common and uncommon vulnerabilities
2. Assessing the codebase to ensure compliance with current best practices and industry standards
3. Ensuring contract logic meets the specifications and intentions of the client
4. Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders
5. Thorough line-byline AI review of the entire codebase by industry

Token Transfer Stats

Transactions (Latest Mine Block)	Token holders	Compiler
1	42687	v0.4.15

Smart Contract Stats

Functions	Events	Constructor
19	4	1

Detail Analysis

Threat Level

● High — Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment

● Medium — Issues on this level are critical to the smart contract's performace/functionality and should be fixed before moving to a live enviroment

● Low — Issues on this level are minor details and warning that can remain unfixed

● Informational — Informational level is to offer suggestions for improvement of efficacy or secruity for fratures with risk free factor

Threat Level

● High	5 threats found
● Medium	1 threats found
● Low	1 threats found
● Informational	1 threats found

Detail Analysis

Vulnerability Check

🟢 14 Passed 🔴 7 Fail

- 🟢 Arbitrary Jump/Storage Write
- 🔴 Centralization of Control
- 🟢 Compiler Issues
- 🟢 Delegate Call to Untrusted Contract
- 🔴 Dependence on Predictable Variables
- 🟢 Ether/Token Theft
- 🟢 Flash Loans
- 🔴 Front Running
- 🟢 Improper Events
- 🔴 Improper Authorization Scheme
- 🟢 Integer Over/Underflow
- 🟢 Logical Issues
- 🟢 Oracle Issues
- 🔴 Outdated Compiler Version
- 🟢 Race Conditions
- 🟢 Reentrancy
- 🟢 Signature Issues
- 🟢 Sybil Attack
- 🟢 Unbounded Loops
- 🔴 Unused Code
- 🔴 Overall Contract Safety

Detail Analysis

Detail Analysis 🟢 14 Passed 🔴 7 Fail

CATEGORY	STATUS	NOTES
Arbitrary Jump/Storage Write	🟢	No arbitrary jumps or storage writes detected.
Centralization of Control	🔴	Contract has central control by owner, posing risks of unilateral actions.
Compiler Issues	🟢	Compiled with a known version of Solidity without known compiler issues.
Delegate Call to Untrusted Contract	🟢	No delegate calls to untrusted contracts present.
Dependence on Predictable Variables	🔴	Some functions depend on predictable variables (e.g., block.timestamp).

Detail Analysis

Detail Analysis

🟢 14 Passed 🔴 7 Fail

CATEGORY	STATUS	NOTES
Ether/Token Theft	🟢	No apparent vulnerabilities leading to Ether/token theft.
Flash Loans	🟢	No flash loan functions present.
Front Running	🔴	Susceptible to front-running attacks due to external calls.
Improper Events	🟢	All events are properly declared and emitted.
Improper Authorization Scheme	🔴	Authorization scheme is over-reliant on the owner, increasing centralization risk.
Integer Over/Underflow	🟢	SafeMath library used, mitigating integer overflow/underflow.

Detail Analysis

Detail Analysis 🟢 14 Passed 🔴 7 Fail

CATEGORY	STATUS	NOTES
Logical Issues	🟢	No logical inconsistencies or issues detected.
Oracle Issues	🟢	Contract does not use oracles.
Outdated Compiler Version	🔴	Uses an outdated compiler version, potential for unknown vulnerabilities.
Race Conditions	🟢	No race conditions detected.
Reentrancy	🟢	No reentrancy vulnerabilities found.
Signature Issues	🟢	No signature-related functions that could be exploited.

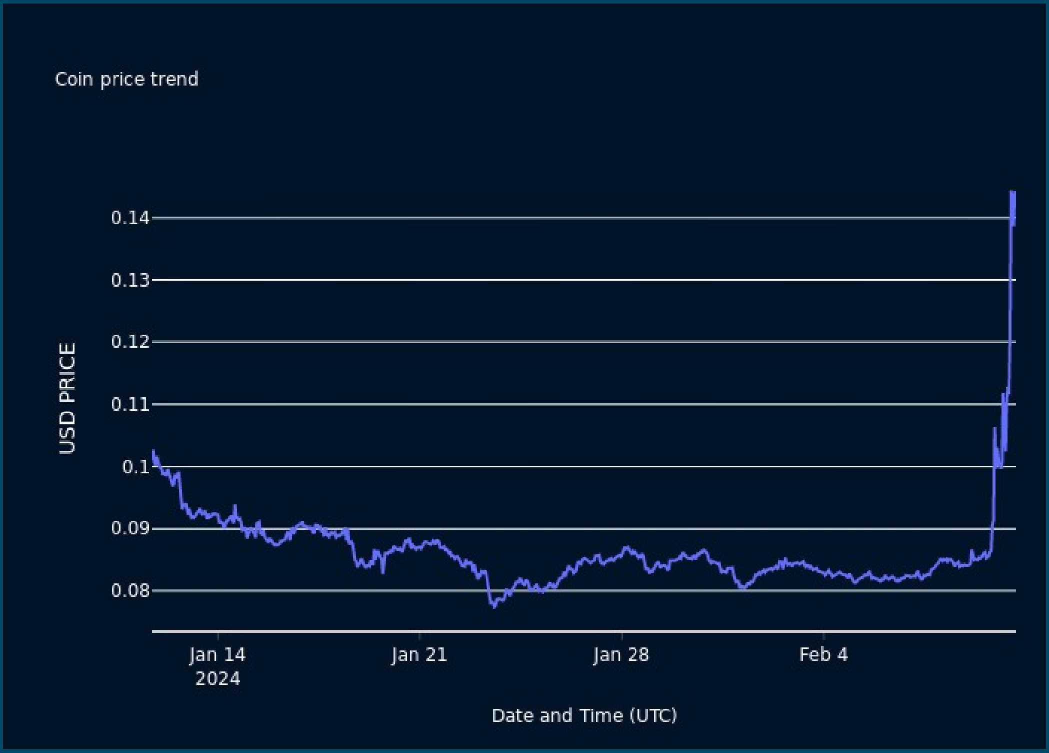
Detail Analysis

Detail Analysis

🟢 14 Passed 🔴 7 Fail

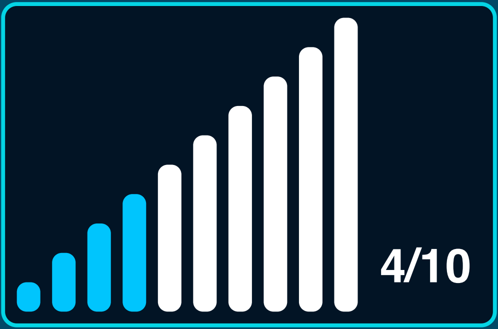
CATEGORY	STATUS	NOTES
Sybil Attack	🟢	No functionalities susceptible to Sybil attacks.
Unbounded Loops	🟢	No unbounded loops that could lead to gas limit issues.
Unused Code	🔴	Contains unused or redundant code, which increases attack surface unnecessarily.
Overall Contract Safety	🔴	Contract has some vulnerabilities, particularly in centralization and outdated compiler version.

Market Analysis

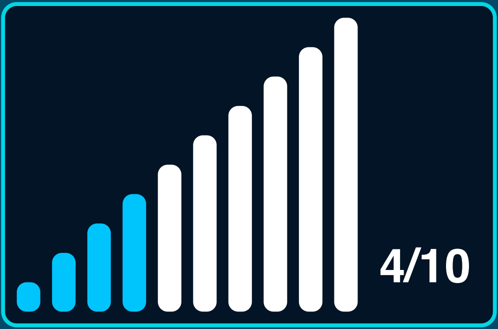


Score

Total Audit Score


4/10

Security Score


4/10

Legal Disclaimer

0xscans operates as an automated system for smart contract due diligence, acknowledging the possibility of bugs or vulnerabilities impacting token values. We do not hold specific obligations regarding your trading outcomes or the utilization of audit content. Users release 0xscans from any liability associated with content obtained through the tool.

AI generated by 0xscans AI technology

Chat with us

Telegram

For more information. Visit below:

Twitter

Github