Orange
Cyberdefense

Poundtoken.io

Smart Contract Source Code Review

Date	**2022-05-18**

1 Executive Summary

1.1 Assessment Overview

The source code review of Poundtoken.io smart contracts commenced on the 11th of April 2022 and concluded on the 5th of May 2022.

Poundtoken.io engaged the services of Orange Cyberdefense to:

- Evaluate whether security requirements and best practices were followed during the development and deployment of the in-scope smart contracts.
- Gauge whether the risk identified was at a level acceptable to the organisation and that such risk would not have a significant business impact, expose clients to harm or loss, or other such consequences.

1.1.1 Risk Summary

The overall information security risk rating was calculated as: **Informational**

This is based on the following statistics:

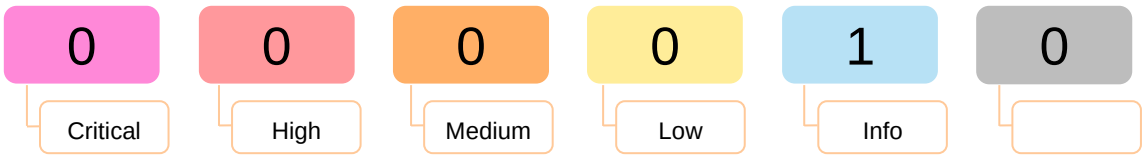

Table 1 – Risk Summary. See Appendix A.2 for the Qualitative Severity Rating Scale (QSR).

1.2 Qualitative Severity Rating Summary

Critical QSR: Such attacks could have a catastrophic impact on the confidentiality, integrity and availability of the systems and the business. This could result in a significant financial loss, significant reputational damage, serious legal and compliance-related fines, and other effects on the business.

High QSR: Such attacks could have a significant impact on the confidentiality, integrity and availability of the systems and the business. This could result in a significant financial loss, significant reputational damage, serious legal and compliance-related fines, and other effects on the business.

Medium QSR: Such attacks could have a noticeable impact on the confidentiality, integrity and availability of the systems and the business, which could result in a noticeable financial loss, considerable reputational damage, legal and compliance-related fines, and other effects on the business.

Low QSR: Such attacks are unlikely to have a noticeable impact on the business. However, such issues do not exist in isolation. An attacker may use them as part of more complicated, blended attack.

Info QSR: Such attacks have no direct impact on the business. However, such issues do not exist in isolation. An attacker may use them as part of more complicated, blended attack.

1.3 Smart Contracts Health

The overall security of the assessed smart contracts. It provides an overview of how easily they were compromised and what information was accessed during the assessment. For a more detailed analysis, please make contact with Poundtoken.io.

How easy was it to compromise the smart contracts?	The smart contracts were not compromised. issues of lower severity were identified.
What would be the impact of the compromise?	This could potentially have negative consequences; however, a direct security risk could not be identified.

1.4 Conclusion and Recommendations

Overall, the security posture of the assessed smart contracts followed several industry best practices. This included the use of the security focused OpenZeppelin[1] smart contracts, and the implementation of role-based access control.

[1] https://www.openzeppelin.com/contracts

The following strategic recommendations have been determined based on an interpretation of the results identified during the project:

Business Area	Strategic Recommendations
Software Development	Security should be addressed from the start of a project, right through design and development, and finally during deployment. Integrating security processes into development processes will reduce the number of vulnerabilities present in the final solution, and sometimes reduce costly redesign work. Numerous methodologies exist to assist with this and can be consulted. Additionally, developers should receive security training to better assist with securing applications.
Multiple Reviews	Due to the public nature of Ethereum, smart contracts are under significant risk of attack, especially when doing so would provide attackers with a financial benefit. Various platforms implementing smart contracts such as crypto exchanges and stable coins have been subject to attacks, resulting in significant financial loss. It is thus recommended that upmost scrutiny be applied before deploying smart contracts to the public Ethereum blockchain. Poundtoken.io should consider conducting multiple audits of the smart contracts by vendors specialising in smart contract review, to identify any possible security issues.
Access Control	Significant care should be applied when assigning access control roles to addresses, to avoid an attacker obtaining privileged access. It is highly recommended that any administrative functionality to the environment be scrutinised. The use of multi-signature wallets is recommended, to implement granular control over transactions and administrative actions.

2 Project Summary

2.1 Assessment Scope

Orange Cyberdefense was tasked with performing a source code review against Poundtoken.io smart contracts. This commenced on the 11th of April 2022 and concluded on the 5th of May 2022. The assessment followed the Orange Cyberdefense methodologies.

The targets included during the assessment were:

Scope
A source code review of the smart contracts was requested, including the following key test areas: • Unintentionally exposed public functions • Authorisation • Authentication • Configuration management • Smart contract-specific vulnerabilities, such as re-entrancy and arithmetic flaws.

2.2 Assessment Timeline

Table 5 provides a breakdown of the timeline of the assessment.

Date	Activity
2022-04-11 – 2022-04-25	Familiarisation with Ethereum, Solidity, Hardhat, OpenZeppelin, smart contracts and their security vulnerabilities.
2022-04-26 – 2022-05-04	Familiarisation and manual review of the Poundtoken.io smart contracts' source code, and the identification of potential vulnerabilities.
2022-05-05	Data collation and report generation.

2.4 Assessment Process

A manual source code review of the smart contracts was performed to identify any potential security vulnerabilities. Specifically, each contract was reviewed to identity if any of the following issues were present:

- Unintentionally exposed public functions
- A lack of authorization of authentication checks
- Smart contract-specific flaws as specified by DASP[2]
- Re-entrancy attacks
- Arithmetic errors
- Entropy issues
- External contract calling issues
- Front Running
- Potential DOS conditions
- Block Timestamp dependence
- Uninitialized variables
- The use of unsafe variables and functions

To augment the manual source code review, the automated semgrep[3], slither[4] and mithril[5] source code scanners were employed.

3 Findings Summary

One security issue was identified during the assessment and has been classified as an:

- Informational risk.

Appendix A. Risk Rating System

Appendix A.1. CVSS3: An Open Standard for Vulnerability Scoring

The Common Vulnerability Scoring System (version 3) is an established method for scoring technical vulnerabilities identified in systems.

The CVSS3 is based on three metric groups:

- **Base Metric Group**: “represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.” It covers metrics relating to the complexity (proximity of attacker, authentication requirements) of the attack and its impact on the security qualities of the system (confidentiality, integrity, and availability).
- **Temporal Metric Group**: “represents the characteristics of a vulnerability that change over time but not among user environments.” It covers metrics relating to the current state of the vulnerability (exploitability and remediation options) and to the confidence of the issue at hand.
- **Environmental Metric Group**: “represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment”. These metrics allow Poundtoken.io to ensure that the controls in place are factored into the assessment of the vulnerability’s actual relationship with the environment, leading to a more accurate representation of the technical risk.

During an assessment, only the base metric group is calculated for each vulnerability. By request, and provided with additional information, the temporal and environmental metric groups can be calculated.

For further information on the CVSS3 system, see the following reference site:

http://www.first.org/cvss/user-guide