SMART CONTRACTS REVIEW

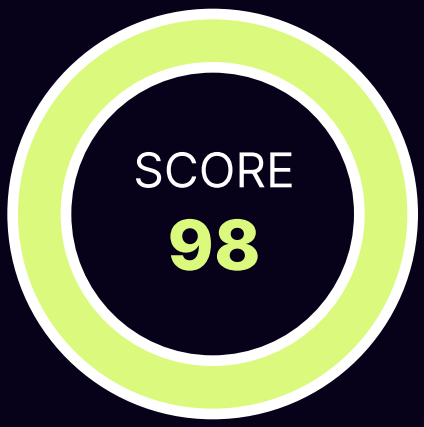
zokyo

July 12th 2024 | v. 1.0

Security Audit Score

PASS

Zokyo Security has concluded that this smart contract passed a security audit.



ZOKYO AUDIT SCORING GPT360

1. Severity of Issues:
    - Critical: Direct, immediate risks to funds or the integrity of the contract. Typically, these would have a very high weight.
    - High: Important issues that can compromise the contract in certain scenarios.
    - Medium: Issues that might not pose immediate threats but represent significant deviations from best practices.
    - Low: Smaller issues that might not pose security risks but are still noteworthy.
    - Informational: Generally, observations or suggestions that don't point to vulnerabilities but can be improvements or best practices.
2. Test Coverage: The percentage of the codebase that's covered by tests. High test coverage often suggests thorough testing practices and can increase the score.
3. Code Quality: This is more subjective, but contracts that follow best practices, are well-commented, and show good organization might receive higher scores.
4. Documentation: Comprehensive and clear documentation might improve the score, as it shows thoroughness.
5. Consistency: Consistency in coding patterns, naming, etc., can also factor into the score.
6. Response to Identified Issues: Some audits might consider how quickly and effectively the team responds to identified issues.

HYPOTHETICAL SCORING CALCULATION:

Let's assume each issue has a weight:
- Critical: -30 points
- High: -20 points
- Medium: -10 points
- Low: -5 points
- Informational: -1 point

Starting with a perfect score of 100:
- 0 Critical issues: 0 points deducted
- 0 High issues:0 points deducted
- 0 Medium issues:0 points deducted
- 1 Low issue: 1 acknowledged = -2 points deducted
- 1 Informational issue: 1 resolved = 0 points deducted

Thus, 100 - 2 = 98

TECHNICAL SUMMARY

This document outlines the overall security of the GPT360 smart contract/s evaluated by the Zokyo Security team.

The scope of this audit was to analyze and document the GPT360 smart contract/s codebase for quality, security, and correctness.

Contract Status

There were 0 critical issues found during the review. (See Complete Analysis)

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract/s but rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that can withstand the Ethereum network's fast-paced and rapidly changing environment, we recommend that the GPT360 team put in place a bug bounty program to encourage further active analysis of the smart contract/s.

Table of Contents

AUDITING STRATEGY AND TECHNIQUES APPLIED

The source code of the smart contract was taken from the GPT360 repository:
Repo: https://github.com/GPT360/Contracts
Token address - https://bscscan.com/address/0×25134680375c9Ee5b95F3dB514eB450E608549a6#code

Fixes - https://bscscan.com/address/0×26AdAfCcD3D37Fef1Eaec90A78668DECA8610028#code

Within the scope of this audit, the team of auditors reviewed the following contract(s):

- Gpt360TokenOneChain.sol

During the audit, Zokyo Security ensured that the contract:

- Implements and adheres to the existing standards appropriately and effectively;
- The documentation and code comments match the logic and behavior;
- Distributes tokens in a manner that matches calculations;
- Follows best practices, efficiently using resources without unnecessary waste;
- Uses methods safe from reentrance attacks;
- Is not affected by the most recent vulnerabilities;
- Meets best practices in code readability, etc.

Zokyo Security has followed best practices and industry-standard techniques to verify the implementation of GPT360 smart contract/s. To do so, the code was reviewed line by line by our smart contract developers, who documented even minor issues as they were discovered. In summary, our strategies consist largely of manual collaboration between multiple team members at each stage of the review:

01 Due diligence in assessing the overall code quality of the codebase.

02 Cross-comparison with other, similar smart contract/s by industry leaders.

03 Thorough manual review of the codebase line by line.

Executive Summary

The Zokyo team has performed a security audit of the provided codebase. The contracts submitted for auditing are well-crafted and organized. Detailed findings from the audit process are outlined in the "Complete Analysis" section.

GPT360, is a pioneering platform that stands at the forefront of integrating the dynamic world of Web3 with the expansive reach of Web2. At its core, GPT360 is designed to serve as a superApp, offering an extensive suite of tools and features that cater to the diverse needs of Web3 project owners and enthusiasts alike.

The Gpt360Token contract is an ERC20-compliant token, utilizing the ERC20Burnable extension. This contract mints 500 million tokens (with a custom decimal setting of 9) to the deployer's address upon initialization. The name and symbol for the token are "G360" and "G360" respectively. The custom decimal setting is different from the standard 18 decimals. Additionally, the burnable feature enables token holders to reduce the total supply by burning their tokens.

STRUCTURE AND ORGANIZATION OF THE DOCUMENT

For the ease of navigation, the following sections are arranged from the most to the least critical ones. Issues are tagged as “Resolved” or “Unresolved” or “Acknowledged” depending on whether they have been fixed or addressed. Acknowledged means that the issue was sent to the GPT360 team and the GPT360 team is aware of it, but they have chosen to not solve it. The issues that are tagged as “Verified” contain unclear or suspicious functionality that either needs explanation from the Client or remains disregarded by the Client. Furthermore, the severity of each issue is written as assessed by the risk of exploitation or other unexpected or otherwise unsafe behavior:

Critical

The issue affects the contract in such a way that funds may be lost, allocated incorrectly, or otherwise result in a significant loss.

High

The issue affects the ability of the contract to compile or operate in a significant way.

Medium

The issue affects the ability of the contract to operate in a way that doesn’t significantly hinder its behavior.

Low

The issue has minimal impact on the contract’s ability to operate.

Informational

The issue has no impact on the contract’s ability to operate.

COMPLETE ANALYSIS

FINDINGS SUMMARY

#	Title	Risk	Status
1	Centralization Risk Due to Whole Total Supply Minted to One Wallet	Low	Acknowledged
2	Floating Pragma	Informational	Resolved

LOW-1 | RESOLVED

Centralization Risk Due to Whole Total Supply Minted to One Wallet

On deployment, the entire total supply of the token is minted to a single wallet. This poses a centralization risk as it gives one wallet complete control over the entire asset. This concentration of power can lead to trust issues and potential misuse of tokens.

Recommendation:
To mitigate this centralization risk, consider transferring the tokens to a multisig wallet, which requires multiple approvals for transactions, thereby distributing the control. Additionally, implementing a vesting schedule for the tokens would ensure that not all tokens are available for use immediately, which can help in maintaining stability and reducing risks associated with large, single-point control.

Client comment: tokens will get locked closer to IDO and vested accordingly

INFORMATIONAL-1 | RESOLVED

Floating Pragma

The `Gpt360TokenOneChain.sol` smart contract uses a floating pragma version `(^0.8.0)`. Contracts should be deployed using the same compiler version and settings as were used during development and testing. Locking the pragma version helps ensure that contracts are not inadvertently deployed with a different compiler version.

Recommendation:
Consider locking the pragma version to a specific, tested version to ensure consistent compilation and behavior of the smart contract.

	Gpt360TokenOneChain.sol
Reentrance	Pass
Access Management Hierarchy	Pass
Arithmetic Over/Under Flows	Pass
Unexpected Ether	Pass
Delegatecall	Pass
Default Public Visibility	Pass
Hidden Malicious Code	Pass
Entropy Illusion (Lack of Randomness)	Pass
External Contract Referencing	Pass
Short Address/ Parameter Attack	Pass
Unchecked CALL Return Values	Pass
Race Conditions / Front Running	Pass
General Denial Of Service (DOS)	Pass
Uninitialized Storage Pointers	Pass
Floating Points and Precision	Pass
Tx.Origin Authentication	Pass
Signatures Replay	Pass
Pool Asset Security (backdoors in the underlying ERC-20)	Pass

We are grateful for the opportunity to work with the GPT360 team.

The statements made in this document should not be interpreted as an investment or legal advice, nor should its authors be held accountable for the decisions made based on them.

Zokyo Security recommends the GPT360 team put in place a bug bounty program to encourage further analysis of the smart contract by third parties.

zokyo