GORDIAN AGENCY

SMART CONTRACT SECURITY AUDIT

December 7th, 2021

Professional Auditing Agency

Website https://gordian.agency/

AUDIT DETAILS

GORDIAN AGENCY

Project

Bomb Money

Deployer Address

0x0DCC098Fa701906a49c3196B1FD2464F4802F4E2

Client Contacts

@BombMoneyBSC
https://t.me/bombmoneybsc

Blockchain

Binance Smart Chain

Project Website

https://app.bomb.money/

BACKGROUND

GORDIAN AGENCY

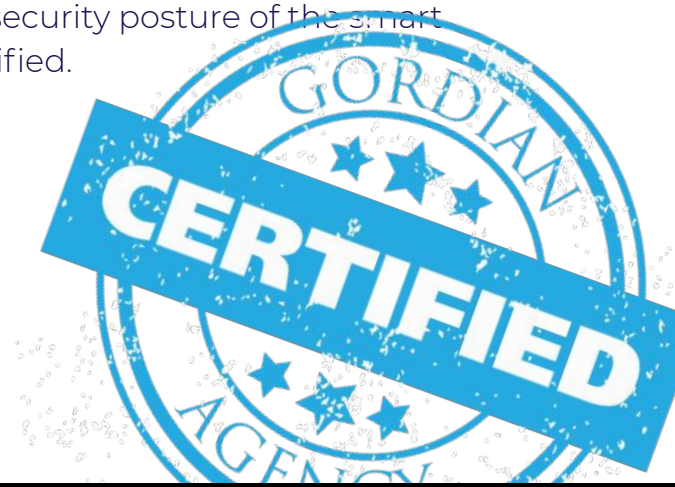
Gordian Agency was commissioned by Bomb Money to perform an audit of smart contracts:

- BBond
- BShare
- Boardroom
- Bomb
- BombGenesisRewardPool
- BombRewardPool
- BShareRewardPool
- Distributor
- DummyToken
- Oracle
- SimpleERCFund
- TaxOffice
- TaxOfficeV2
- TaxOracle
- Timelock
- Treasury
- Zap

The purpose of this audit was to achieve the following:

- Ensure that the token contract functions as intended
- Identify potential security issues with the token contracts
- Provide a code peer review

The information in this report should be used to understand the risk exposure of the smart contracts, and as a guide to improve the security posture of the smart contracts by remediating the issues that were identified.



CONTRACT DETAILS

GORDIAN AGENCY

Bomb Money Smart Contract Details

Bomb money is a full fork of Tomb finance project on Fantom network. Tomb finance is a highly successful project, with TVL in hundreds of millions USD, trusted by many users. The key difference is the pegging mechanism - unlike Tomb finance, bomb money is pegged to BTC and not FTM. The contracts have modified names. Other amendments were to do with a different commission structure and a different pegging mechanism that required a different degree of precision in token price estimations.

THREAT ASSESSMENT

GORDIAN AGENCY

EXTERNAL THREAT RESULTS

Vulnerability Category	Notes	Result
Arbitrary Storage Write	N/A	PASS
Arbitrary Jump	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Deprecated Opcodes	N/A	PASS
Ether Thief	N/A	PASS
Exceptions	N/A	PASS
External Calls	N/A	PASS
Integer Over/Underflow	N/A	PASS
Multiple Sends	N/A	PASS
Suicide	N/A	PASS
State Change External Calls	N/A	PASS
Unchecked Retval	N/A	PASS
User Supplied Assertion	N/A	PASS
Critical Solidity Compiler	N/A	PASS
Overall Contract Safety	N/A	PASS

Bomb Money optimization suggestions

For all contracts
non-view external and public methods should returns boolean execution status to improve interaction between the contracts

BShare.sol
communityFundRewardRate - should be a public constant, because it calculates inside the ***constructor*** using only public constants

devFundRewardRate - should be a public constant, because it calculates inside the ***constructor*** using only public constants

Treasury.sol
bombPriceOne - should be a public constant, because it's hardcoded in the ***initialize*** function

bombPriceCeiling - should be a public constant, because it's calculates using bombPriceOne and hardcoded values in the ***initialize*** function

CONCLUSION

The audited contract contains no issues and is safe to deploy.

NOTES:

Please check the disclaimer below and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is solely provided for the contracts mentioned in the report and does not include any other potential contracts deployed by the Owner.

DISCLAIMER

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Gordian and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Gordian) owe no duty of care towards you or any other person, nor does Gordian make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Gordian hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, Gordian hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Gordian, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.