



Smart contracts security assessment

Final report

Tariff: Standard

Hexther Finance

January 2022



0xguard.com



hello@0xguard.com

Contents

1. Introduction	3
2. Contracts checked	3
3. Procedure	3
4. Classification of issue severity	4
5. Issues	4
6. Conclusion	6
7. Disclaimer	7

Introduction

The report has been prepared for the Hexther Finance team. The project website is <https://hexther.finance>. The audited project is a fork of the Tomb Finance Project. The purpose of the audit was to ensure that no issues were introduced with the changes to the original code and that known vulnerabilities (e.g. [circumventing](#) the protocol's fee system) are fixed.

Name	Hexther Finance
Audit date	2022-01-24 - 2022-01-24
Language	Solidity
Platform	Binance Smart Chain

Contracts checked

Name	Address
Oracle	0xbdEA123bE01D63b79e59cBbCcea4005587d84F3e
HexBond	0xb84e6aa0AafA54cD4DA2e220B99a711c9D21a010
Hexther	0x12E0D9E59c6b218F4c43DA7b1ce8d8ef889d62be
HexGate	0xF390635070876A2b4d8E26112c6668479AD243D3
HexSharesRewardPool	0x405C55dB91891B3828f3388FFF3dd4570D8D16fc
HexShares	0x21BA6D5b10ded5E4b86A87c09F35841773776Fd6
Treasury	0xC61D3AbBa8D6405364Ca158E8dc2aCfc4166E337

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Comparing the project to the Tomb Finance implementation

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

No issues were found

Medium severity issues

No issues were found

Low severity issues

No issues were found

Conclusion

The Hexther Finance Project was compared with the Tomb Project. Hexther Finance has changed the implementation of Treasury contract.

The Token contract is affected by the vulnerability that was discovered in the Tomb Project.

In the contract Treasury removed the array of pools excludedFromTotalSupply.

No serious issues were found in the audited changes.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without 0xGuard prior written consent.

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts 0xGuard to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.



 Guard