



BlockApex

SMART CONTRACT SECURITY ANALYSIS REPORT

```
pragma solidity 0.7.0;
contract Contract {

    function hello() public returns (string) {
        return "Hello World!";
    }

    function findVulnerability() public returns (string) {
        return "Finding Vulnerability";
    }

    function solveVulnerability() public returns (string) {
        return "Solve Vulnerability";
    }
}
```



Powered by XORD

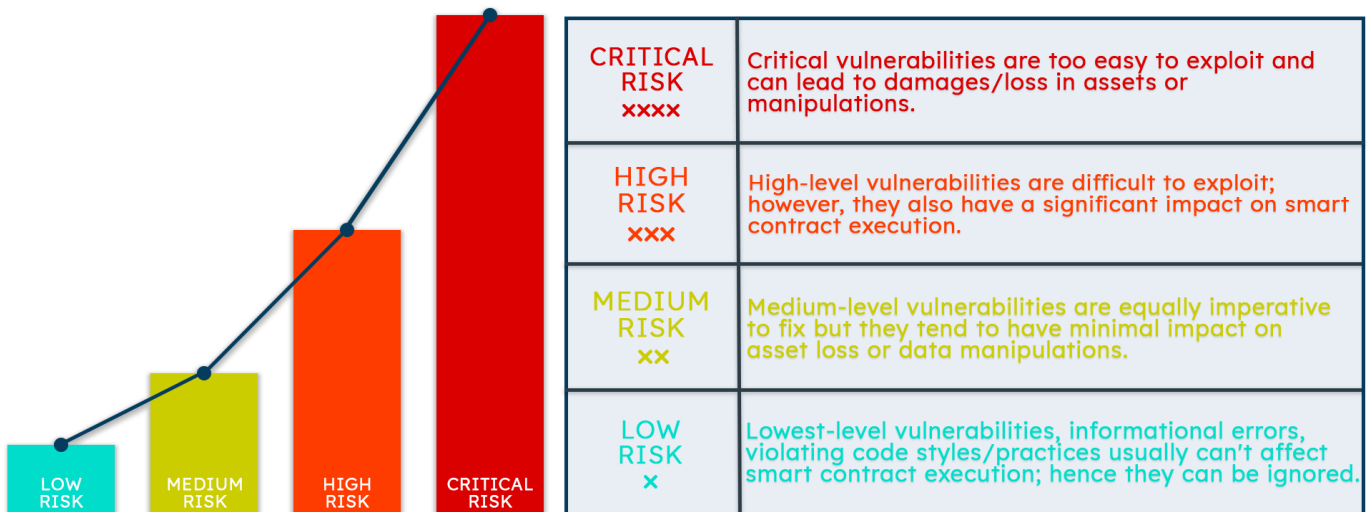
PREFACE

Objectives

The purpose of this document is to highlight the identified bugs/issues in the provided codebase. This audit has been conducted in a closed and secure environment, free from influence or bias of any sort. This document may contain confidential information about IT systems/architecture and intellectual property of the client. It also contains information about potential risks and the processes involved in mitigating/exploiting the risks mentioned below.

The usage of information provided in this report is limited, internally, to the client. However, this report can be disclosed publicly with the intention to aid our growing blockchain community; under the discretion of the client.

Key understandings



The contents of this document are proprietary and highly confidential. Information from this document should not be extracted/disclosed in any form to a third party without the prior written consent of BlockApex.

[BlockApex | Fortifying The Move Towards Decentralization](#)

Table of Contents

PREFACE	2
Objectives	2
Key understandings	2
INTRODUCTION	4
Project details	4
Scope	5
AUDIT REPORT	6
Executive Summary	6
Findings	7
Critical-risk issues	7
High-risk issues	7
Medium-risk issues	7
Low-risk issues	7
Informatory issues	8
DISCLAIMER	9

INTRODUCTION

BlockApex (Auditor) was contracted by PhoenixDAO (Client) for the purpose of conducting a Smart Contract Audit/Code Review. This document presents the findings of our analysis which took place on 26th June 2021.

Project details

Name
PheonixDAO staking (Initial Audit)
Auditor
Moazzam Arif Shakeib Shaida
Platform
Ethereum/Solidity
Type of review
Staking
Methods
Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Git Repository
(insert git repo link for the contract)
Document log
Day 1: 26th June 2021 (Initial Audit)
Day 2: (Final Audit pending)



Scope

The git-repository shared was checked for common code violations along with vulnerability-specific probing to detect major issues/vulnerabilities. Some specific checks are as follows:

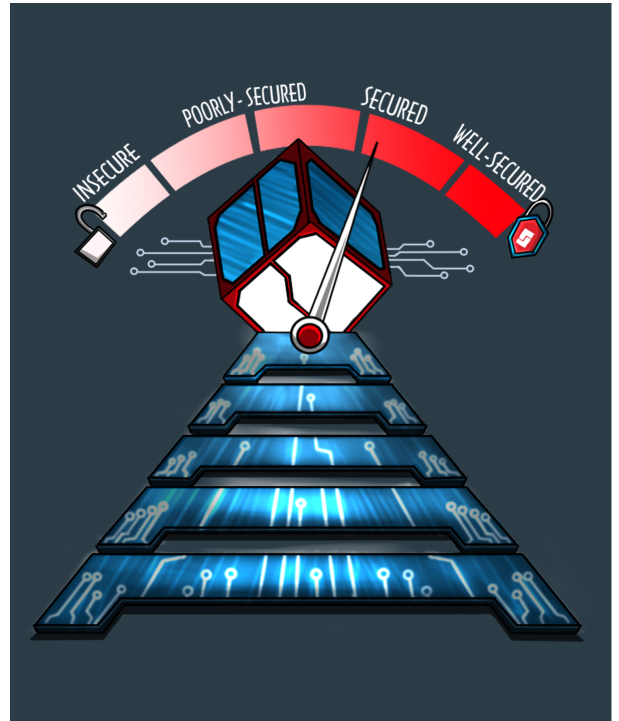
Code review		Functional review
Reentrancy	Unchecked external call	Business Logics Review
Ownership Takeover	ERC20 API violation	Functionality Checks
Timestamp Dependence	Unchecked math	Access Control & Authorization
Gas Limit and Loops	Unsafe type inference	Escrow manipulation
DoS with (Unexpected) Throw	Implicit visibility level	Token Supply manipulation
DoS with Block Gas Limit	Deployment Consistency	Asset's integrity
Transaction-Ordering Dependence	Repository Consistency	User Balances manipulation
Style guide violation	Data Consistency	Kill-Switch Mechanism
Costly Loop		Operation Trails & Event Generation

AUDIT REPORT

Executive Summary

The analysis indicates that the contracts audited are **secure** (with some low severity issues).

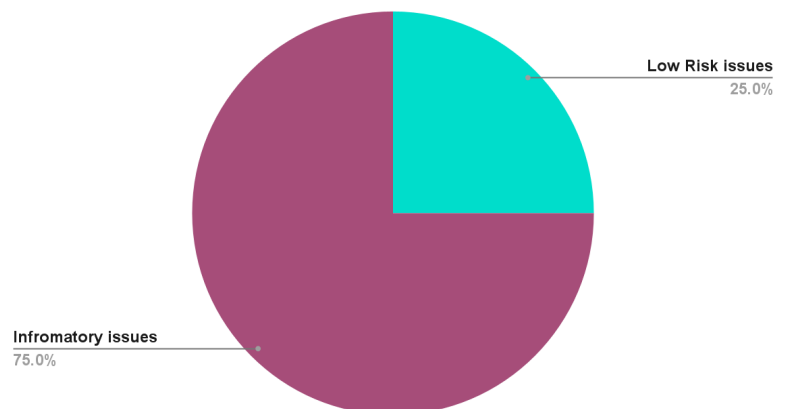
Our team performed a technique called “Filtered Audit”, where the contract was separately audited by two individuals. After their thorough and rigorous process of manual testing, an automated review was carried out using Mythril, MythX and Slither. All the flags raised were manually reviewed and re-tested.



Our team found:

# of issues	Severity of the risk
0	Critical Risk issue
0	High Risk issue
0	Medium Risk issue
1	Low Risk issue
3	Informatory issues

Proportion of Vulnerabilities





Findings

Critical-risk issues

No issues found

High-risk issues

No issues found

Medium-risk issues

No issues found

Low-risk issues

1. Precision Error

ONE_DAY is used in calculating remaining days. If a user wants to unstake before the durationTimeStamp (in StakerData Struct) then he/she will bear a burn fee. Here is the code for the remaining days.

```
uint256 _remainingDays = (  
    stakerData[_expiredTimestamps[i]]  
        .durationTimestamp  
        .add(_expiredTimestamps[i])  
        .sub(block.timestamp)  
)  
    .div(ONE_DAY);
```

Attack Scenario:

If a user stakes for ONE_DAY, and unstake immediately (before ONE_DAY, he/she will not have to pay the burn fee). Let's put some values in the above code for better understanding

```
uint256 durationTimeStamp = ONE_DAY; (86400)

uint256 initiationTimeStamp = 1624872985 (06/28/2021 @ 9:36am)
// if user unstake in next second i.e block,timestamp =
1624872986, then
uint256 remainingDays = (1624872985 + 86400 -
624872986)/86400 return 0
```

Remedy:

Timestamps should be used instead of ONE_DAY

Informatory issues

1. Floating pragma versions.
2. Zero-address check missing while setting the phoenix token contract address.
3. There is a **rug-pull** indicator function withDrawToken allows the owner to pull all funds (whitepaper/documentation was not provided).

DISCLAIMER

The smart contracts provided by the client for audit purposes have been thoroughly analyzed in compliance with the global best practices till date w.r.t cybersecurity vulnerabilities and issues in smart contract code, the details of which are enclosed in this report.

This report is not an endorsement or indictment of the project or team, and they do not in any way guarantee the security of the particular object in context. This report is not considered, and should not be interpreted as an influence, on the potential economics of the token, its sale or any other aspect of the project.

Crypto assets/tokens are results of the emerging blockchain technology in the domain of decentralized finance and they carry with them high levels of technical risk and uncertainty. No report provides any warranty or representation to any third-Party in any respect, including regarding the bug-free nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third-party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project.

Smart contracts are deployed and executed on a blockchain. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The scope of our review is limited to a review of



the Solidity code and only the Solidity code we note as being within the scope of our review within this report. The Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond Solidity that could present security risks.

This audit cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only - we recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.