

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: Seedify.Fund
Date: March 18th, 2021

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed - upon a decision of the Customer.

Document

Name	Smart Contract Code Review and Security Analysis Report for Seedify.Fund - Draft
Approved by	Andrew Matiukhin CTO Hacken OU
Type	Vesting
Platform	Ethereum / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Deployed contract	https://bscscan.com/address/0x477bc8d23c634c154061869478bce96be6045d12#code
Timeline	16 MARCH 2021 - 18 MARCH 2021
Changelog	18 MARCH 2021 - INITIAL AUDIT



Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	6
AS-IS overview	7
Conclusion	14
Disclaimers	15

Introduction

Hacken OÜ (Consultant) was contracted by Seedify.Fund (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on March 16th, 2021.

Scope

The scope of the project is smart contracts deployed in the Binance smart chain network:

Contract deployment address:

<https://bscscan.com/address/0x477bc8d23c634c154061869478bce96be6045d12#code>

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none">▪ Reentrancy▪ Ownership Takeover▪ Timestamp Dependence▪ Gas Limit and Loops▪ DoS with (Unexpected) Throw▪ DoS with Block Gas Limit▪ Transaction-Ordering Dependence▪ Style guide violation▪ Costly Loop▪ ERC20 API violation▪ Unchecked external call▪ Unchecked math▪ Unsafe type inference▪ Implicit visibility level▪ Deployment Consistency▪ Repository Consistency▪ Data Consistency

Functional review	<ul style="list-style-type: none"> ▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Asset's integrity ▪ User Balances manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation
-------------------	---

Executive Summary

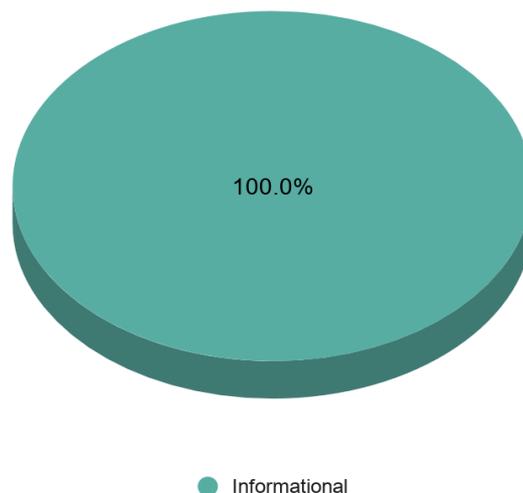
According to the assessment, the Customer's smart is Secured.



Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. A general overview is presented in AS-IS section, and all found issues can be found in the Audit overview section.

Security engineers found 3 informational issues during the first review.

Graph 1. The distribution of vulnerabilities after the first review.



Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations.
High	High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations.
Low	Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Audit overview

■ ■ ■ ■ Critical

No Critical severity issues were found.

■ ■ ■ High

No High severity issues were found.

■ ■ Medium

No Medium severity issues were found.

■ Lowest / Code style / Best Practice

1. Vulnerability: Incorrect versions of Solidity
Contract: InitializableERC20

Pragma version 0.6.9 is known to contain severe issues (check here: <https://solidity.readthedocs.io/en/latest/bugs.html>)
solc-0.6.9 is not recommended for deployment. Please consider using one of the:

- 0.6.8,
- 0.6.10 - 0.6.11

Line: #14

```
pragma solidity 0.6.9;
```

2. Vulnerability: Conformance to Solidity naming conventions
Contract: InitializableERC20

Solidity defines a naming convention that should be followed (<https://docs.soliditylang.org/en/v0.6.9/style-guide.html#naming-conventions>).

Lines: #90-96

```
function init(  
    address _creator,  
    uint256 _totalSupply,
```

```
    string memory _name,  
    string memory _symbol,  
    uint256 _decimals  
  ) public {
```

3. Vulnerability: Public function that could be declared external
Contract: InitializableERC20

public functions that are never called by the contract should be declared external to save gas.

Lines: #90-96

```
function init(  
    address _creator,  
    uint256 _totalSupply,  
    string memory _name,  
    string memory _symbol,  
    uint256 _decimals  
  ) public {
```

Line: #107

```
function transfer(address to, uint256 amount) public returns (bool) {
```

Line: #117

```
function balanceOf(address owner) public view returns (uint256 balance) {
```

Lines: #121-125

```
function transferFrom(  
    address from,  
    address to,  
    uint256 amount  
  ) public returns (bool) {
```

Line: #137

```
function approve(address spender, uint256 amount) public returns (bool) {
```

Line: #143

```
function allowance(address owner, address spender) public view returns  
(uint256) {
```

Conclusion

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. For the contract, high-level description of functionality was presented in As-Is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security engineers found 3 informational issues during the audit.

Category	Check Items	Comments
Code Review	Style guide violation	Incorrect versions of Solidity
		Conformance to Solidity naming conventions
		Public function that could be declared external



Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree 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.

Technical Disclaimer

Smart contracts are deployed and executed on blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. Thus, the audit can't guarantee the explicit security of the audited smart contracts.