HackSafe

Smart Contract Security Audit Report

FUNFI

June 2022

Security Status

★ ★ ★ ★ ★

www.hacksafe.io

Audit Details

Audited project
FUNFI

Deployer address
0x500E2F2450AD075cccef0Db3f4081D1aBeb2F73E

Client contacts
FUNFI team

Blockchain
Binance Smart Chain

Website
https://www.funfi.org/

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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe 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 HackSafe 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, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, 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.

Procedure

Step 1 - In-Depth Manual Review

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

Step 2 - Automated Testing

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

Step 3 – Leadership Review

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

Step 4 - Resolution of Issues

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

Step 5 - Published Audit Report

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

Background

HackSafe was commissioned by FUNFI to perform an audit of smart contracts:

- https://bscscan.com/address/0xad5dde288573162dfbcc3d7c5c7c648c609b0394#code

Contract Details

Token contract details for 04.06.2022

Contract name	: Token
Contract address	: 0xAd5dDe288573162dFBcC3D7C5c7C648c609b0394
Compiler version	: v0.8.2+commit.661d1103
Max Total supply	: 1,000,000,000,000
Token Ticker	: FNF
Decimals	: 18
Token Holders	: 6,597
Top 100 token holder's dominance	: 99.97%
Transactions count	: 8,538
Contract deployer address	: 0x500E2F2450AD075cccef0Db3f4081D1aBeb2F73E
owner address	: No Owner

Social profiles

CoinmarketCap profile	: https://coinmarketcap.com/currencies/funfi/
Twitter Profile	: https://twitter.com/Funfi_token
Telegram Profile	: https://t.me/FunfiOfficial
WhitePaper Link	: https://www.funfi.org/whitepaper

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics : • **Name** : FUNFI • **Symbol** : FNF • **Decimals** : 18 • **Total Supply** : 1,000,000,000	YES, this is valid. Tokenomics have maximum total supply of 1,000,000,000 but smart contract has 1,000,000,000,000 total supply. Smart contract should have said total supply.

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “**Secured**”. These Protocol contracts do contain owner control, which does not make it fully decentralized.

Insecure	Poor secured	Secure	Well-secured

You are here 

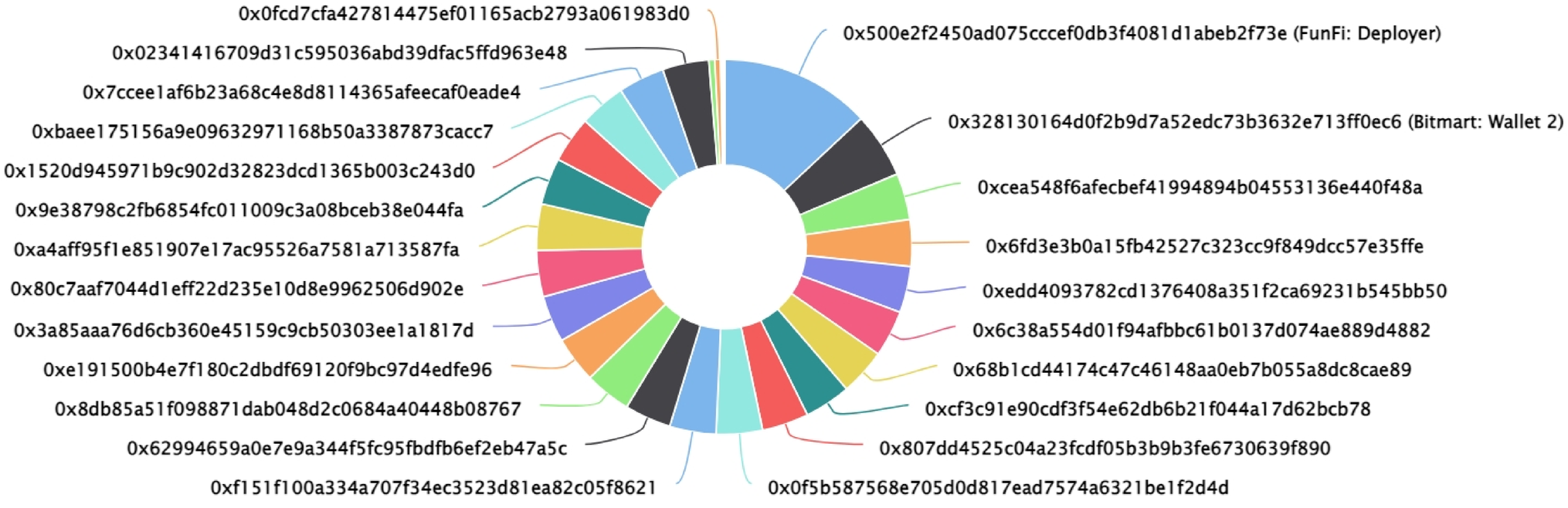
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 2 low and some very low level issues. These issues are not critical ones.

FUNFI Token Distribution

FunFi Top 500 Token Holders

Source: BscScan.com



FUNFI Token Distribution

FUNFI Top 20 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	FunFi: Deployer	130,327,437,499	13.0327%
2	Bitmart: Wallet 2	56,384,491,993	5.6384%
3	0xcea548f6afecbef41994894b04553136e440f48a	40,069,587,243.585528451350560816	4.0070%
4	0x6fd3e3b0a15fb42527c323cc9f849dcc57e35ffe	40,057,582,363.788175257732641803	4.0058%
5	0xedd4093782cd1376408a351f2ca69231b545bb50	40,050,862,356.515009591337127331	4.0051%
6	0x6c38a554d01f94afbbc61b0137d074ae889d4882	40,048,237,747.817164699990126029	4.0048%
7	0x68b1cd44174c47c46148aa0eb7b055a8dc8cae89	40,039,725,965.109220993710976661	4.0040%
8	0xcf3c91e90cdf3f54e62db6b21f044a17d62bcb78	40,032,864,108.725984112210598294	4.0033%
9	0x807dd4525c04a23fcdf05b3b9b3fe6730639f890	40,026,003,110.128598324550340664	4.0026%
10	0x0f5b587568e705d0d817ead7574a6321be1f2d4d	40,000,000,000	4.0000%
11	0xf151f100a334a707f34ec3523d81ea82c05f8621	40,000,000,000	4.0000%
12	0x62994659a0e7e9a344f5fc95fbdfb6ef2eb47a5c	40,000,000,000	4.0000%
13	0x8db85a51f098871dab048d2c0684a40448b08767	40,000,000,000	4.0000%
14	0xe191500b4e7f180c2dbdf69120f9bc97d4edfe96	40,000,000,000	4.0000%
15	0x3a85aaa76d6cb360e45159c9cb50303ee1a1817d	40,000,000,000	4.0000%
16	0x80c7aaf7044d1eff22d235e10d8e9962506d902e	40,000,000,000	4.0000%
17	0xa4aff95f1e851907e17ac95526a7581a713587fa	40,000,000,000	4.0000%
18	0x9e38798c2fb6854fc011009c3a08bceb38e044fa	40,000,000,000	4.0000%
19	0x1520d945971b9c902d32823dcd1365b003c243d0	40,000,000,000	4.0000%
20	0xbaee175156a9e09632971168b50a3387873cacc7	39,982,376,754.103885466922617767	3.9982%

FUNFI Token Distribution

FUNFI Contract overview

Contract functions details

+Token

-<constructor> #

- [Pub] balanceOf

- [Pub] transfer #

- [Pub] transferFrom #

- [Pub] approve #

($) = payable function

= non-constant function

Issues Checking Status

No.	Title	Status
1.	Unlocked Compiler Version	Low issue
2.	Missing Input Validation	Passed
3.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
4.	Possible delays in data delivery	Passed
5.	Oracle calls.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Passed
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	Private use data leaks.	Passed
13.	Malicious Event log.	Passed
14.	Scoping and Declarations.	Passed
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Passed
18.	Safe Open Zeppelin contracts implementation and usage.	Passed
19.	Incorrect Naming State Variable	Passed

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.

Security Issues

- **Critical Severity Issues**
  No critical severity issue found.

- **High Severity Issues**
  No high severity issue found.

- **Medium Severity Issues**
  No medium severity issues found.

- **Low Severity Issues**
  One low severity issue found.

1. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.8.2 the contract should contain the following line:

  pragma solidity 0.8.2;

Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

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