



Smart Contract Security Audit Report

SOAR FI

April 2022

Security Status



www.hacksafe.io



Audit Details



Audited project

SOAR FI



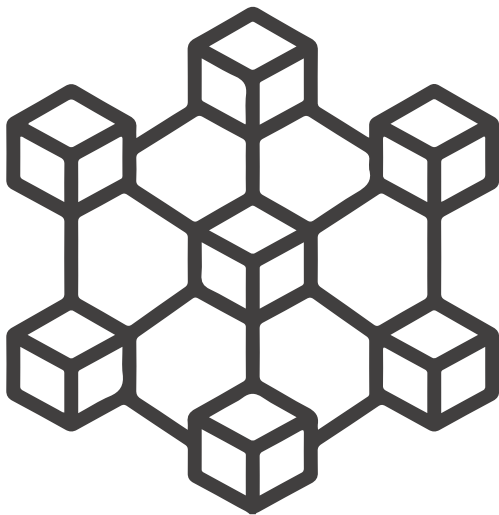
Deployer address

0x401C51Ebe418D2809921565e606B60851bACE4Ec



Client contacts

SOAR FI team



Blockchain

Ethereum



Website

www.soar.fi

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.

Background

HeckSafe was commissioned by Soar Fi to perform an audit of smart contracts:

- <https://etherscan.io/address/0xbae5f2d8a1299e5c4963eaff3312399253f27ccb#code>

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issue with the smart contract.

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

Contracts Details

Token contract details for 13.04.2022

Contract name	: SOAR FI
Contract address	: 0xbae5f2d8a1299e5c4963eaff3312399253f27ccb
Total supply	: 10, 000, 000
Token Ticker	: SOAR
Decimals	: 9
Network	: Ethereum
Transactions count	: 13,352
Token Holders	: 1701 addresses
Contract deployer address	: 0x401C51Ebe418D2809921565e606B60851bACE4Ec
Owner address	: 0x401C51Ebe418D2809921565e606B60851bACE4Ec

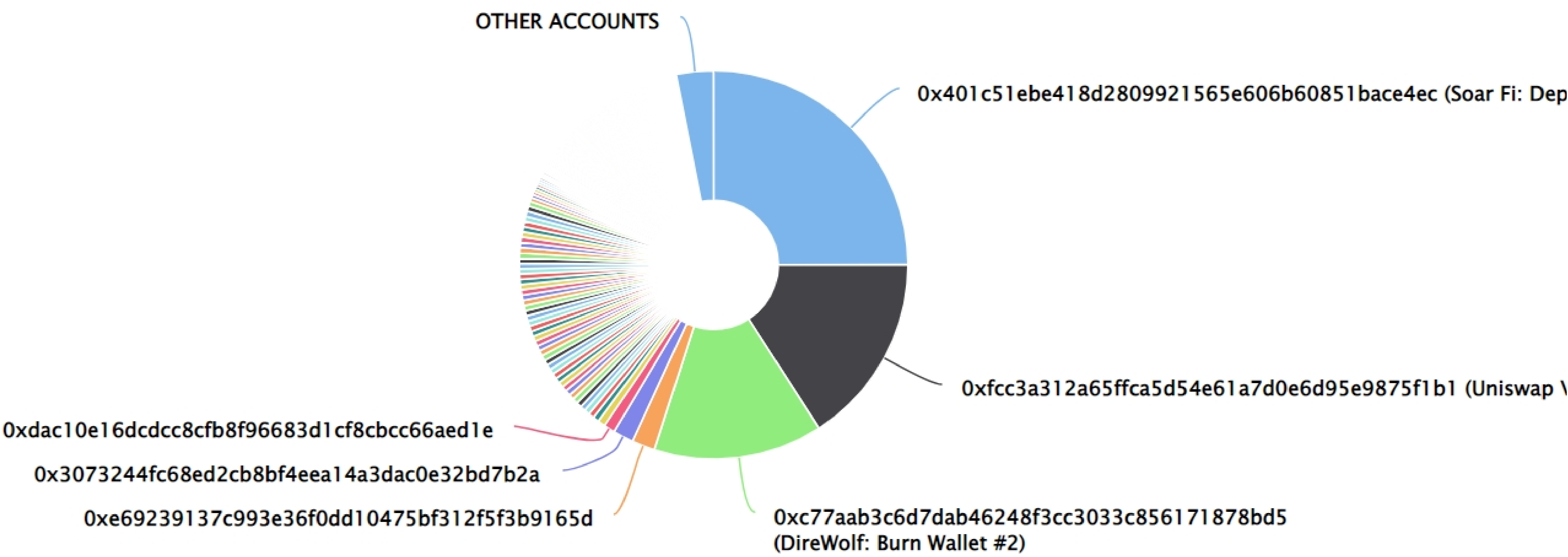
SOAR FI Token Distribution

The top 500 holders collectively own 96.90% (9,689,758.13 Tokens) of SOAR.FI

💡 Token Total Supply: 10,000,000.00 Token | Total Token Holders: 1,



SOAR.FI Top 500 Token Holders

Source: Etherscan.io



Soar FI Top 10 Token Holders

(A total of 6,156,960.73 tokens held by the top 10 accounts from the total supply of 10,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	Soar Fi: Deployer	2,499,799.344148156	24.9980%
2	 Uniswap V2: SOAR	1,589,465.439626868	15.8947%
3	 DireWolf: Burn Wallet #2	1,407,737.142963991	14.0774%
4	0xe69239137c993e36f0dd10475bf312f5f3b9165d	191,944.532164713	1.9194%
5	0x3073244fc68ed2cb8bf4eea14a3dac0e32bd7b2a	169,914.376899912	1.6991%
6	0xdac10e16dcdcc8cfb8f96683d1cf8cbcc66aed1e	93,269.646486993	0.9327%
7	0x5bfce71a1909b4525156290a8fa61af0f723ab4b	61,221.665393474	0.6122%
8	0xcce02df050d8b4045997b458f9af9fe1c45d6fd4	51,550.340455921	0.5155%
9	0xaac8fac303b573bfb5156265b743aad166f4e4b	46,828.62586922	0.4683%
10	0x60e9d91ca34a26497720707e93c9cc1900af497c	45,229.61268126	0.4523%

Contract functions details

+ Context

- [Int] _msgSender
- [Int] _msgData

+ [Int] IERC20

- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] sub
- [Int] mul
- [Int] div
- [Int] div
- [Int] mod
- [Int] mod

+ [Lib] Address

- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue
- [Pvt] _functionCallWithValue

+ Ownable (Context)

- [Int] <constructor> #
- [Pub] owner
- [Pub] renounceOwnership
 - Modifier: onlyOwner
- [Pub] transferOwnership
 - Modifier: onlyOwner

Contract functions details

+ SOAR (Context, IERC20, Ownable)

-[Pub] <constructor> #

-[Pub] name

-[Pub] symbol

-[Pub] decimals

-[Pub] totalSupply

-[Pub] balanceOf

-[Pub] transfer

-[Pub] allowance

-[Pub] approve

-[Pub] transferFrom

-[Pub] increaseAllowance

-[Pub] decreaseAllowance

-[Pub] isExcluded

-[Pub] totalFees

-[Pub] reflect

-[Pub] reflectionFromToken

-[Pub] tokenFromReflection

-[Ext] excludeAccount

-Modifier: onlyOwner

-[Ext] includeAccount

-Modifier: onlyOwner

-[Pvt] _approve

-[Pvt] _transfer

-[Pvt] _transferStandard

-[Pvt] _transferToExcluded

-[Pvt] _transferFromExcluded

-[Pvt] _transferBothExcluded

-[Pvt] _reflectFee

-[Pvt] _getValues

-[Pvt] _getTValues

-[Pvt] _getRValues

-[Pvt] _getRate

-[Pvt] _getCurrentSupply

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.	Low issue
15.	Uninitialized storage pointers.	Passed
16.	Arithmetic accuracy.	Passed
17.	Design Logic.	Low issue
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 issue found.

✔ Low Severity Issues

Three 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 v0.6.2 the contract should contain the following line:

```
pragma solidity 0.6.2;
```

2. Scoping and Declarations.

Unused function.

- **Description**

The `_msgData`, `sendValue`, `functionCall`, `functionCallWithValue`, `_functionCallWithValue`, `mod` function does nothing.

- **Location**

Line no: 24, 238, 254, 308, 334, 344, 359, 369, 374.

- **Recommendation**

We advise to remove unused code.

3. Design Logic.

- **Description**

Default condition is unreachable for all ifs in transfer.

- **Location**

Transfer function.

- **Recommendation**

We advise to have 3 if..else checks and the default should be standard transfer. It may potentially save some gas.

Owner Privileges

Owner Privileges (in the period when the owner is not renounced) :

- SOAR FI Contract:
 - Owner can renounce ownership.
 - Owner can transfer ownership.
 - Owner can exclude account for fee.
 - Owner can include account for fee.

Conclusion

Smart contract contains low severity issues!

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.