

# SMART CONTRACT AUDIT

SECURITY ANALYSIS REPORT  
FOR

**beFITTER**

July 12th, 2022

# Security Rating



The rating is based on the number, severity and latest status of detected issues

**beFITTER**

## Disclaimer

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

SecuriChain does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed.

The report in no way provides investment advice, nor should be leveraged as investment advice of any sort.

# TABLE OF CONTENTS

## 1. VULNERABILITY ASSESSMENT OVERVIEW

- 1.1 Assigning risk levels
- 1.2 Scope of work
- 1.3 Checksum File
- 1.4 Assessment results

## 2. DETAILED RESULTS

## 3. CONCLUSION

- Appendix 1. Assessment list
- Appendix 2. Risk rating

# VULNERABILITY ASSESSMENT OVERVIEW

## 1.1. ASSIGNING RISK LEVELS

The Auditor categorizes each of the detected vulnerabilities into 4 levels (High, Medium, Low, and Info) according to the degree of the risks it may cause in the Customer's operations. For details of the rating standards, please refer to "Appendix 2 Risk Rating." Please also note that the assessment of the findings is based on Auditor's own perspective and may contain speculations in some cases.

## 1.2. SCOPE OF WORK

<b>Project Name</b>	<b>beFITTER Token (FIU)</b>
<b>Platform</b>	<b>BSC</b>
<b>Languages</b>	<b>Solidity</b>
<b>Methods</b>	<b>Automation scan, architecture review, functional testing, manual code review</b>
<b>Scope</b>	<b><a href="https://bscscan.com/address/0xef7d50069406a2f5a53806f7250a6c0f17ad9dcd#code">https://bscscan.com/address/0xef7d50069406a2f5a53806f7250a6c0f17ad9dcd#code</a></b>
<b>Documents</b>	<b>No</b>
<b>Timelines</b>	<b>July 11th - July 12th, 2022</b>

**beFITTER**

## 1.3. CHECKSUM FILE

### SCOPE

No.	Contract Address	Name
1	0xef7d50069406a2f5a53806f7250a6c0f17ad9dcd	beFITTER.sol

**beFITTER**





## 1.4. ASSESSMENT RESULTS

According to the assessment, the Customer's smart contracts have a security rating of 100/100

RATE	DESCRIPTION
96-100	<b>No vulnerabilities</b> were found or all detected ones have been resolved
70-95	Unresolved <b>Low-level</b> vulnerabilities exist
40-69	Unresolved <b>Medium-level</b> vulnerabilities exist
0-39	Unresolved <b>High-level</b> vulnerabilities exist



For more information on criteria for risk rating, refer to Appendix.2



## DETAILED RESULTS

**No vulnerabilities were found**



For rating each vulnerability,  
refer to Appendix 2.



## CONCLUSION

This document, and its appendices, represent our best effort to capture the results of several days of intensive activity.

Smart contracts within the scope were analyzed with static analysis tools and manually reviewed.

Please feel free to direct any questions on this assessment to:  
[audit@securichain.io](mailto:audit@securichain.io)

## APPENDIX 1: ASSESSMENT LIST

	CHECKLIST	
	Integer Overflow/Underflow	Integer Overflow/Underflow
<b>Arithmetic operations</b>	Integer Truncation	Integer Sign
	Wrong Operator	
<b>Re-entrancy</b>		
<b>Bad Randomness</b>	Timestamp Dependence	Blockhash
<b>Front running</b>		
<b>DDos</b>	DOS By Complex Fallback Function	DOS By Gaslimit
	DOS By Non-existent Address Or Malicious Contract	
<b>Gas usage</b>	Invariants in Loop	Invariants State Variables Are Not Declared Constant
<b>Unsafe external calls</b>		
<b>Business Logics Review</b>		
<b>Access Control &amp; Authorization</b>	Replay Attack	Use tx.origin For Authentication
<b>Logic Vulnerability</b>		

## APPENDIX 2: LIST RATING

Risk Level	Explain	Example Types
High	The issue puts a large number of users' sensitive information at risk, or is reasonably likely to lead to catastrophic impact for client's reputation or serious financial implications for client and users.	Re-entrancy Front running DDos Bad Randomness Logic Vulnerability Arithmetic operations
Medium	The issue puts a subset of users' sensitive information at risk, would be detrimental for the client's reputation if exploited, or is reasonably likely to lead to moderate financial impact.	Access Control Unsafe external calls Business Logics Review Logic Vulnerability
Low	The risk is relatively small and could not be exploited on a recurring basis, or is a risk that the client has indicated is low impact in view of the client's business circumstances.	Gas Usage
Info	The issue does not pose an immediate risk, but is relevant to security best practices or Defense in Depth.	Blockhash