SECURICHAIN

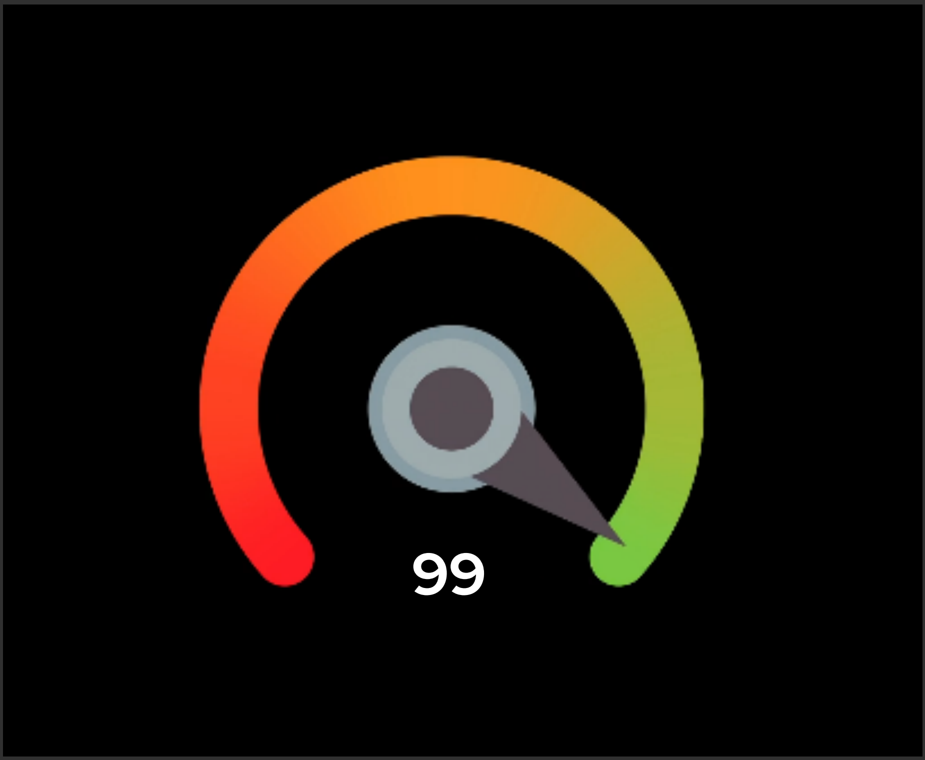
SMART CONTRACT AUDIT

SECURITY ANALYSIS REPORT FOR

BLOCKCHAIN FOOTBALL

July 1st , 2022

Security Rating



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

Blockchain Football

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.

SECURICHAIN

TABLE OF CONTENTS

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

Project Name	Blockchain Football
Platform	Polygon
Languages	Solidity
Methods	Automation scan, architecture review, functional testing, manual code review
Repository	tokens.zip
Documents	Blockchain Football (BFB) - Whitepaper.pdf; TokenSpecifications.pdf
Timelines	June 30th - July 1st, 2022

1.3. CHECKSUM FILE

SCOPE

No.	Hash	Name
1	1e2629250662e988a01a7bdd3d8b19b0a730d7d3	BFBToken.sol
2	7c5662be27e1b131cb713b01f0c66a3dde1a35c3	GoalToken.sol

1.4. ASSESSMENT RESULTS

According to the assessment, the Customer's smart contracts have a security rating of 99/100

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

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

FINDINGS

2.1 List of Vulnerabilities

The detected vulnerabilities are listed below. Please refer to "Appendix.2 Risk Rating" for the risk assessment method.

Vulnerabilities distributed in the smart contract

ID	Risk Level	Name	Amount	Status
SC1	Low	Unlocked Pragma	1	Acknowledged

For rating each vulnerability, refer to Appendix 2.

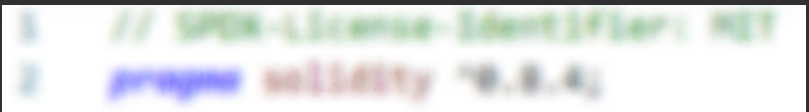
2.1 Details

[1] Unlocked Pragma

Information: 1

Overview

Contracts should be deployed with the same compiler version and flags that they have been thoroughly tested.
Locking the pragma helps to ensure that contracts do not accidentally get deployed using.



```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.4;
```

(Blurred image of the code snippet in the public report due to the Customer's code being in the private repository)

Possible Impacts

An outdated compiler version might introduce bugs affecting the contract system negatively.

Recommendation

Lock the pragma version and also consider known bugs (https://github.com/ethereum/solidity/releases) for the chosen compiler version.
Pragma statements can be allowed to float when a contract is intended for consumption by other developers, as in the case of contracts in a library or EthPM package. Otherwise, the developer would need to manually update the pragma to compile it locally.

Location

BlockchainFootball:: All Contracts

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

SECURICHAIN

APPENDIX 1: ASSESSMENT LIST

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

SECURICHAIN

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