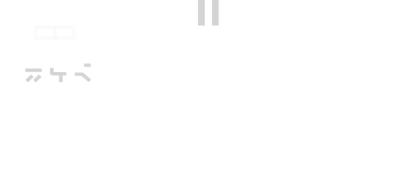


SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Customer: Cookies

Date: April 12, 2023



This report 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 can be disclosed publicly after prior consent by another Party. Any subsequent publication of this report shall be without mandatory consent.

Document

Name	Smart Contract Code Review and Security Analysis Report for Cookies		
Approved By	Marcin Ugarenko Lead Solidity SC Auditor at Hacken OU		
Туре	ERC20 token;		
Platform	EVM		
Language	Solidity		
Methodology	<u>Link</u>		
Website	https://nexusderby.com/		
Changelog	12.04.2023 - Initial Review		



Table of contents

Introduction	4
Scope	4
Severity Definitions	5
Executive Summary	6
Risks	7
System Overview	8
Checked Items	9
Findings	12
Critical	12
High	12
Medium	12
Low	12
L01. Floating Pragma	12
Disclaimers	13



Introduction

Hacken OÜ (Consultant) was contracted by Cookies (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report presents the findings of the security assessment of the Customer's smart contracts.

Scope

The scope of the project includes the following smart contracts from the provided repository:

Initial review scope

Repository	https://github.com/GotBit/TjayToken		
Commit	20e5bc28a995592c08b8568415dec26bc6b2a8e1		
Functional Requirements	Nexus Derby.pdf		
Contracts	File: ./contracts/Token.sol SHA3: fbc4c3eb4bde277deaecda278e45ec11e4b32530e6ad20aaa7e6332bbba27b77		



Severity Definitions

Risk Level	Description		
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to the loss of user funds or contract state manipulation by external or internal actors.		
High	High vulnerabilities are usually harder to exploit, requiring specific conditions, or have a more limited scope, but can still lead to the loss of user funds or contract state manipulation by external or internal actors.		
Medium	Medium vulnerabilities are usually limited to state manipulations but cannot lead to asset loss. Major deviations from best practices are also in this category.		
Low	Low vulnerabilities are related to outdated and unused code or minor Gas optimization. These issues won't have a significant impact on code execution but affect code quality		



Executive Summary

The score measurement details can be found in the corresponding section of the <u>scoring methodology</u>.

Documentation quality

The total Documentation Quality score is 10 out of 10.

• Functional requirements are provided.

Code quality

The total Code Quality score is 10 out of 10.

Environment is configured.

Test coverage

Code coverage of the project is 100% (branch coverage).

• Tests are provided.

Security score

As a result of the audit, the code contains 1 low severity issue. The security score is 10 out of 10.

All found issues are displayed in the "Findings" section.

Summary

According to the assessment, the Customer's smart contract has the following score: 10. The system users should acknowledge all the risks summed up in the risks section of the report.

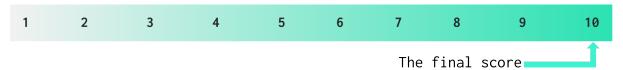


Table. The distribution of issues during the audit

Review date	Low	Medium	High	Critical
12 April 2023	1	0	0	0



Risks

• All the tokens are minted to a specific address.



System Overview

Token — simple ERC-20 token that mints all of its initial supply and sends it to a specific address. Additional minting is not allowed. It has the following attributes:

• Name: Specified in the constructor (name)

• Symbol: Specified in the constructor (symbol)

• Decimals: 18 (inherited from the ERC20 standard)

• Total supply: 2,100,000,000 tokens



Checked Items

We have audited the Customers' smart contracts for commonly known and specific vulnerabilities. Here are some items considered:

Item	Туре	Description	Status
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	Passed
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	Not Relevant
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	Passed
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	Failed
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	Not Relevant
Access Control & Authorization	CWE-284	Ownership takeover should not be possible. All crucial functions should be protected. Users could not affect data that belongs to other users.	Passed
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	Not Relevant
Check-Effect- Interaction	SWC-107	Check-Effect-Interaction pattern should be followed if the code performs ANY external call.	Passed
Assert Violation	SWC-110	Properly functioning code should never reach a failing assert statement.	Passed
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	Passed
Delegatecall to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	Not Relevant
DoS (Denial of Service)	SWC-113 SWC-128	Execution of the code should never be blocked by a specific contract state unless required.	Passed



Race Conditions SWC-114 Race Conditions and Transactions Order Dependency should not be possible. Passed Lace Conditions and Transactions Order Dependency should not be possible. Lace Conditions order Dependency should not be used for authorization. Not Relevant SWC-115 Block values as a proxy for time calculations. Not Relevant
through tx.origin Block values as a proxy for SWC-116 SWC-116 Block numbers should not be used for time calculations. Not Relevant Not Relevant
as a proxy for SWC-116 time calculations. Not Relevant
Signature Unique Id SWC-121 SWC-122 EIP-155 EIP-712 Signed messages should always have a unique id. A transaction hash should not be used as a unique id. Chain identifiers should always be used. All parameters from the signature should be used in signer recovery. EIP-712 should be followed during a signer verification. Not Relevant
Shadowing State Variable SWC-119 State variables should not be shadowed. Passed
Weak Sources of RandomnessSWC-120Random values should never be generated from Chain Attributes or be predictable.Not Relevant
Incorrect Inheritance Order When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. Not Relevant
Calls Only to Trusted Addresses EEA-Lev
Presence of Unused Variables The code should not contain unused variables if this is not justified by design. Passed
EIP Standards Violation EIP standards should not be violated. Not Relevant
Assets Integrity Custom Funds are protected and cannot be withdrawn without proper permissions or be locked on the contract. Not Relevant
User Balances Manipulation Custom Contract owners or any other third party should not be able to access funds belonging to users. Not Relevant



Flashloan Attack	Custom	When working with exchange rates, they should be received from a trusted source and not be vulnerable to short-term rate changes that can be achieved by using flash loans. Oracles should be used.	Not Relevant
Token Supply Manipulation	Custom	Tokens can be minted only according to rules specified in a whitepaper or any other documentation provided by the Customer.	Not Relevant
Gas Limit and Loops	Custom	Transaction execution costs should not depend dramatically on the amount of data stored on the contract. There should not be any cases when execution fails due to the block Gas limit.	Not Relevant
Style Guide Violation	Custom	Style guides and best practices should be followed.	Passed
Requirements Compliance	Custom	The code should be compliant with the requirements provided by the Customer.	Passed
Environment Consistency	Custom	The project should contain a configured development environment with a comprehensive description of how to compile, build and deploy the code.	Passed
Secure Oracles Usage	Custom	The code should have the ability to pause specific data feeds that it relies on. This should be done to protect a contract from compromised oracles.	Not Relevant
Tests Coverage	Custom	The code should be covered with unit tests. Test coverage should be sufficient, with both negative and positive cases covered. Usage of contracts by multiple users should be tested.	Passed
Stable Imports	Custom	The code should not reference draft contracts, which may be changed in the future.	Passed



Findings

Critical

No critical severity issues were found.

High

No high severity issues were found.

Medium

No medium severity issues were found.

Low

L01. Floating Pragma

The project uses floating pragmas ^0.8.0.

This may result in the contracts being deployed using the wrong pragma version, which is different from the one they were tested with. For example, they might be deployed using an outdated pragma version which may include bugs that affect the system negatively.

Path: ./contracts/Token.sol;

Recommendation: Consider locking the pragma version whenever possible and avoid using a floating pragma in the final deployment. Consider known bugs (https://github.com/ethereum/solidity/releases) for the compiler version that is chosen.

Found in: c9000f0

Status: New



Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed based on best industry practices at the time of the writing of this report, with 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 report contains no statements or warranties on the identification of all vulnerabilities and security of the code. The report covers the code submitted and reviewed, so it may not be relevant after any modifications. Do not consider this report as a final and sufficient assessment regarding the utility and safety of the code, bug-free status, or any other contract statements.

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 the security of smart contracts.

English is the original language of the report. The Consultant is not responsible for the correctness of the translated versions.

Technical Disclaimer

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