

HACKEN

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Customer: XPayBack
Date: Mar 03, 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 XPayBack
Approved By	Yevheniy Bezuhlyi SC Audits Head at Hacken OU
Type	ERC20 token
Platform	EVM
Language	Solidity
Methodology	Link
Website	https://xactrewards.com
Changelog	21.02.2023 - Initial Review 03.03.2023 - Second Review

Table of contents

Introduction	4
Scope	4
Severity Definitions	4
Executive Summary	6
Checked Items	6
System Overview	10
Findings	11
Critical	11
High	11
Medium	11
M01. Best Practice Violations	11
Low	11
L01. Technical Description Is Limited	11
Disclaimers	12

Introduction

Hacken OÜ (Consultant) was contracted by XPayBack (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 is smart contracts in the repository:

Initial review scope

Repository	https://github.com/aloshyakasoto/XACT-Token
Commit	6259285317b638828f5c7f3e47ac726f70836b9e
Whitepaper	https://docs.google.com/document/d/1MIfBwXWCGQz0vn116CGydwOM2G14DIA5/edit
Functional Requirements	https://docs.google.com/document/d/1MIfBwXWCGQz0vn116CGydwOM2G14DIA5/edit
Technical Requirements	https://docs.google.com/document/d/1MIfBwXWCGQz0vn116CGydwOM2G14DIA5/edit
Contracts	File: ./contracts/XACTToken.sol SHA3: 4ddf4c123054dbdf92636e5c4a83ff8f865dc7a0ffe2a66ab5727381f6d1d0cd

Second review scope

Repository	https://github.com/Code-XPB/XPB_XACT-Token
Commit	7c448f783657c0f92516d370a13c31ade1787bd9
Whitepaper	https://xactrewards.com/wp-content/uploads/whitepaper/XActRewards-Whitepaper-V.1.0.pdf
Functional Requirements	https://xactrewards.com/wp-content/uploads/whitepaper/XActRewards-Whitepaper-V.1.0.pdf
Technical Requirements	https://xactrewards.com/wp-content/uploads/whitepaper/XActRewards-Whitepaper-V.1.0.pdf
Contracts	File: ./contracts/XACTToken.sol SHA3: e5834940b24d81ceedfc45de30377ba04cc693ac2508c977251c126661e6b770
Contracts Addresses	https://polygonscan.com/token/0xd6c93ab226455c524663eebd79fa2de9395c7d8d#code

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 [scoring methodology](#).

Documentation quality

The total Documentation Quality score is **8** out of **10**.

- Project overview is detailed
- Technical specification is provided.
- NatSpec is insufficient.

Code quality

The total Code Quality score is **9** out of **10**.

- Best practice violations.

Test coverage

Code coverage of the project is **0.00%** (branch coverage).

- Code is not covered with tests.

Security score

As a result of the audit, the code contains **1** medium severity issue. The security score is **9** 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: **8.9**.

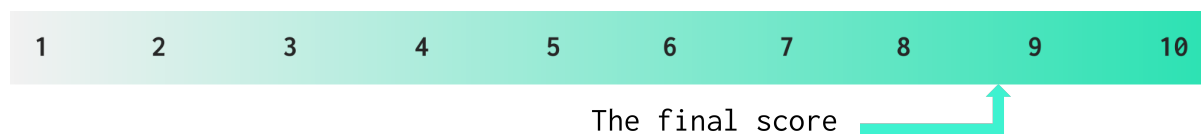


Table. The distribution of issues during the audit

Review date	Low	Medium	High	Critical
21 February 2023	1	1	0	0
03 March 2023	0	1	0	0

Checked Items

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

Item	Type	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.	Passed
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.	Passed
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.	Passed
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
Authorization through tx.origin	SWC-115	tx.origin should not be used for authorization.	Passed
Block values as a proxy for time	SWC-116	Block numbers should not be used for time calculations.	Passed
Signature Unique Id	SWC-117 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 Randomness	SWC-120	Random values should never be generated from Chain Attributes or be predictable.	Passed
Incorrect Inheritance Order	SWC-125	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order.	Passed
Calls Only to Trusted Addresses	EEA-Leve1-2 SWC-126	All external calls should be performed only to trusted addresses.	Not Relevant
Presence of Unused Variables	SWC-131	The code should not contain unused variables if this is not justified by design.	Passed
EIP Standards Violation	EIP	EIP standards should not be violated.	Passed
Assets Integrity	Custom	Funds are protected and cannot be withdrawn without proper permissions or be locked on the contract.	Passed
User Balances Manipulation	Custom	Contract owners or any other third party should not be able to access funds belonging to users.	Passed
Data Consistency	Custom	Smart contract data should be consistent all over the data flow.	Passed

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.	Passed
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.	Passed
Style Guide Violation	Custom	Style guides and best practices should be followed.	Failed
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

System Overview

XACTToken is an ERC-20 token that adds a cap to the supply of tokens. Additional minting is allowed to the owner of the smart contract, but not more than cap.

It has the following attributes:

- Name: XactToken
- Symbol: XACT
- Decimals: 18
- Initial supply: 100m tokens.
- Maximum supply: 10b tokens.

Privileged roles

- The owner can mint any amount of tokens at any time, but not more than cap.

Findings

Critical

No critical severity issues were found.

High

No high severity issues were found.

Medium

M01. Best Practice Violations

The number of tokens passed as an argument to the method is multiplied later. Usually, the final quantity is transferred in the parameter. This may lead to an erroneous number of minted tokens.

Path: ./contracts/XACTToken.sol : mint(address, uint)

Recommendation: remove the multiplication inside the method, pass the exact value instead.

Found in: 6259285317b638828f5c7f3e47ac726f70836b9e

Status: Reported

Low

L01. Technical Description Is Limited

Only the development environment is configured. No run instructions. No NatSpec with technical information.

Path: ./contracts/XACTToken.sol : mint(address, uint)

Recommendation: add run instructions, and NatSpec with technical information.

Found in: 6259285317b638828f5c7f3e47ac726f70836b9e

Status: Fixed (Revised commit:
7c448f783657c0f92516d370a13c31ade1787bd9)

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.