




HACKEN




SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT



Customer: Xtsunami

Date: January 14th, 2022



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

Document

Name	Smart Contract Code Review and Security Analysis Report for Xtsunami.
Approved by	Andrew Matiukhin CTO Hacken OU
Type	Subscription
Platform	Binance / Solidity
Methods	Architecture Review, Functional Testing, Computer-Aided Verification, Manual Review
Repository	https://github.com/xtblock/subscription-payment
Commit	0e6823f2f9d9fbecf2e19e249d000e14dd61bd55
Technical Documentation	NO
JS tests	NO
Website	xtsunami.com
Timeline	18 NOVEMBER 2021 - 14 JANUARY 2022
Changelog	26 NOVEMBER 2021 - INITIAL AUDIT 03 DECEMBER 2021 - SECOND REVIEW 14 JANUARY 2022 - THIRD REVIEW



Table of contents

Introduction	4
Scope	4
Executive Summary	5
Severity Definitions	7
Audit overview	8
Conclusion	10
Disclaimers	11

Introduction

Hacken OÜ (Consultant) was contracted by Xtsunami (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 contract and its code review conducted between November 18th, 2021 – November 26th, 2021.

Second review conducted on December 3rd, 2021.

Third review conducted on January 14th, 2022.

Scope

The scope of the project is smart contracts in repository:

Repository:

<https://github.com/xtblock/subscription-payment>

Commits:

[0e6823f2f9d9fbecf2e19e249d000e14dd61bd55](#)

Technical Documentation: No

JS tests: No

Contracts:

[Subscription-Payment-V2.sol](#)

We have scanned this smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that are considered:

Category	Check Item
Code review	<ul style="list-style-type: none">▪ Reentrancy▪ Ownership Takeover▪ Timestamp Dependence▪ Gas Limit and Loops▪ DoS with (Unexpected) Throw▪ DoS with Block Gas Limit▪ Transaction-Ordering Dependence▪ Style guide violation▪ Costly Loop▪ ERC20 API violation▪ Unchecked external call▪ Unchecked math▪ Unsafe type inference▪ Implicit visibility level▪ Deployment Consistency▪ Repository Consistency▪ Data Consistency

Functional review	<ul style="list-style-type: none"> ▪ Business Logics Review ▪ Functionality Checks ▪ Access Control & Authorization ▪ Escrow manipulation ▪ Token Supply manipulation ▪ Assets integrity ▪ User Balances manipulation ▪ Data Consistency manipulation ▪ Kill-Switch Mechanism ▪ Operation Trails & Event Generation
-------------------	---

Executive Summary

According to the assessment, the Customer's smart contracts are secured.



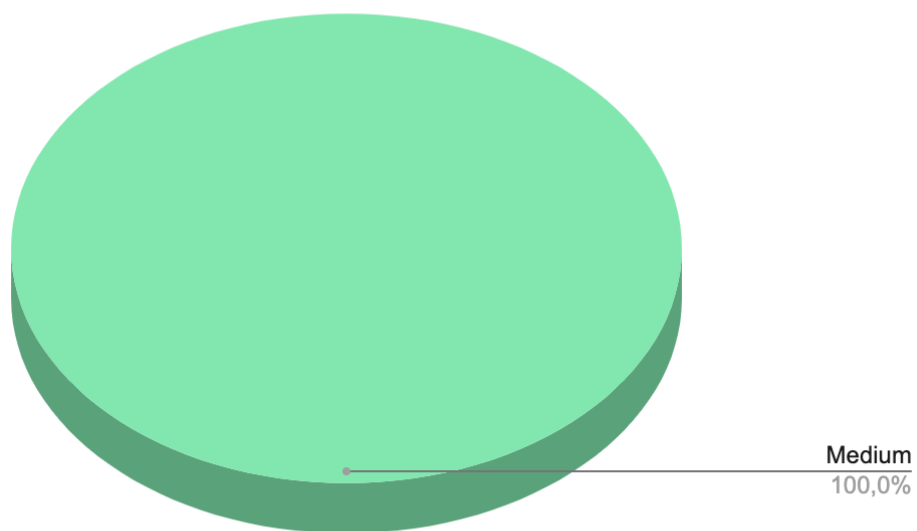
Our team performed an analysis of code functionality, manual audit, and automated checks with Mythril and Slither. All issues found during automated analysis were manually reviewed, and important vulnerabilities are presented in the Audit overview section. All found issues can be found in the Audit overview section.

As a result of the audit, security engineers found **1** medium and **3** low severity issues.

After the second review security engineers found **1** medium severity issue.

As a result of the third review, security engineers found that functionality was slightly changed. Therefore found **1** medium severity issue.

Graph 1. The distribution of vulnerabilities after the audit.



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

Audit overview

■ ■ ■ ■ Critical

No critical issues were found.

■ ■ ■ High

No high severity issues were found.

■ ■ Medium

No tests were provided

It's recommended to cover all non-trivial contracts with tests.

The recommended coverage is minimum 95% for branches, while it should be definitely 100% for the main logic contracts.

■ Low

1. State variables that could be declared constant

Constant state variables should be declared constant to save gas.

Contracts: Subscription-Payment.sol

Variables: _minSubscriptionDay

Recommendation: Add the constant attributes to state variables that never change.

Status: fixed

2. A public function that could be declared external.

public functions that are never called by the contract should be declared **external** to save gas.

Contracts: Subscription-Payment.sol

Functions: getMaxSubscriptionTime, getCurrentUserId,
balanceTokenForPayment, getUserExpiryTimeById,
getUserExpiryTimeByAddress, getUserAddressById, getIdByAddress,
getUserDataById, getUserDataByAddress, extendSubscription

Recommendation: Use the **external** attribute for functions never called from the contract.

Status: fixed



3. Too many digits

Literals with many digits are difficult to read and review.

Contracts: Subscription-Payment.sol

Recommendation: Please use scientific notation with ether suffix
(ex: *100e3 ether*).

Status: fixed

Conclusion

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

The audit report contains all found security vulnerabilities and other issues in the reviewed code.

As a result of the audit, security engineers found **1** medium and **3** low severity issues.

After the second review security engineers found **1** medium severity issue.

As a result of the third review, security engineers found that functionality was slightly changed. Therefore found **1** medium severity issue.

Disclaimers

Hacken Disclaimer

The smart contracts given for audit have been analyzed in accordance with the best industry practices at the date of this report, in relation to 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 audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. 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.

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 audit can't guarantee the explicit security of the audited smart contracts.