auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

Xpayments

DATED : 22 Jan, 2024

AUDIT SUMMARY

Project name – Xpayments

Date: 22 Jan, 2024

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **Passed With High Risk**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	1	0	0	0
Acknowledged	0	0	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:
A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :
The code has undergone static analysis using Slither.

Testnet version:
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
https://testnet.bscscan.com/address/0x5153BBbe7ed09A557B7b90Cb88efe010701D3905#code

Token Information

Token Name : Xpayments

Token Symbol: Xpayments

Decimals: 18

Token Supply: 1000000000000

Network: BscScan

Token Type: BEP-20

Token Address:
0x6E29F73B44121B87fa6f30a47A8Ed0744F75e0C8

Checksum:
Eb7acbefe2a12642d388659dffd20712

Owner:
0x116d32a25baa7Bce7Fa7Daf21565005aA12fFcCd
(at time of writing the audit)

Deployer:
0x116d32a25baa7Bce7Fa7Daf21565005aA12fFcCd

TOKEN OVERVIEW

Fees:

Buy Fee: 1-10%

Sell Fee: 1-10%

Transfer Fee: 0%

Fees Privilege: Owner

Ownership: Owned

Minting: No mint function

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

Other Privileges:

- **Whitelist to transfer without enabling trades**
- **Enabling trades**

AUDIT METHODOLOGY

The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code isexercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

VULNERABILITY CHECKLIST

- Return values of low-level calls
- Private modifier
- Multiple Sends
- Using Suicide
- Gas Limitand Loops
- Address hardcoded
- Exception Disorder
- Using inline assembly
- Divide before multiply
- Missing Zero Address Validation
- Compiler version not fixed
- **Gasless Send**
- Using block.timestamp
- Re-entrancy
- Tautology or contradiction
- Timestamp Dependence
- Revert/require functions
- Use of tx.origin
- Integer overflow/underflow
- Dangerous strict equalities
- Using SHA3
- Using throw

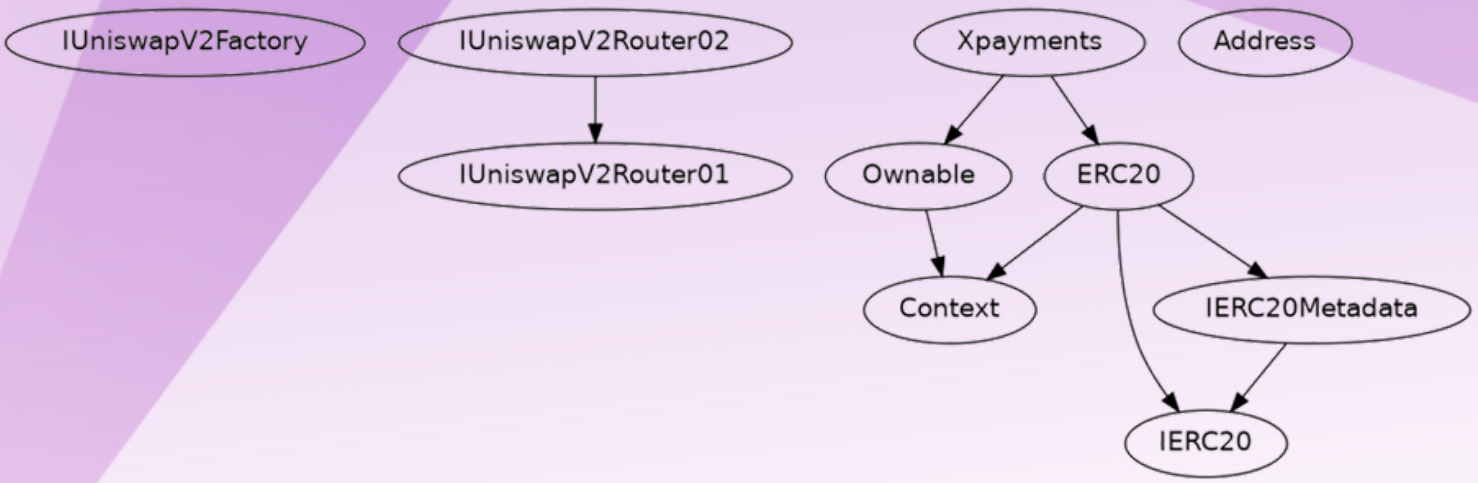
STATIC ANALYSIS

A static analysis of the code was performed using Slither.

No issues were found.

```
INFO:Detectors:
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
WARNING:Slither:No contract was analyzed
INFO:Slither:Xpayments.sol analyzed (0 contracts with 93 detectors), 1 result(s) found
```

INHERITANCE TREE



OWNERSHIP PRIVILEGES

- The owner can transfer ownership.
- The owner can renounce ownership.
- The owner can Enable trading.
- The owner can update buy, and sell fees of not more than 10%.
- The owner can exclude accounts from fees.
- The owner can change the fee receiver address.

Functional Tests

1- Approve (passed):

https://testnet.bscscan.com/tx/0xa1dd70df9b9c7425720afe8beb857158ec936eb5561000e9bc5da04b3a112158

2- Increase Allowance (passed):

https://testnet.bscscan.com/tx/0x7d11a1d68ca868aed2b10337f5f454df1d538bfb87e9a719fe27f32084fc7923

3- Decrease Allowance (passed):

https://testnet.bscscan.com/tx/0x1d1f4b998c5ba506221e7e4adc832b4e3a70d87c0f93a60c709174c8ad1ad565

4- Enable Trading (passed):

https://testnet.bscscan.com/tx/0x7bf509e7773c3916dfe512b5049a823d39e3bdc4c4ac251df69ef3532bf7627b

5- Update Fees (passed):

https://testnet.bscscan.com/tx/0xca5de77e61cd1f3c64f255c69dc8385aad9ac02ebc39b93eea8f0c6dd330f123

CLASSIFICATION OF RISK

Severity	Description
Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Gas Optimization /Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
Critical	0
High-Risk	1
Medium-Risk	0
Low-Risk	0
Gas Optimization / Suggestions	0

MANUAL TESTING

Centralization – Enabling Trades

Severity: High

Function: Enabling Trades

Status: Open

Overview:

The EnableTrading function permits only the contract owner to activate trading capabilities. Until this function is executed, no investors can buy, sell, or transfer their tokens. This places a high degree of control and centralization in the hands of the contract owner.

```
function enableTrading() external onlyOwner{
        require(!tradingEnabled, "CSLT: Trading already enabled.");
        tradingEnabled = true;
        swapEnabled = true;

        emit TradingEnabled(tradingEnabled);
    }
```

Suggestion:

To reduce centralization and potential manipulation, consider one of the following approaches:

1.Automatically enable trading after a specified condition, such as the completion of a presale, is met.

2.If manual activation is still desired, consider transferring the ownership of the contract to a trustworthy, third-party entity like a certified "PinkSale Safu" developer. This can give investors more confidence in the eventual activation of trading capabilities, mitigating concerns of potential bad-faith actions by the original owner.

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.

ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.

https://auditace.tech/

https://t.me/Audit_Ace

https://twitter.com/auditace_

https://github.com/Audit-Ace