IT Solutions
ArhamSoft (Pvt) Ltd.

# WELCOME to ArhamSoft

ArhamSoft (Pvt) Ltd. is an ISO certified IT services provider setting a benchmark of excellence in delivering innovative solutions for the benefit of businesses.

Since 2007, we are operating with synergistic approach to deliver high-end Web and Mobile Apps, Custom Software Development, Cloud Computing Solutions, Microsoft Dynamics, SharePoint, Blockchain, Digital Marketing, and more.

**Our long-term collaborative customer relationships are based on trust, transparency and global perspective. We follow international standards of quality and excellence**

ISO 9001:2015

ISO 27001:2013

SECP

PAKISTAN PSEB SOFTWARE EXPORT BOARD

P@SHA

www.arhamsoft.com

Audit Report

# Smart Contract Audit Report

**Prepared by:**

IT Solutions
ArhamSoft (Pvt) Ltd.

Office # 17-N, Main Boulevard,
Johar Town, Lahore, Pakistan
*www.arhamsoft.com*

## Disclaimer

This is a limited report on our findings based on our analysis, following good industry practice as at the date of this report, about cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. To get a full view of our analysis, you must read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us based on what it says or doesn’t say, or how we produced it, and you need to conduct your independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any part of it. If you do not agree to the conditions, please report immediately and delete and destroy any copies you have downloaded and/or printed. This material is offered for informational purposes only and is not intended to be relied upon; it does not represent investment advice. No one has any right to depend on the report or its contents, or on its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives).

The report is supplied "as is," with no warranties, or other terms of any kind except as set out in this disclaimer, hereby excludes all representations, warranties, conditions, and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have an effect about the report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

# Project Scope

The scope of the project is a smart contract audit. We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but is not limited to)

## Smart Contract Details

Smart Contract Name: xWin Lucky Draw

Smart Contract Address: 0x6F995c3e2001D45e2Aca7df537ce6a106767Beb

Chain Name: Binance Smart Chain

# Audit Goals

The focus of this audit was to verify whether the smart contract is secure, resilient, and working properly according to the specs. The audit activity can be grouped into three categories.

1. Correctness
2. Section of code with high complexity
3. Readability
4. Quantity and quality of test coverage.

## Issues Checking Status

| Sr # | Issue Description | Checking Status |
|---|---|---|
| **1** | Compiler errors | Passed, no compilation errors found |
| **2** | Race conditions and Reentrancy.<br>Cross-function race Passed conditions | Passed, no race condition found |
| **3** | Possible delays in data delivery | Passed, No delays in data delivery |
| **4** | Constructor parameters need to go on functions. Avoiding that is good – low | Passed Now, Because of immutability updated constructor values |
| **5** | Warning: Unused function parameter. Remove or comment out the variable name to silence this warning. | Passed, all warnings have been removed. |
| **6** | High Severity Issues | Passed, No high severity issues were found. |
| **7** | Medium Severity Issues | Passed, No medium severity issues were found. |
| **8** | Low Severity Issues | Passed, No low severity issues were found. |
| **9** | Owner privileges (In the period when the owner is not renounced) | Passed, Owner privileges have been clearly defined. |
| **10** | Owner can pause/un-pause contract. | Passed, Owner can pause/un-pause |
| **13** | Integer Overflow and Underflow | Passed, Condition met correctly |
| **14** | DoS with Revert | Passed, Prevent malicious attacks |

| | | |
|---|---|---|
| **15** | DoS with block gas limit | Passed, prevents attackers from creating an infinite transaction loop |
| **16** | Methods execution permissions | Passed, Permissions are written well for execution |
| **18** | Private user data leaks | Passed, Data will be encrypted. |
| **19** | Malicious Event log | Passed, Declared event log. |
| **20** | Scoping and Declarations | Passed, pointers are positioned well. |
| **21** | Uninitialized storage pointers | Passed |
| **22** | Arithmetic accuracy Design Logic | Passed, For Arithmetic accuracy, we have used SafeMath library/Function |
| **23** | Cross-function race conditions | Passed, All conditions met safely |
| **25** | Fallback function security | Passed, Declared correctly |
| **26** | Average Time Between Blocks | Passed, Depends on the slippage fee |
| **27** | Require Statement Without Error Message | Passed |

## Conclusion:

Smart contracts do not contain high severity issues.

## Important Note:

Please read the disclaimer above and remember that the audit makes no guarantees or assurances regarding company strategy, investment attractiveness, or code sustainability. The report only covers the contract specified in the report, and any additional prospective contracts deployed by the Owner are not included.