

Smart Contract Security Audit V1

xfuzion xfortune Smart Contract Audit

<https://xfuzion.finance/>

Nov 30, 2023



<https://saferico.com/>

business@saferico.com

https://t.me/SFI_ANN

—

Table of Contents

Table of Contents

Background

Project Information

Smart Contract Information

Executive Summary

File and Function Level Report

File in Scope:

Issues Checking Status

SWC Attack Analysis

Severity Definitions

Audit Findings

Automatic testing

Testing proves

Inheritance graph

Call graph

Source lines

Risk level

Source units in scope

Capabilities

Unified Modeling Language (UML)

Functions signature

Automatic general report

Conclusion

Disclaimer

Background

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Project Information

- **Platform:** Pulse Chain
- **Name:** xfortune
- **Language :** solidity
- **Contract Address:** 0x7291a375D3498980d94d1649C0249B795E950505
- **Code Source:**
<https://scan.pulsechain.com/address/0x7291a375D3498980d94d1649C0249B795E950505/contracts#address-tabs>
- **Website:** <https://xfuzion.finance/>
- **Telegram:** <https://t.me/XfuzionFinance>
- **X:** <https://x.com/xfuzionfinance>
- **Youtube:** <https://youtube.com/@XfuzionFinance?si=nfNwrOVxVWNJgnq2>
- **Discord:** <https://discord.gg/FCcD8YTuxc>

Executive Summary

According to our assessment, the customer's solidity smart contract is **Well-Secured**.

| | |
|--------------|---|
| Well Secured | ✓ |
| Secured | |
| Poor Secured | |
| Insecure | |

Automated checks are with remix IDE. All issues were performed by the team, which included the analysis of code functionality, manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the Project Information section and all issues found are located in the audit overview section.

Team found 0 critical, 0 high, 0 medium, 3 low, 0 very low-level issues and 0 note in all solidity files of the contract

The files:

xfourtune.sol

Audit Score:

100% secure



File and Function Level Report

File in Scope:

| Contract Name | SHA 256 hash | Contract Address |
|---------------|--|--|
| xfortune.sol | 8b011f38fc451225f2b1e154b71df0fa38578bfa | 0x7291a375D3498980d94d1649C0249B795E950505 |

- Contract: xfortune
- Inherit: ReentrancyGuard, IXFortune, Ownable
- Observation: All passed including security check
- Test Report: **passed**
- Score: **passed**
- Conclusion: **passed**

| Function | Test Result | Type / Return Type | Score |
|-----------------------------------|-------------|--------------------|---------------|
| calculateTotalPriceForBulkTickets | ✓ | Read / public | Passed |
| currentLotteryId | ✓ | Read / public | Passed |
| currentTicketId | ✓ | Read / public | Passed |
| owner | ✓ | Read / public | Passed |
| injectorAddress | ✓ | Read / public | Passed |
| MAX_LENGTH_LOTTERY | ✓ | Read / public | Passed |
| MAX_TREASURY_FEE | ✓ | Read / public | Passed |
| maxNumberTicketsPerBuyOrClaim | ✓ | Read / public | Passed |
| maxPriceTicketInXfn | ✓ | Read / public | Passed |
| MIN_DISCOUNT_DIVISOR | ✓ | Read / public | Passed |
| MIN_LENGTH_LOTTERY | ✓ | Read / public | Passed |

| | | | |
|--|---|----------------|---------------|
| minPriceTicketInXfn | ✓ | Read / public | Passed |
| operatorAddress | ✓ | Read / public | Passed |
| pendingInjectionNextLottery | ✓ | Read / public | Passed |
| randomGenerator | ✓ | Read / public | Passed |
| treasuryAddress | ✓ | Read / public | Passed |
| viewCurrentLotteryId | ✓ | Read / public | Passed |
| viewLottery | ✓ | Read / public | Passed |
| viewNumbersAndStatusesForTicketIds | ✓ | Read / public | Passed |
| viewRewardsForTicketId | ✓ | Read / public | Passed |
| viewUserInfoForLotteryId | ✓ | Read / public | Passed |
| xfnToken | ✓ | Read / public | Passed |
| buyTickets | ✓ | Write / public | Passed |
| claimTickets | ✓ | Write / public | Passed |
| changeRandomGenerator | ✓ | Write / public | Passed |
| closeLottery | ✓ | Write / public | Passed |
| drawFinalNumberAndMakeLotteryClaimable | ✓ | Write / public | Passed |
| injectFunds | ✓ | Write / public | Passed |
| recoverWrongTokens | ✓ | Write / public | Passed |
| setMaxNumberTicketsPerBuy | ✓ | Write / public | Passed |
| setMinAndMaxTicketPriceInXfn | ✓ | Write / public | Passed |
| transferOwnership | ✓ | Write / public | Passed |
| renounceOwnership | ✓ | Write / public | Passed |
| setOperatorAndTreasuryAndInjectorAddresses | ✓ | Write / public | Passed |
| startLottery | ✓ | Write / public | Passed |

Issues Checking Status

SWC Attack Analysis

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) for more info check

<https://swcregistry.io/>

| No. | Issue Description | Checking Status |
|-----|---|-----------------|
| 136 | Unencrypted Private Data On-Chain | Passed |
| 135 | Code With No Effects | Passed |
| 134 | Message call with hardcoded gas amount | Passed |
| 133 | Hash Collisions With Multiple Variable Length Arguments | Passed |
| 132 | Unexpected Ether balance | Passed |
| 131 | Presence of unused variables | Passed |
| 130 | Right-To-Left-Override control character (U+202E) | Passed |
| 129 | Typographical Error | Passed |
| 128 | DoS with block gas limit. | Passed |
| 127 | Arbitrary Jump with Function Type Variable | Passed |
| 126 | Insufficient Gas Griefing | Passed |
| 125 | Incorrect Inheritance Order | Passed |
| 124 | Write to Arbitrary Storage Location | Passed |
| 123 | Requirement Violation | Passed |
| 122 | Lack of Proper Signature Verification | Passed |
| 121 | Missing Protection against Signature Replay Attacks | Passed |
| 120 | Weak Sources of Randomness from Chain Attributes | Passed |
| 119 | Shadowing State Variables | Passed |

| | | |
|-----|--------------------------------------|-------------------|
| 118 | Incorrect Constructor Name | Passed |
| 117 | Signature Malleability | Passed |
| 116 | Block values as a proxy for time | Passed |
| 115 | Authorization through tx.origin | Passed |
| 114 | Transaction Order Dependence | Passed |
| 113 | DoS with Failed Call | Passed |
| 112 | Delegatecall to Untrusted Callee | Passed |
| 111 | Use of Deprecated Solidity Functions | Passed |
| 110 | Assert Violation | Passed |
| 109 | Uninitialized Storage Pointer | Passed |
| 108 | State Variable Default Visibility | Passed |
| 107 | Reentrancy | Passed |
| 106 | Unprotected SELFDESTRUCT Instruction | Passed |
| 105 | Unprotected Ether Withdrawal | Passed |
| 104 | Unchecked Call Return Value | Passed |
| 103 | Floating Pragma | Not Passed |
| 102 | Outdated Compiler Version | Passed |
| 101 | Integer Overflow and Underflow | Passed |
| 100 | Function Default Visibility | Passed |

Severity Definitions

| Risk Level | Description |
|------------|--|
| Critical | Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc. |
| High | High-level vulnerabilities are difficult to exploit; however, they also have 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 tokens lose |
| Low | Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution |
| Note | Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored. |

Audit Findings

Critical:

No Critical severity vulnerabilities were found.

High:

No High severity vulnerabilities were found.

Medium:

No Medium severity vulnerabilities were found.

Low:

#Improved Variable Naming in _calculateRewardsForTicketId()

Description

xfortune handles the logic for starting and closing lotteries, buying tickets, or viewing lottery information and the second one generates the final random winning number. For each purchased ticket, there is a helper routine to compute its rewards. In the following, we examine this specific helper routine `_calculateRewardsForTicketId()`.

To elaborate, we show below the `_calculateRewardsForTicketId()` routine. For a given ticket ID, this routine retrieves the user ticket number (line 1303) as well as the winning number (line 1300) and then transforms these two numbers to determine whether there is any match. It turns out that the user ticket number is internally named as `winningTicketNumber` while the winning number is represented as `userNumber`. These two internal variables can be exchanged to better present their intended semantic meanings.

```
function _calculateRewardsForTicketId(
    uint256 _lotteryId,
    uint256 _ticketId,
    uint32 _bracket
) internal view returns (uint256) {
    // Retrieve the winning number combination
    uint32 userNumber = _lotteries[_lotteryId].finalNumber;

    // Retrieve the user number combination from the ticketId
    uint32 winningTicketNumber = _tickets[_ticketId].number;

    // Apply transformation to verify the claim provided by the user is true
    uint32 transformedWinningNumber = _bracketCalculator[_bracket] +
        (winningTicketNumber % (uint32(10)**(_bracket + 1)));

    uint32 transformedUserNumber = _bracketCalculator[_bracket] + (userNumber %
        (uint32(10)**(_bracket + 1)));

    // Confirm that the two transformed numbers are the same, if not throw
    if (transformedWinningNumber == transformedUserNumber) {
```

```

        return _lotteries[_lotteryId].xfnPerBracket[_bracket];
    } else {
        return 0;
    }
}

```

Remediation

Choose variable names that better represent the intended purpose.

Status: **Acknowledged**.

#Multiple pragma statements

| Line | Pragma |
|------|-------------------------|
| 9 | pragma solidity ^0.8.0; |
| 34 | pragma solidity ^0.8.0; |
| 102 | pragma solidity ^0.8.0; |
| 165 | pragma solidity ^0.8.0; |
| 247 | pragma solidity ^0.8.0; |
| 464 | pragma solidity ^0.8.0; |
| 564 | pragma solidity ^0.8.4; |
| 583 | pragma solidity ^0.8.4; |
| 655 | pragma solidity ^0.8.4; |

Description

There are multiple pragma statements in the code. The newest compiler version 0.8.23 will work with the code, but keeping only one pragma statement helps in maintaining readability of the code.

Remediation

Keep a single pragma statement.

Status: **Acknowledged**.

Use of block.timestamp for comparisons

The value of block.timestamp can be manipulated by the miner. And conditions with strict equality is difficult to achieve - block.timestamp.

```

function closeLottery(uint256 _lotteryId) external override onlyOperator
nonReentrant {
    require(_lotteries[_lotteryId].status == Status.Open, "XFortune not open");
    require(block.timestamp > _lotteries[_lotteryId].endTime, "XFortune not
over");
    _lotteries[_lotteryId].firstTicketIdNextLottery = currentTicketId;

    // Request a random number from the generator based on a seed

    randomGenerator.getRandomNumber(uint256(keccak256(abi.encodePacked(_lotteryId,
currentTicketId))));
}

```

```
        _lotteries[_lotteryId].status = Status.Close;  
        emit LotteryClose(_lotteryId, currentTicketId);  
    }
```

Recommendation

Avoid use of block.timestamp.

Status

Acknowledged.

Very Low:

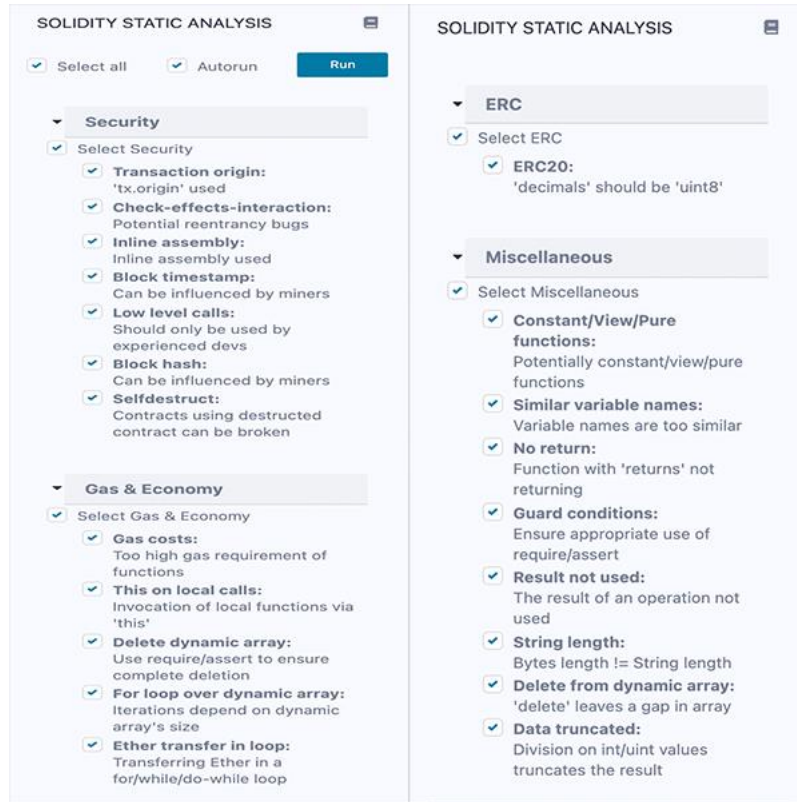
No Very Low severity vulnerabilities were found.

Notes:

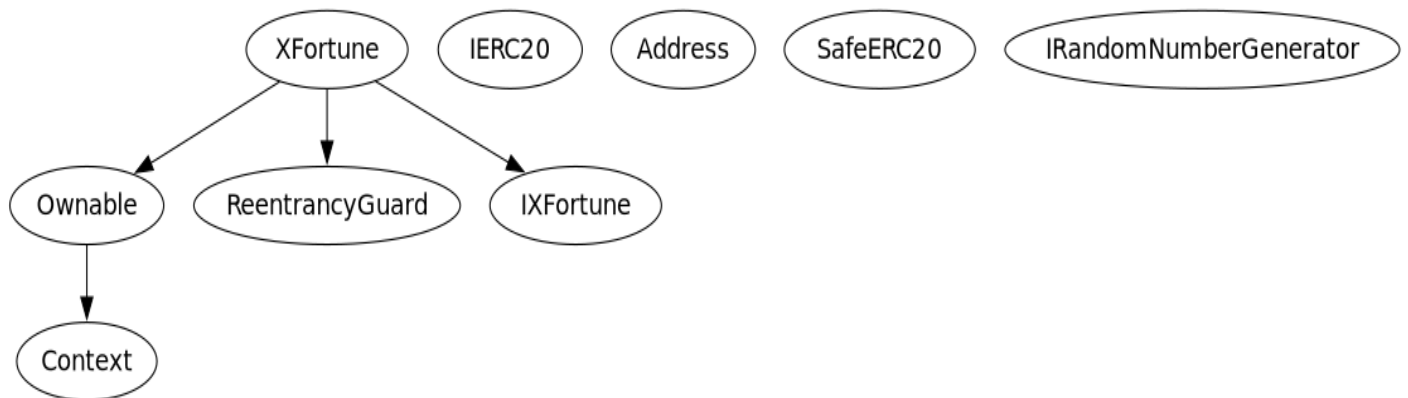
No Notes were found.

Automatic Testing

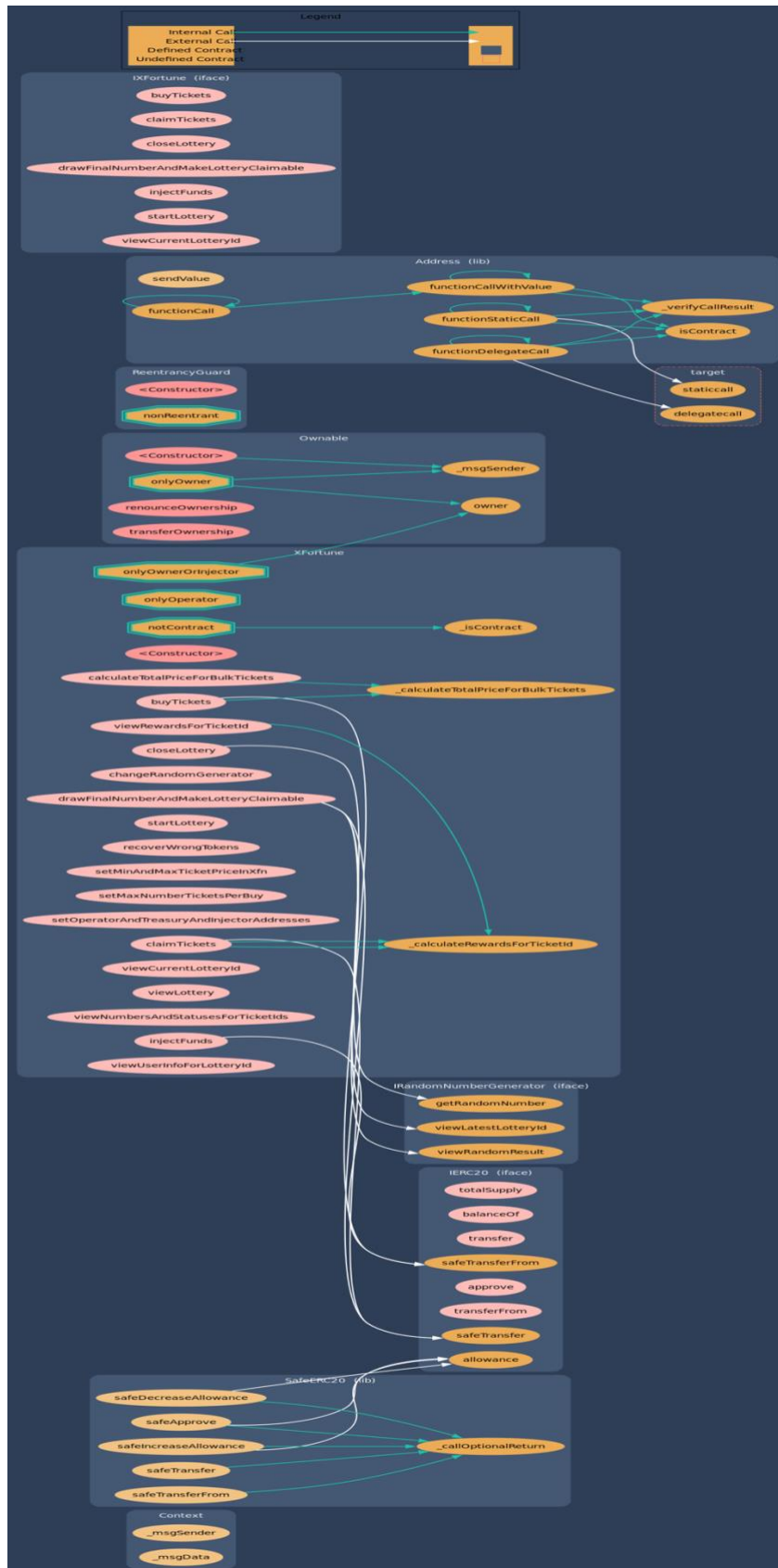
1- SOLIDITY STATIC ANALYSIS



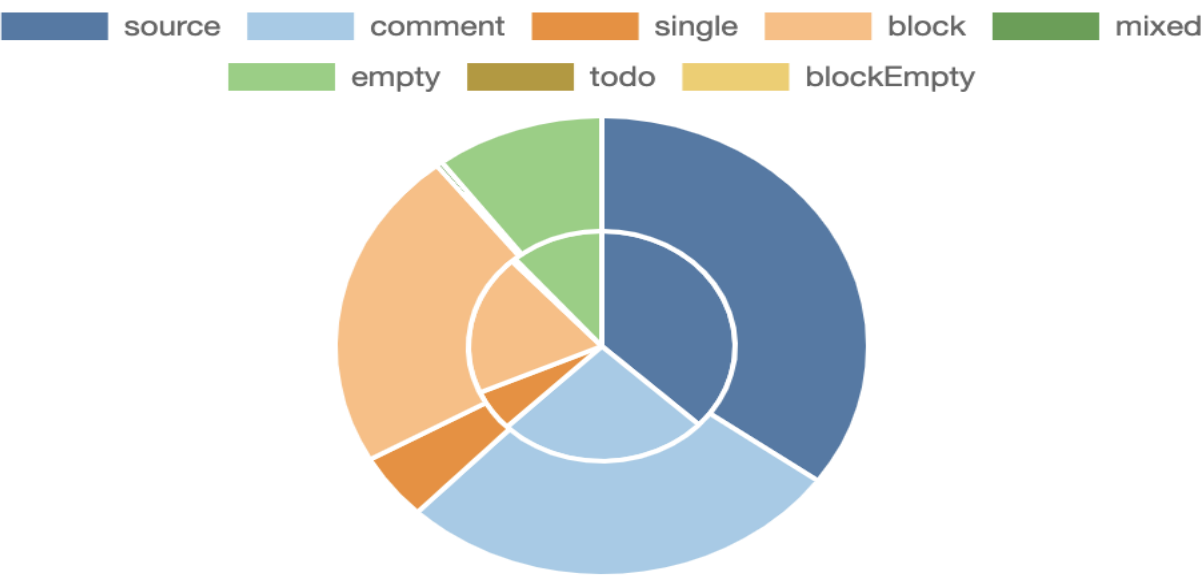
2- Inheritance graph



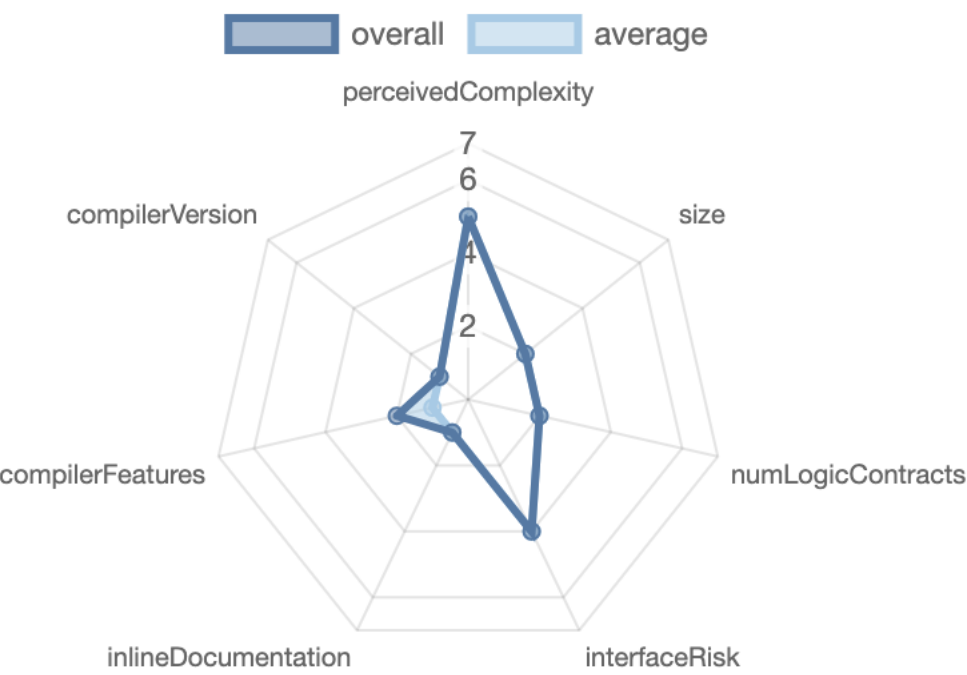
3- Call graph



Source lines



Risk level



Source units in scope

Source Units Analyzed: 1
Source Units in Scope: 1 (100%)

| Type | File | Logic Contracts | Interfaces | Lines | nLines | nSLOC | Comment Lines | Complex. Score | Capabilities |
|------|----------------------|-----------------|------------|-------|--------|-------|---------------|----------------|--------------|
| | xfuzion xfortune.sol | 6 | 3 | 1350 | 1080 | 544 | 510 | 415 | |
| | Totals | 6 | 3 | 1350 | 1080 | 544 | 510 | 415 | |

Legend: [-]

- **Lines**: total lines of the source unit
- **nLines**: normalized lines of the source unit (e.g. normalizes functions spanning multiple lines)
- **nSLOC**: normalized source lines of code (only source-code lines; no comments, no blank lines)
- **Comment Lines**: lines containing single or block comments
- **Complexity Score**: a custom complexity score derived from code statements that are known to introduce code complexity (branches, loops, calls, external interfaces, ...)

Capabilities

Components

| Contracts | Libraries | Interfaces | Abstract |
|-----------|-----------|------------|----------|
| 1 | 2 | 3 | 3 |

Exposed Functions

This section lists functions that are explicitly declared public or payable. Please note that getter methods for public stateVars are not included.

| Public | Payable |
|--------|---------|
| 36 | 0 |

| External | Internal | Private | Pure | View |
|----------|----------|---------|------|------|
| 33 | 60 | 2 | 3 | 18 |

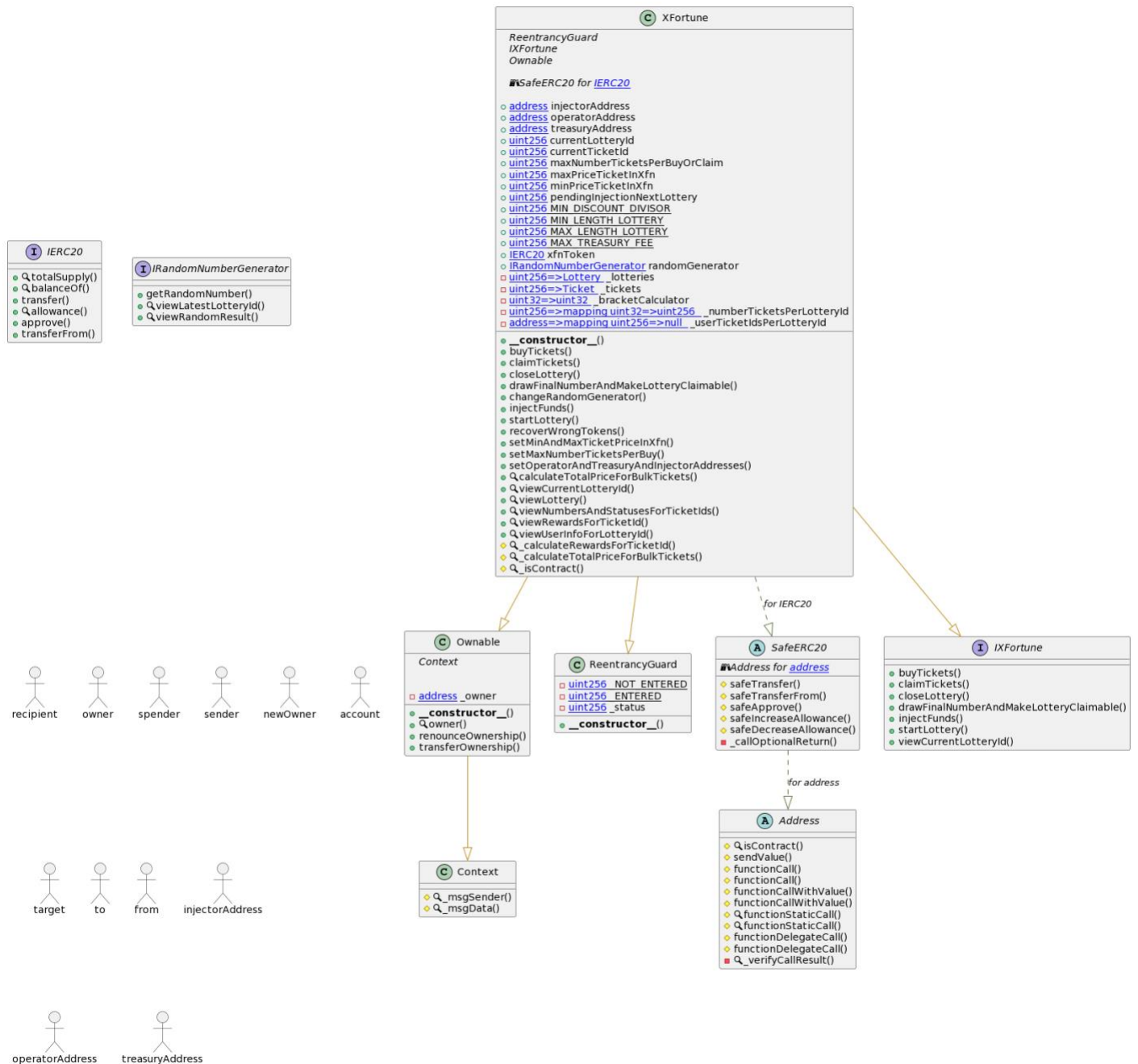
StateVariables

| Total | Public |
|-------|--------|
| 24 | 15 |

Capabilities

| Solidity Versions observed |  Experimental Features |  Can Receive Funds |  Uses Assembly |  Has Destroyable Contracts | |
|---|---|---|---|---|--|
| <div>^0.8.0</div> <div>^0.8.4</div> | | | <div>yes</div> <div>(3 asm blocks)</div> | | |
|  Transfers ETH |  Low-Level Calls |  DelegateCall |  Uses Hash Functions |  ECREcover |  New/Create/Create2 |
| | | <div>yes</div> | <div>yes</div> | | |

Unified Modeling Language (UML)



Functions signature

| Function Name | Sighash | Function Signature |
|--|----------|---|
| owner | 8da5cb5b | owner() |
| renounceOwnership | 715018a6 | renounceOwnership() |
| transferOwnership | f2fde38b | transferOwnership(address) |
| totalSupply | 18160ddd | totalSupply() |
| balanceOf | 70a08231 | balanceOf(address) |
| transfer | a9059cbb | transfer(address,uint256) |
| allowance | dd62ed3e | allowance(address,address) |
| approve | 095ea7b3 | approve(address,uint256) |
| transferFrom | 23b872dd | transferFrom(address,address,uint256) |
| getRandomNumber | b37217a4 | getRandomNumber(uint256) |
| viewLatestLotteryId | fbe5d917 | viewLatestLotteryId() |
| viewRandomResult | a1c4f55a | viewRandomResult() |
| buyTickets | 88303dbd | buyTickets(uint256,uint32[]) |
| claimTickets | c914914f | claimTickets(uint256,uint256[],uint32[]) |
| closeLottery | 9d8ca531 | closeLottery(uint256) |
| drawFinalNumberAndMakeLotteryClaimable | c38de539 | drawFinalNumberAndMakeLotteryClaimable(uint256,bool) |
| injectFunds | 471aeab4 | injectFunds(uint256,uint256) |
| startLottery | 0c915699 | startLottery(uint256,uint256,uint256,uint256[],uint256) |
| viewCurrentLotteryId | 80a06160 | viewCurrentLotteryId() |
| buyTickets | 88303dbd | buyTickets(uint256,uint32[]) |
| claimTickets | c914914f | claimTickets(uint256,uint256[],uint32[]) |
| closeLottery | 9d8ca531 | closeLottery(uint256) |
| drawFinalNumberAndMakeLotteryClaimable | c38de539 | drawFinalNumberAndMakeLotteryClaimable(uint256,bool) |
| changeRandomGenerator | 98359fa1 | changeRandomGenerator(address) |
| injectFunds | 471aeab4 | injectFunds(uint256,uint256) |
| startLottery | 0c915699 | startLottery(uint256,uint256,uint256,uint256[],uint256) |
| recoverWrongTokens | 3f138d4b | recoverWrongTokens(address,uint256) |
| setMinAndMaxTicketPriceInXfn | 33107d0d | setMinAndMaxTicketPriceInXfn(uint256,uint256) |
| setMaxNumberTicketsPerBuy | 6b873788 | setMaxNumberTicketsPerBuy(uint256) |
| setOperatorAndTreasuryAndInjectorAddresses | da4ca039 | setOperatorAndTreasuryAndInjectorAddresses(address,address,address) |
| calculateTotalPriceForBulkTickets | c4937ab9 | calculateTotalPriceForBulkTickets(uint256,uint256,uint256) |
| viewCurrentLotteryId | 80a06160 | viewCurrentLotteryId() |
| viewLottery | 2423807a | viewLottery(uint256) |
| viewNumbersAndStatusesForTicketIds | 8fc3539a | viewNumbersAndStatusesForTicketIds(uint256[]) |
| viewRewardsForTicketId | 2e530cae | viewRewardsForTicketId(uint256,uint256,uint32) |
| viewUserInfoForLotteryId | 05531eeb | viewUserInfoForLotteryId(address,uint256,uint256,uint256) |

Automatic general report




























Files Description Table

| File Name | SHA-1 Hash |
|---|--|
| /Users/macbook/Desktop/smart contracts/xfuzion xfortune.sol | 8b011f38fc451225f2b1e154b71df0fa38578bfa |

Contracts Description Table



| Contract | Type | Bases | | |
|---------------------|-----------------------|----------------|----------------|-----------|
| : | : | : | : | : |
| : | : | : | : | : |
| L | **Function Name** | **Visibility** | **Mutability** | |
| **Modifiers** | | | | |
| | | | | |
| **Context** | Implementation | | | |
| L | _msgSender | Internal | | |
| L | _msgData | Internal | | |
| | | | | |
| **Ownable** | Implementation | Context | | |
| L | <Constructor> | Public | | NO |
| L | owner | Public | | NO |
| L | renounceOwnership | Public | | onlyOwner |
| L | transferOwnership | Public | | onlyOwner |
| | | | | |
| **ReentrancyGuard** | Implementation | | | |
| L | <Constructor> | Public | | NO |
| | | | | |
| **IERC20** | Interface | | | |
| L | totalSupply | External | | NO |
| L | balanceOf | External | | NO |
| L | transfer | External | | NO |
| L | allowance | External | | NO |
| L | approve | External | | NO |
| L | transferFrom | External | | NO |
| | | | | |
| **Address** | Library | | | |
| L | isContract | Internal | | |
| L | sendValue | Internal | | |
| L | functionCall | Internal | | |
| L | functionCall | Internal | | |
| L | functionCallWithValue | Internal | | |
| L | functionCallWithValue | Internal | | |
| L | functionStaticCall | Internal | | |
| L | functionStaticCall | Internal | | |
| L | functionDelegateCall | Internal | | |
| L | functionDelegateCall | Internal | | |
| L | _verifyCallResult | Private | | |
| | | | | |
| **SafeERC20** | Library | | | |
| L | safeTransfer | Internal | | |
| L | safeTransferFrom | Internal | | |

```

| L | safeApprove | Internal |  |  | | |
| L | safeIncreaseAllowance | Internal |  |  | | |
| L | safeDecreaseAllowance | Internal |  |  | | |
| L | _callOptionalReturn | Private |  |  | | |
| | | | |
| **IRandomNumberGenerator** | Interface | | | |
| L | getRandomNumber | External |  |  | NO |
| L | viewLatestLotteryId | External |  | | NO |
| L | viewRandomResult | External |  | | NO |
| | | | |
| **IXFortune** | Interface | | | |
| L | buyTickets | External |  |  | NO |
| L | claimTickets | External |  |  | NO |
| L | closeLottery | External |  |  | NO |
| L | drawFinalNumberAndMakeLotteryClaimable | External |  |  | NO |
| L | injectFunds | External |  |  | NO |
| L | startLottery | External |  |  | NO |
| L | viewCurrentLotteryId | External |  |  | NO |
| | | | |
| **XFortune** | Implementation | ReentrancyGuard, IXFortune, Ownable | | |
| L | <Constructor> | Public |  |  | NO |
| L | buyTickets | External |  |  | notContract nonReentrant |
| L | claimTickets | External |  |  | notContract nonReentrant |
| L | closeLottery | External |  |  | onlyOperator nonReentrant |
| L | drawFinalNumberAndMakeLotteryClaimable | External |  |  | onlyOperator nonReentrant |
| L | changeRandomGenerator | External |  |  | onlyOwner |
| L | injectFunds | External |  |  | onlyOwnerOrInjector |
| L | startLottery | External |  |  | onlyOperator |
| L | recoverWrongTokens | External |  |  | onlyOwner |
| L | setMinAndMaxTicketPriceInXfn | External |  |  | onlyOwner |
| L | setMaxNumberTicketsPerBuy | External |  |  | onlyOwner |
| L | setOperatorAndTreasuryAndInjectorAddresses | External |  |  | onlyOwner |
| L | calculateTotalPriceForBulkTickets | External |  | | NO |
| L | viewCurrentLotteryId | External |  | | NO |
| L | viewLottery | External |  | | NO |
| L | viewNumbersAndStatusesForTicketIds | External |  | | NO |
| L | viewRewardsForTicketId | External |  | | NO |
| L | viewUserInfoForLotteryId | External |  | | NO |
| L | _calculateRewardsForTicketId | Internal |  | | |
| L | _calculateTotalPriceForBulkTickets | Internal |  | | |
| L | _isContract | Internal |  | | |

```

Legend

| Symbol | Meaning |
|---|---------------------------|
|  | Function can modify state |
|  | Function is payable |

Conclusion

The contracts are written systematically. Team found no critical issues. So, it is good to go for production.

Since possible test cases can be unlimited and developer level documentation (code flow diagram with function level description) not provided, for such an extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan Everything.

Security state of the reviewed contract is “Well Secured”.

- ✓ No volatile code.
- ✓ No high severity issues were found.

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to 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 the team on the basis of what it says or doesn't say, or how team produced it, and it is important for you to conduct your own independent investigations before making any decisions. team go into more detail on this in the below disclaimer below – please make sure to read it in full.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Saferico and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (Saferico s) owe no duty of care towards you or any other person, nor does Saferico make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and Saferico 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 effect in relation to the report. Except and only to the extent that it is prohibited by law, Saferico hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against Saferico, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this 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.