Nisedo's Checklist

Summary

Author: Nisedo

Source: Nisedo's Checklist

Checklist

Input Validation and Data Handling

1. **Improper Input Validation**
    - Incorrect Calculation
    - Passing zero as an input
    - Insufficient User-Input Validation
    - Accepting any data from an arbitrary address (Malicious bytes)
    - Addresses that might be empty at one point, yet house contract code at another
2. **Oracle/Price Manipulation**
    - Price manipulation
    - Problems with ERC20 decimals
3. **Data and Calculations**
    - Integer Overflow-Underflow
    - Integer Division
    - Integer Sign
    - Integer Truncation
    - Wrong Operator
    - Conversion Problem
    - Decimals interoperability
4. **Hidden Data and Initialization**
    - Hidden built-in symbols
    - Hidden state variables
    - Incorrect Inheritance Order
    - Uninitialised Local/State variables
    - Uninitialised Storage variables

Access Control and Authorization

1. **Weak Access Control**
    - Lack of Access Controls
    - Governance Attacks
2. **Replay Attacks/Signature Malleability**
    - Signatures (replay, malleability, recover to 0 address etc.)
3. **Authority Control and Privacy**
    - Replay Attack
    - Signature Maleability

- Use tx.origin for authentication
- Non-public variable are accessed by public/external functions
- Sybil attacks on incentives / Tokenomics

4. **Architecture and Maintainability**
   - Circuit break mechanism should not prevent users from withdrawing their funds
   - Least privilege principle should be used for the rights of each role
   - Implicity Visibility Level
   - Nonstandard Naming
   - Too many digits
   - Unlimited Compiler Version
   - Use deprecated built-in symbols

Mathematical Operations and Logic

1. **Rounding Errors**
   - Rounding Error
   - Forced precision loss when precision really matters (min balance checks etc...)
2. **Overflow/Underflow**
   - Overflow / Underflow
   - Divide before multiply
3. **Logic and Fairness**
   - Results of contract execution affected by miners
   - Transaction order dependence
   - Frontrunning
   - Missing upper/lower bounds or address(0) validation
4. **Storage and Signatures**
   - Storage overlap attack
   - Proxy Storage Collision
   - No nonce - signature replay attack
   - No chain ID - cross-chain replay attack on an instance of your protocol on another chain
   - No domain (address of contract) - signature replay in another similar project
   - Not checking for addr(0) when using ecrecover

Code and Storage

1. **Code Asymmetries and Loops**
   - Arbitrarily long loops
   - Code asymmetries
2. **Storage Issues**
   - Uninitialized Proxy
   - Write to Arbitrary storage collision

External Calls and Transactions

1. **Front-running and Race Conditions**
   - Frontrunning / Backrunning / Race Conditions / Sandwich attacks
     - Merkle trees are front-runnable
     - Be aware of sandwich attack on Vaults and DEXes

2. **Denial Of Service (DOS)**
    - DOS by complex fallback function
    - DOS by gaslimit
3. **External Calls and Ether Flow**
    - Reentrancy vulnerability (ERC721, ERC1155, ERC777, inter-function, inter-contract, inter-system)
    - Reentrancy Read-only
    - Unhandled Exception
    - Unchecked return values
    - Calls to phantom functions (fallback)
    - Arbitrary Calls Through Tokens (Sand Token)
    - Forced to receive ether
    - Locked Ether
    - Pre-sent Ether
    - External calls without gas stipends
    - Gas griefing with external call / Block stuffing

Token Standards and Interfaces

1. **ERC20 Specific**
    - Blacklisted ERC20 addresses
    - Weird ERC20 tokens (fees, 777, return values, etc.)
2. **ERC721/ERC1155 Specific**
    - Reentrancy (ERC721, ERC1155)
3. **Parameter and Token Interface**
    - Call/Delegatecall data/address is controlled externally
    - Hash collision with multiple variable length arguments
    - Short address attack
    - Signature with wrong parameter
    - Non-standard token interface