Jonas's Checklist

Summary

Author: Jonas

Source: Jonas's Checklist

Checklist

1. **Data**

   a. Calculations

   - ☐ Integer Overflow-Underflow
   - ☐ Integer Division
   - ☐ Integer Sign
   - ☐ Integer Truncation
   - ☐ Wrong Operator
   - ☐ Conversion Problem
   - ☐ Decimals interoperability

   b. **Hidden**

   - ☐ Hidden built-in symbols
   - ☐ Hidden state variables
   - ☐ Incorrect Inheritance Order

   c. Initialization

   - ☐ Uninitialised Local/State variables
   - ☐ Uninitialised Storage variables

2. **Description**

   a. Output

   - ☐ Right-to-Left-Override Control Character
   - ☐ Typo check
   - ☐ Check for events in admin changes
   - ☐ NatSpec incomplete

3. **Environment**

   a. Supporting Software

   - ☐ Delete Dynamic Array Elements
   - ☐ Using continue-statements in do-while-statements

4. **Interaction**

a. Contract call

- [ ] Reentrancy vulnerability
- [ ] Reentrancy Read-only
- [ ] Unhandled Exception
- [ ] Unchecked return values
- [ ] External calls without gas stipends
- [ ] Calls to phantom functions (fallback)

b. Ether flow

- [ ] Forced to receive ether
- [ ] Locked Ether
- [ ] Pre-sent Ether

c. ERC

- [ ] Check for special ERC20 cases

5. **Interface**

a. Parameter

- [ ] Call/Delegatecall data/address is controlled externally
- [ ] Hash collision with multiple variable lenght arguments
- [ ] Short address attack
- [ ] Signature with wrong parameter

b. Token Interface

- [ ] Non-standard token interface

6. **Logic**

a.Assemble code

- [ ] Returning results using assembly code in the constructor
- [ ] Specify function variable as any type

b. Denial of service

- [ ] DOS by complex fallback function
- [ ] DOS by gaslimit
- [ ] DOS by non-existent address or malicious contract

c. Fairness

- [ ] Transaction order dependence
- [ ] Frontrunning

f. Timestamp dependence

- [ ] Block.timestamp Manipulation

- [ ] Long time to execute might be a problem

7. **Performance**

   a. Gas

   - [ ] Byte[]
   - [ ] Invariants in loop
   - [ ] Invariant state variable are not declared constant
   - [ ] Unused public function within the contract should be declared as external

8. **Security**

   a. Authority control

   - [ ] Replay Attack
   - [ ] Signature Maleability - OZ version < 4.7.3
   - [ ] Suicide Contracts
   - [ ] Use tx.origin for authentication
   - [ ] Wasteful Contracts
   - [ ] Wrong Constructor Name

   b. Privacy

   - [ ] Public data

9. **Standard**

   a. Maintainability

   - [ ] Implicity Visibility Level
   - [ ] Nonstandard Naming
   - [ ] Too many digits
   - [ ] Unlimited Compiler Version
   - [ ] Use deprecated built-in symbols

   b. Programming Specification

   - [ ] View/contstant function changes contract state
   - [ ] Improper use of require, assert and revert
   - [ ] Check for EIPs implementation

10. **Bridges**

    a. Precompiles

    - [ ] Check precompiles for **Missing Call Checks (can be called with delegate calls)**

11. **Attacks**

    - [ ] Price Oracle Manipulation
    - [ ] Flash Loan Attacks
    - [ ] Cross-Chain Bridge Manipulation

    - [ ] Insolvency
    - [ ] Incorrect Slippage - When slippage % is fixed
    - [ ] Initial Supply Mint Issue
    - [ ] Malicious Honeypot (Compromised ERC20/ERC777/etc)
    - [ ] Sandwich Attacks

Complex Exploits:

- Multiple contract reentrancy
- Flash-loan to lend, borrow, burn and then liquidate itself

Common Lending/Borrowing Vulns

- [ ] Liquidation Before Default
- [ ] Borrower Can't Be Liquidated
- [ ] Debt Closed Without Repayment
- [ ] Repayments Paused While Liquidations Enabled
- [ ] Collateral Pause Stops Existing Repayment & Liquidation
- [ ] Liquidator Takes Collateral With Insufficient Repayment
- [ ] Infinite Loan Rollover
- [ ] Repayment Sent to Zero Address
- [ ] Borrower Permanently Unable To Repay Loan
- [ ] Borrower Repayment Only Partially Credited
- [ ] Check if it's possible to lend and borrow same token - flash-loan + inflating price attack