**Code Review Checklists of Croc Application**

**Static Code Analysis**

|  |  |  |
| --- | --- | --- |
| Checklist Item | Category | Notes |
| Check static code analyzer report for the classes added/modified | Manual Code Analysis | There must be automated Code Analysis for the project we are working on, do not forget to check the report for the modified/added classes  If no automated Code Analysis is setup for your project, we do not use automatic analysis |

**Clean Code**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Classes should be small | Classes |
| Functions should be small | Functions |
| Avoid duplication functions | Functions |
| Documentation properly | Comments |
| Use exceptions rather than return code | Exceptions |
| Don’t return null | Exceptions |
| Use intention-revealing names | Meaningful names |
| No spelling error | Meaningful names |

**Security**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Make class final if not being used | Fundamentals |
| Avoid repeat code | Fundamentals |
| Restrict privilege: application to run with least privilege mode required for functioning | Fundamentals |
| Document security related information | Fundamentals |
| Input into a system ought to be checked for valid data size and range | Denial of services |
| Clean sensitive information from exceptions (exposing file path, internals of the system, configuration) | Confidential information |
| Consider purging highly sensitive information from memory after use | Confidential information |
| Validate inputs (data size and range) | Input validation |
| Only use trusted interface when necessary | Access Control |

**Performance**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Avoid creating unnecessary process or threads | Creating and Destroying threads |

**General**

|  |  |
| --- | --- |
| Checklist Item | Category |
| Don’t ignore exceptions | Exceptions |
| Check parameters for validity | Methods |
| Return empty arrays or collections, not nulls | Methods |
| Prefer to use standard exception | Exceptions |
| Minimize the scope of local variables | General programming |
|  |  |
| Always overwrite string to a desired value while it has been used | General programming |
| Document thread safety | Concurrency |
| Carefully access to shared mutable data | Concurrency |

**Possibly Related CWE**

|  |  |
| --- | --- |
| [CWE-20](https://cwe.mitre.org/data/definitions/20.html) | Improper Input Validation |
| [CWE-200](https://cwe.mitre.org/data/definitions/200.html) | Exposure of Sensitive Information to an Unauthorized Actor |
| [CWE-287](https://cwe.mitre.org/data/definitions/287.html) | Improper Authentication |
| [CWE-434](https://cwe.mitre.org/data/definitions/434.html) | Unrestricted Upload of File with Dangerous Type |
| [CWE-94](https://cwe.mitre.org/data/definitions/94.html) | Improper Control of Generation of Code ('Code Injection') |
| [CWE-522](https://cwe.mitre.org/data/definitions/522.html) | Insufficiently Protected Credentials |
| [CWE-269](https://cwe.mitre.org/data/definitions/269.html) | Improper Privilege Management |
| [CWE-306](https://cwe.mitre.org/data/definitions/306.html) | Missing Authentication for Critical Function |
| [CWE-862](https://cwe.mitre.org/data/definitions/862.html) | Missing Authorization |
| CWE-250 | Execution with Unnecessary Privileges |
| CWE-676 | Use of Potentially Dangerous Function |
| CWE-253 | Incorrect Check of Function Return Value |
| CWE-920 | Improper Restriction of Power Consumption |
| CWE-400 | Uncontrolled Resource Consumption |
| CWE-410 | Insufficient Resource Pool |
| CWE-779 | Logging of Excessive Data |
| CWE-471 | Modification of Assumed-Immutable Data(MAID) |
| CWE-602 | Client-side Enforcement of Server-side Security |
| CWE-300 | Channel Accessible by Non-Endpoint |
| CWE-354 | Improper Validation of Integrity Check Value |
| CWE-290 | Authentication Bypass by Spoofing |
| CWE-291 | Reliance on IP Address for Authentication |
| CWE-201 | Insertion of Sensitive Information Into Sent Data |
| CWE-202 | Exposure of Sensitive Information Through Data Queries |
| CWE-266 | Incorrect Privilege Assignment |
| CWE-267 | Privilege Defined With Unsafe Actions |
| CWE-770 | Allocation of Resources Without Limits or Throttling |
| CWE-307 | Improper Restriction of Excessive Authentication Attempts |
| CWE-477 | Use of Obsolete Function |
| CWE-242 | Use of Inherently Dangerous Function |
| CWE-615 | Inclusion of Sensitive Information in Source Code Comments |
| CWE-248 | Uncaught Exception |
| CWE-397 | Declaration of Throws for Generic Exception |
| CWE-1126 | Declaration of Variable with Unnecessarily Wide scope |
| CWE-253 | Incorrect Check of Function Return Value |
| CWE-359 | Exposure of Private Personal Information to an Unauthorized Actor |
| CWE-209 | Generation of Error Message Containing Sensitive Information |
| CWE-1292 | Incorrect Conversion of Security Identifiers |
| CWE-364 | Signal Handler Race Condition (Thread) |
| CWE-367 | Time-of-check Time-of-use (TOCTOU) Race Condition |
| CWE-1041 | Use of Redundant Code |
| CWE-158 | Improper Neutralization of Null Byte or NUL Character |
| CWE-170 | Improper Null Termination |
| CWE-308 | Use of Single-factor Authentication |