The Java rules and recommendations in this wiki are a work in progress and reflect the current thinking of the secure coding community. Because this is a development website, many pages are incomplete or contain errors. As rules and recommendations mature, they are published in report or book form as official releases. These releases are issued as dictated by the needs and interests of the secure software development community.

Create a sign-in account if you want to comment on existing content. If you wish to be more involved and directly edit content on the site, you still need to request edit privileges.

Front Matter

- Rule. Preface

Rules

- Rule 00. Input Validation and Data Sanitization (IDS)
- Rule 01. Declarations and Initialization (DCL)
- Rule 02. Expressions (EXP)
- Rule 03. Numeric Types and Operations (NUM)
- Rule 04. Characters and Strings (STR)
- Rule 05. Object Orientation (OBJ)
- Rule 06. Methods (MET)
- Rule 07. Exceptional Behavior (ERR)
- Rule 08. Visibility and Atomicity (VNA)
- Rule 09. Locking (LCK)
- Rule 10. Thread APIs (THI)
- Rule 11. Thread Pools (TPS)
- Rule 12. Thread-Safety Miscellaneous (TSM)
- Rule 13. Input Output (FIO)
- Rule 14. Serialization (SER)
- Rule 15. Platform Security (SEC)
- Rule 16. Runtime Environment (ENV)
- Rule 17. Java Native Interface (JNI)
- Rule 18. Concurrency (CON)
- Rule 22. Reader/Writer Locks (RDL)
- Rule 23. Java Naming and Directory Interface (JNDI)
- Rule 24. Access Control (ACB)
- Rule 25. Transactions and Locking (TXN)
- Rule 26. Security Token Services (STS)
- Rule 27. Cryptography (CRY)
- Rule 29. Security Management (SMG)
- Rule 30. Network Security (NET)
- Rule 31. Secure Configuration (SCF)
- Rule 32. Secure Interfaces (IFI)
- Rule 33. Security Interfaces (IFI)
- Rule 34. Security Interfaces (IFI)
- Rule 35. Security Interfaces (IFI)
- Rule 36. Security Interfaces (IFI)
- Rule 37. Security Interfaces (IFI)
- Rule 38. Security Interfaces (IFI)
- Rule 39. Security Interfaces (IFI)
- Rule 40. Security Interfaces (IFI)
- Rule 41. Security Interfaces (IFI)
- Rule 42. Security Interfaces (IFI)
- Rule 43. Security Interfaces (IFI)
- Rule 44. Security Interfaces (IFI)
- Rule 45. Security Interfaces (IFI)
- Rule 46. Security Interfaces (IFI)
- Rule 47. Security Interfaces (IFI)
- Rule 48. Security Interfaces (IFI)
- Rule 49. Miscellaneous (MSC)
- Rule 50. Android (DRD)
- Rule AA. References
- Rule BB. Glossary
- Rule or Rec. CC. Analyzers
- Rule or Rec. DD. Related Guidelines
- Rule or Rec. EE. Risk Assessments

Recommendations

- Rec. 00. Input Validation and Data Sanitization (IDS)
- Rec. 01. Declarations and Initialization (DCL)
- Rec. 02. Expressions (EXP)
- Rec. 03. Numeric Types and Operations (NUM)
- Rec. 04. Characters and Strings (STR)
- Rec. 05. Object Orientation (OBJ)
- Rec. 06. Methods (MET)
- Rec. 07. Exceptional Behavior (ERR)
- Rec. 08. Visibility and Atomicity (VNA)
- Rec. 09. Locking (LCK)
- Rec. 10. Thread APIs (THI)
- Rec. 11. Thread Pools (TPS)
- Rec. 12. Thread-Safety Miscellaneous (TSM)
- Rec. 13. Input Output (FIO)
- Rec. 14. Serialization (SER)
- Rec. 15. Platform Security (SEC)
- Rec. 16. Runtime Environment (ENV)
- Rec. 17. Java Native Interface (JNI)
- Rec. 18. Concurrency (CON)
- Rec. 19. Reader/Writer Locks (RDL)
- Rec. 20. Java Naming and Directory Interface (JNDI)
- Rec. 21. Access Control (ACB)
- Rec. 22. Transactions and Locking (TXN)
- Rec. 23. Security Token Services (STS)
- Rec. 24. Cryptography (CRY)
- Rec. 25. Security Policy (SEC)
- Rec. 26. Security Management (SMG)
- Rec. 27. Network Security (NET)
- Rec. 28. Secure Configuration (SCF)
- Rec. 29. Secure Interfaces (IFI)
- Rec. 30. Security Interfaces (IFI)
- Rec. 31. Security Interfaces (IFI)
- Rec. 32. Security Interfaces (IFI)
- Rec. 33. Security Interfaces (IFI)
- Rec. 34. Security Interfaces (IFI)
- Rec. 35. Security Interfaces (IFI)
- Rec. 36. Security Interfaces (IFI)
- Rec. 37. Security Interfaces (IFI)
- Rec. 38. Security Interfaces (IFI)
- Rec. 39. Security Interfaces (IFI)
- Rec. 40. Security Interfaces (IFI)
- Rec. 41. Security Interfaces (IFI)
- Rec. 42. Security Interfaces (IFI)
- Rec. 43. Security Interfaces (IFI)
- Rec. 44. Security Interfaces (IFI)
- Rec. 45. Security Interfaces (IFI)
- Rec. 46. Security Interfaces (IFI)
- Rec. 47. Security Interfaces (IFI)
- Rec. 48. Security Interfaces (IFI)
- Rec. 49. Miscellaneous (MSC)
- Rec. 50. Android (DRD)

Secure Java Coding Books

There are two books available that cover Java: one for rules and the other for guidelines.

- Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs provides guidelines, recommendations, and examples to enable the creation of reliable, robust, fast, maintainable, and secure code.

Source Code Analysis Laboratory (SCALe)

SCALe offers conformance testing of Java language software systems against the CERT Oracle Secure Coding Standard for Java.

Contact Us

Contact us if you

- have questions about the Secure Coding wiki
- have recommendations for standards in development
- want to request privileges to participate in standards development

Thank You!

We acknowledge the contributions of the following folks, and we look forward to seeing your name here as well.
Rules vs. Recommendations

This coding standard consists of rules and recommendations, collectively referred to as guidelines. Rules are meant to provide normative requirements for code, whereas recommendations are meant to provide guidance that, when followed, should improve the safety, reliability, and security of software systems. Learn more about the differences.

Linking to Our Pages

Link to guidelines using the Tiny Link under ToolsLink to this Page... (This URL will not change if the name of the guideline changes.)

Information for Editors

- To eliminate a section from the lists above, label it section and void.
- To have a section listed as a recommendation, label it section and recommendation.
- To have a section listed as a rule, label it section and rule.