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 an account, but you’ll also need to request edit privileges.

Front Matter

Rules

Page: Rule. Preface

Recommendations

Page: Rec. 00. Input Validation and Data Sanitization (IDS)
Page: Rec. 01. Declarations and Initialization (DCL)
Page: Rec. 02. Expressions (EXP)
Page: Rec. 03. Numeric Types and Operations (NUM)
Page: Rec. 04. Characters and Strings (STR)
Page: Rec. 05. Object Orientation (OBJ)
Page: Rec. 06. Methods (MET)
Page: Rec. 07. Exceptional Behavior (ERR)
Page: Rec. 08. Visibility and Atomicity (VNA)
Page: Rec. 09. Locking (LCK)
Page: Rec. 10. Thread APIs (THI)
Page: Rec. 11. Thread Pools (TPS)
Page: Rec. 12. Thread-Safety Miscellaneous (TSM)
Page: Rec. 13. Input Output (FIO)
Page: Rec. 15. Platform Security (SEC)
Page: Rec. 16. Runtime Environment (ENV)
Page: Rec. 17. Java Native Interface (JNI)
Page: Rec. 18. Concurrency (CON)
Page: Rec. 19. Miscellaneous (MSC)

Source Code Analysis Laboratory (SCALe)

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