

00. Input Validation and Data Sanitization (IDS)

Guidelines

- IDS00-J. Prevent SQL injection
- IDS01-J. Normalize strings before validating them
- IDS02-J. Canonicalize path names before validating them
- IDS03-J. Do not log unsanitized user input
- IDS04-J. Safely extract files from ZipInputStream
- IDS05-J. Use a safe subset of ASCII for file and path names
- IDS06-J. Exclude unsanitized user input from format strings
- IDS07-J. Sanitize untrusted data passed to the Runtime.exec() method
- IDS08-J. Sanitize untrusted data included in a regular expression
- IDS09-J. Specify an appropriate locale when comparing locale-dependent data
- IDS10-J. Don't form strings containing partial characters
- IDS11-J. Perform any string modifications before validation
- IDS13-J. Use compatible character encodings on both sides of file or network IO
- IDS14-J. Do not trust the contents of hidden form fields
- IDS15-J. Do not allow sensitive information to leak outside a trust boundary
- IDS16-J. Prevent XML Injection
- IDS17-J. Prevent XML External Entity Attacks
- IDS50-J. Use conservative file naming conventions
- IDS51-J. Properly encode or escape output
- IDS52-J. Prevent code injection
- IDS53-J. Prevent XPath Injection
- IDS54-J. Prevent LDAP injection
- IDS55-J. Understand how escape characters are interpreted when strings are loaded
- IDS56-J. Prevent arbitrary file upload
- Rec. 00. Input Validation and Data Sanitization (IDS)
- Rule 00. Input Validation and Data Sanitization (IDS)

