

Rule 00. Input Validation and Data Sanitization (IDS)

Rules

- [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](#)

Risk Assessment Summary

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
IDS00-J	High	Probable	Medium	P12	L1
IDS01-J	High	Probable	Medium	P12	L1
IDS03-J	Medium	Probable	Medium	P8	L2
IDS04-J	Low	Probable	High	P2	L3
IDS06-J	Medium	Unlikely	Medium	P4	L3
IDS07-J	High	Probable	Medium	P12	L1
IDS08-J	Medium	Unlikely	Medium	P4	L3
IDS11-J	High	Probable	Medium	P12	L1
IDS16-J	High	Probable	Medium	P12	L1
IDS17-J	Medium	Probable	Medium	P8	L2

