# Rule 01. Input Validation and Data Sanitization (IDS)

- IDS30-PL. Exclude user input from format strings
- IDS31-PL. Do not use the two-argument form of open()
- IDS32-PL. Validate any integer that is used as an array index
- IDS33-PL. Sanitize untrusted data passed across a trust boundary
- IDS34-PL. Do not pass untrusted, unsanitized data to a command interpreter
- IDS35-PL. Do not invoke the eval form with a string argument

> **Information for Editors**
> In order to have a new guideline automatically listed above be sure to label it ids and rule.

## Risk Assessment Summary

| Rule | Severity | Likelihood | Remediation Cost | Priority | Level |
|---|---|---|---|---|---|
| IDS30-PL | High | Probable | Low | **P18** | **L1** |
| IDS31-PL | High | Likely | Low | **P27** | **L1** |
| IDS32-PL | Low | Likely | High | **P3** | **L3** |
| IDS33-PL | High | Likely | High | P9 | L2 |
| IDS34-PL | High | Probable | Medium | P12 | L1 |
| IDS35-PL | High | Likely | Medium | **P18** | **L1** |

---