Input Validation Attack

➡ Untrusted input is mixed into a command or query without proper validation or separation

◉ Execute unintended instructions instead of treating the input as data

✓ Can be mitigated with proper inout validation/sanitization

Notable Input Validation Attacks

- **Shellshock** (CVE-2014-6271)
  Command injection in Bash environment variable parsing allowing remote execution on web servers using CGI scripts

- **Log4Shell** (CVE-2021-44228)
  Command injection in Java Naming and Directory Interface (~ LDAP) allowing remote code execution in a widely used Java library