7.12.3 Ulteriori indicazioni per lo sviluppo sicuro

L'input dell'utente e i relativi dati associati rappresentano un rischio se non vengono attuati opportuni controlli di "Input Validation" e "Input Sanitization". Tutte le procedure di convalida dei dati devono essere eseguite su sistemi affidabili (ad esempio sul server) e devono essere eseguite a ogni livello dell'applicazione.

7.12.3.1 Validazione dell'INPUT

I dati dell'input devono essere considerati non sicuri per impostazione predefinita e accettati solo dopo aver effettuato i controlli di sicurezza appropriati. Anche le fonti dei dati devono essere identificate come attendibili o non affidabili e, in caso di fonti non attendibili, devono essere eseguiti controlli di convalida.

Se la convalida fallisce, l'input deve essere rifiutato.

Go dispone di librerie native che includono metodi a supporto del processo di validazione e sanitizzazione dei dati:

- strconv per la *conversione* di stringhe ad altre tipologie di dati:
  - Atoi
  - ParseBool
  - ParseFloat
  - ParseInt
- strings per *gestire* le stringhe e relative proprietà:
  - Trim
  - ToLower
  - ToTitle
- regexp utilizzabile nelle espressioni regolari per gestire *formati* personalizzati.
- *Altre* tecniche per garantire la validità dei dati di input includono:
  - *White listing* – verificare l'input sulla base di una white list di caratteri consentiti.
  - *Boundary checking* – verificare la lunghezza dei numeri e dei dati.
  - Validazione numerica.
  - Verificare i Null Bytes: (`%00`)
  - Verificare i caratteri di linea: `%0d , %0a , \r , \n`
  - Verificare i caratteri di alterazione del percorso `../` oppure `\\..`

NOTA: Assicurarsi che le intestazioni di richiesta e risposta HTTP contengano solo caratteri ASCII.