Contromisure:

- La validazione dell'input deve essere eseguita prima che l'input entri nel 'Web Server' o venga elaborato da quest'ultimo.
- La convalida dei dati ricevuti deve comprendere almeno:
  - La verifica del tipo di dato;
  - Il controllo dell'intervallo di ammissibilità dei valori dei dati per garantire che i valori forniti siano entro i limiti prestabiliti (minimo e massimo / dimensione);
  - Il controllo sulla base delle regole di business previste.
- Definire il set consentito di caratteri da accettare. La convalida basata su White list è da preferire a quella basata su Black list. La White list prevede la definizione esatta di ciò che è consentito, e per definizione, tutto il resto non è ammesso. L'utilizzo di espressioni regolari può facilitare l'implementazione di schemi di validazione basati su White list. La Black List cerca di rilevare caratteri e modelli di attacco ed è un approccio sconsigliato, in quanto è possibile per un aggressore eludere tali filtri.
- Mettere in campo un meccanismo di controllo degli accessi efficace capace di garantire l'accettazione dei dati solo da parte di utenti autorizzati.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	La mancanza di validazione dell'input da parte del Web Server lo espone a un'ampia varietà di attacchi che possono anche arrivare a compromettere la macchina su cui il Web Server è installato come nel caso di "Command Injection". **NOTA BENE** Si tratta di una minaccia molto generica che vuole focalizzare l'attenzione sul principio "all input is evil". Nel prosieguo vengono esaminate minacce più specifiche legate alla mancanza di validazione dell'input (cross-site scripting, sql injection, ecc.).	3
Reproducibility	L'attacco può essere condotto in qualunque momento	3
Exploitability	L'attacco non è banale: occorre una figura senior.	2
Affected Users	100%	3
Discoverability	Occorre identificare un exploit, attraverso la manomissione dei dati di input, cui il Web Server risulta vulnerabile.	1

DREAD Score: 12/15 (ALTO)

7.2.4 Cross Site Scripting

Categoria: Tampering

Descrizione: Il 'Web Server' potrebbe essere soggetto ad un attacco di Cross-Site Scripting in quanto non prevede la bonifica dell'input non affidabile (untrusted) che potrebbe contenere script malevoli

Contromisure:

- Eseguire l'escape del testo HTML prima di inserire i dati non attendibili nel contenuto degli elementi HTML.
- Eseguire l'escape del valore di un attributo prima di inserire dati non attendibili in attributi HTML.