Damage Potential	La possibilità, senza averne diritto, di modificare i dati all'interno del database dell'applicazione la espone potenzialmente alla totale compromissione.	3
Reproducibility	L'attacco può essere condotto in qualunque momento.	3
Exploitability	Per la natura del servizio, l'attacco richiede un'utenza autenticata.	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 (MEDIO)

7.4.4 Consumo eccessivo di risorse da parte del 'Web Server' o del 'SQL Database'

Categoria: Denial Of Service

Descrizione: Il "Web Server" o il "SQL Database" adottano passi espliciti per controllare il consumo di risorse? Fare attenzione che le richieste di risorse non producano deadlock e che, nel caso peggiore, vadano in timeout.

Contromisure:

- Non bloccare (deadlock) le richieste di risorse.
- Impostare i timeout per le richieste di risorse, se è applicabile.
- Validare i dati di input che si riferiscono al consumo di risorse.
- Limitare la dimensione dei dati elaborati dall'applicazione.
- Eseguire il rilascio delle risorse quando non sono più necessarie.
- Gli audit devono dare indicazioni sul consumo eccessivo di risorse da parte dell'applicazione.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	L'attaccante può degradare le prestazioni del sistema fino a renderlo potenzialmente indisponibile.	2
Reproducibility	L'attacco funziona sempre.	3
Exploitability	Per la natura del servizio, l'attacco richiede un'utenza autenticata.	2
Affected Users	100% (la piattaforma è resa indisponibile o comunque ne viene degradato il funzionamento).	3
Discoverability	Il rilevamento della minaccia è contestualizzato nell'ambito di un'utenza autenticata.	2

DREAD Score (Crash): 12/15 (ALTO)