7.4.1 Assunzioni

Si assume che il Web Server si autentica nei confronti del SQL Server utilizzando una username e una password, e può inserire, leggere, modificare, cancellare dati.
Si suppone che l'interazione avvenga all'interno di un Trusted Boundary.
A seguire vengono riportate le minacce individuabili nell'interazione in oggetto.

7.4.2 Vulnerabilità di SQL Injection nel 'SQL Database'

Categoria: Tampering

Descrizione: La SQL Injection è una tecnica di attacco di tipo "code injection", usata per attaccare un database, nella quale viene inserito del codice SQL malevolo all'interno di parametri di input in modo che vada in esecuzione sul database sotto attacco (es. per inviare all'attaccante /modificare/distruggere il contenuto del database e, in certi casi, "saltare dal DB al Sistema Operativo" e prendere il controllo della macchina). A patto che la query risultante da questo tipo di attacco sia sintatticamente corretta, il database la eseguirà.

Contromisure:

- Usare i Prepared Statements con query parametrizzate.
- Usare le Stored Procedures.
- Eseguire la validazione di tipo White List di ogni input esterno usato per costruire statements SQL.
- 4) Eseguire l'escape di ogni input utente.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	La possibilità di eseguire codice malevolo sul 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)

7.4.3 Possibile compromissione del 'SQL Database'

Categoria: Tampering

Descrizione: Assicurare l'integrità dei dati all'interno dell'archivio 'SQL Database'.

Contromisure:

- Autenticare tutti gli utenti.
- Mettere in pratica un efficace meccanismo di controllo degli accessi che garantisca che i dati possono essere scritti o modificati solo da utenti autorizzati.
- Rispettare il principio del privilegio minimo.
- Attuare controlli che seguano e registrino correttamente le azioni degli utenti.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score