7.5 Interazione: da SQL Database a Web Server

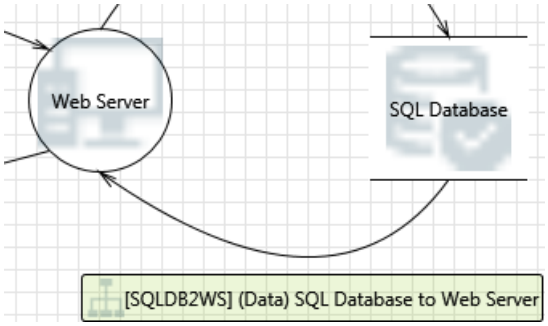

Figura 13 - Interazione tra SQL Database e Web Server

7.5.1 Assunzioni

Il Web Server si autentica nei confronti del SQL Database utilizzando una username e una password ed inserisce, legge, modifica e cancella dati.
Si suppone che l'interazione avvenga all'interno di un Trusted Boundary.
A seguire vengono riportate le minacce individuabili nell'interazione in oggetto.

7.5.2 Persistent Cross Site Scripting

Categoria: Tampering

Descrizione: Il 'Server Web' potrebbe essere soggetto ad un attacco di cross-site scripting di tipo persistente in quanto non bonifica i dati di input al 'SQL Database' in fase di scrittura (che potrebbero contenere uno script malevolo) e non esegue l'escape dei dati di output dal 'SQL Database' in fase di lettura (ciò che si traduce nel mandare in esecuzione su 'Browser Client' lo script malevolo).

Contromisure: Applicare le tecniche di bonifica e di escaping come nel caso di Cross Site Scripting.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	Lo script dannoso può accedere a qualsiasi cookie, token di sessione o altre informazioni sensibili conservate dal browser (qui Browser Client) e utilizzati esclusivamente nel dialogo con il sito d'origine (qui Web Server). Questi script possono anche riscrivere il contenuto della pagina HTML. In definitiva il Tampering dell'url produce Information Disclosure, tra cui la compromissione del token di sessione che abilita il "Session hijacking" (che è una forma di furto di identità – spoofed identity). Nel caso pessimo, l'attaccante potrebbe impersonare l'amministratore del Web Server.	2
Reproducibility	L'attacco funziona sempre. Tuttavia il token di sessione (che è il dato la cui compromissione è particolarmente grave: spoofed identity) è utilizzabile finché la sessione non scade.	2
Exploitability	L'attacco non è banale: occorre una figura senior.	2
Affected Users	100% (nel caso in cui l'attaccante arrivasse a impersonare l'amministratore).	3