## 7.2 Interazione: da Browser Client a Web Server

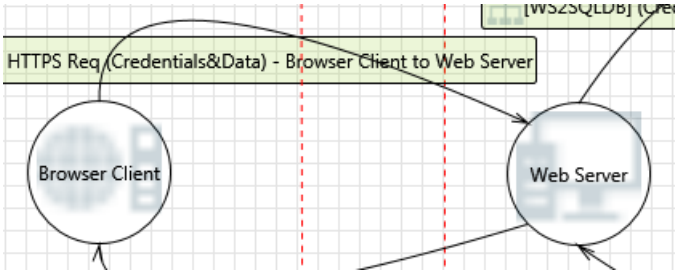


*Figura 10 - Interazione tra Browser Client e Web Server*

### 7.2.1 Assunzioni

Si assume che il Browser Client si autentica nei confronti del Web Server utilizzando una username e una password, ed esegue una post http per leggere e modificare i dati.
Si suppone inoltre, come già detto, che, l'utenza non autenticata (ovvero gli anonymous users) non possa accedere al sistema.
Il protocollo utilizzato è HTTPS, il quale garantisce:

- Autenticazione della Destinazione (Web Server);
- Confidenzialità;
- Integrità.

A seguire vengono riportate le minacce individuabili nell'interazione in oggetto.

### 7.2.2 Accesso a internet non valido

**Categoria:** Compliance

**Descrizione:** L'applicazione Web (qui "Server Web") non dovrebbe essere collegata direttamente a Internet.

**Contromisure:** Interconnettere il "Browser Client" con il "Server Web" tramite un gateway di protezione (firewall).

**Valutazione della priorità della minaccia (Ranking)**

| DREAD | Descrizione | Score |
|---|---|---|
| Damage Potential | Se il Web Server è esposto direttamente sulla rete Internet, un attaccante può facilmente compromettere il sistema. | 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 (es. per mancanza di patching adeguato del Sistema Operativo) cui la macchina su cui il Web Server è installato risulta vulnerabile. | 1 |

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

### 7.2.3 Mancanza di convalida dell'input da parte del "Web Server"

**Categoria:** Tampering

**Descrizione:** Il 'Web Server' non verifica che i dati di input siano nel formato previsto. Questa è la causa principale di un numero molto elevato di problemi sfruttabili. Considerate tutti i percorsi e il modo in cui si gestiscono i dati di input. Verificare che tutti gli input siano verificati e, se in formato non previsto, scartati o bonificati.