Damage Potential	L'attaccante può eseguire richieste di cambio stato al sistema che sono prerogativa di Autheticated User o, peggio, dell'Administrator (es. la modifica di configurazioni o il furto/modifica di dati privati).	2
Reproducibility	L'attacco funziona finché la sessione della vittima non scade.	1
Exploitability	L'attacco non è banale: occorre una figura senior.	2
Affected Users	In genere l'attacco è condotto con tecniche di social engineering: gli utenti coinvolti sono una quota parte del totale.	2
Discoverability	Occorre identificare un url che presenti la vulnerabilità XSRF.	1

DREAD Score: 8/15 (MEDIO)

7.3 Interazione: da Web Server a Browser Client

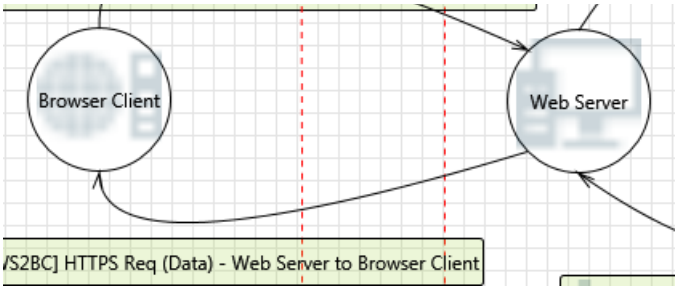

Figura 11 - Interazione tra Web Server e Browser Client

7.3.1 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.

7.3.2 Analisi delle minacce e mitigazioni

Valgono le raccomandazioni già proposte in "Interazione: da Browser Client a Web Server".

7.4 Interazione: da Web Server a SQL Database

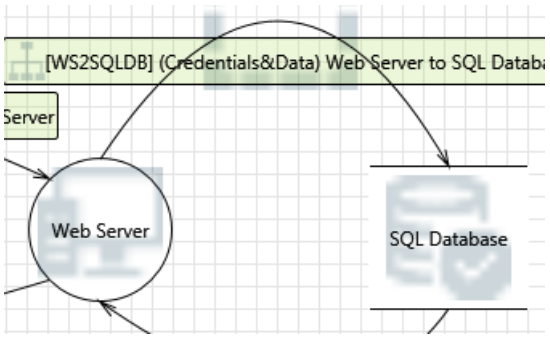

Figura 12 - Interazione tra Web Server e SQL Database