Università degli Studi di Trieste – Dipartimento di Ingegneria e Architettura

Progetto di Programmazione Web

Matteo Ferfoglia - 12 aprile 2021

**Link al repository con il codice sorgente:** <https://github.com/matteoferfoglia/progetto-progrweb-2020>

**Link alla versione live del progetto:** <https://progettoprogrweb2020.appspot.com>

*Credenziali per l’accesso*: username [**admin**] e password [**\*\*\***]

In questo progetto sono stati realizzati una *web application* ed un *client* ***REST***,dimostrativo del funzionamento del ***web service*** *REST* esposto, entrambi implementati in *Java* (versione 8, utilizzando le specifiche *Java EE 7*), usando ***Maven*** (versione 3.5) come strumento di *build automation*. Il *servlet container* utilizzato è ***Google App Engine***. Il progetto *Maven* della *web application* è stato inizialmente generato con *Google Cloud SDK*, usando l’archetipo com.google.appengine.archetypes:appengine-standard-archetype. L’applicazione *Java* fa uso di classi astratte ed “*helper*” nell’intento di mantenere un livello d’astrazione sufficiente da permettere, se necessario in futuro, la migrazione a tecnologie diverse.

Si è usato ***Datastore*** di *Google* come *DBMS*, perché è ben integrato con *App Engine* e fornisce un sistema di archiviazione scalabile e robusto, ed ***Objectify*** (versione 5) come *ORM*, per la sua semplicità d’uso. L’invio dei messaggi e-mail sfrutta la ***API Mail*** di *Google App Engine*. Si è utilizzato ***Jersey*** (implementazione di riferimento della tecnologia ***JAX-RS***) per realizzare le *API REST* (documentate con ***Swagger***) sulle quali si basa l’interazione tra client e server.

Si è realizzata una *Single Page Application* (*SPA*) utilizzando il *framework* ***Vue.js***(versione 3), insieme a ***Bootstrap*** (versione 4) per lo stile grafico e ***Vue Router*** (versione 4) per la navigazione tra i componenti, che si occupi della rappresentazione dei dati, ottenuti dal *web server* per mezzo di richieste asincrone effettuate sfruttando il pacchetto ***axios***, che è stato scelto per l’ottima documentazione e la facilità di configurazione ed integrazione nel progetto *Vue* (usando ***npm*** come gestore di pacchetti). I dati scambiati tra client e server sono perlopiù in formato ***JSON***: ciò permette il trasferimento delle informazioni con basso *overhead* e senza imporre un accoppiamento tra client e server; per ragioni di efficienza, fanno eccezione alcune richieste “semplici” a cui il server risponde in formato testo (*text/plain*) e le richieste di caricamento (in formato *multipart/form-data*) e di scaricamento (in formato *application/octet-stream*) dei file[[1]](#footnote-1).

Si è deciso di esporre un *web service* di tipo *REST*,perché *l’overhead* del traffico è minore rispetto a quello che si avrebbe utilizzando *SOAP* (che fa uso di *XML*); inoltre, il progetto *Maven* includeva già le dipendenze necessarie[[2]](#footnote-2).

Il meccanismo di autenticazione implementato è di tipo *Bearer*: quando il client si autentica presso il server, quest’ultimo gli rilascia un *token* ***JWT*** che il client dovrà allegare come valore del campo “*Authorization*” nelle richieste *HTTP* successive; utilizzando un sistema a chiavi asimmetriche per la firma del *JWT*, il server che verifica il token potrebbe essere diverso da quello che lo ha emesso, quindi sarebbe possibile l’integrazione di servizi esterni. Le *password* degli utenti vengono memorizzate in modalità *hashed&salted* (per evitare di fornirle in chiaro ad un eventuale utente malintenzionato che ne sia venuto a conoscenza) e sono stati implementati dei meccanismi per la verifica dell’account, a seguito della registrazione di un nuovo utente, e per il recupero della password. Gli utenti possono autenticarsi fornendo *username* e *password* oppure tramite il proprio account *Google* (l’utente viene identificato dall’indirizzo e-mail ottenuto tramite ***Firebase***).

Nella *web application* sono stati implementati dei ***filtri*** che, applicati nell’ordine specificato nel file *web.xml*, intercettano le richieste *HTTP* per verificare l’autorizzazione del client prima di procedere. Il *web-server* è stato configurato per accettare solo richieste *HTTPS*, per garantire integrità e riservatezza delle comunicazioni. L’applicazione implementa un meccanismo di prevenzione degli attacchi ***CSRF***: ogni *form* usato per modificare lo stato del sistema include un *token CSRF*, che viene anche aggiunto nel *payload* di un *JWT*, memorizzato come valore di un ***Cookie***. Tutti i *cookie* sono configurati con gli attributi *SameSite* (impostato a “*Lax*”, cosicché vengano allegati solo alle richieste nel contesto del sito di origine), *HttpOnly* (per evitare che vi si possa accedere tramite *script* lato client) e *Secure* (affinché vengano inviati solo con il protocollo HTTPS). È stata inoltre utilizzata la *dependency Maven* org.owasp.encoder:encoder per prevenire le vulnerabilità *XSS*.

Il comando **mvn clean package**, eseguito dal terminale posizionato nella cartella del progetto *Maven*, ne permette la compilazione. Il progetto *Vue* viene automaticamente compilato ed aggiunto durante la fase di *package* della *web-application*. La documentazione (incluso ***Javadoc***) per i progetti *Maven* può essere generata con il comando **mvn site**, dopo averne eseguito la compilazione. L’applicativo *client REST* può essere eseguito con il comando **mvn exec:java**.

1. Il codice per l’upload ed il download dei file è tratto rispettivamente da <https://stackoverflow.com/a/25889454> e <https://stackoverflow.com/a/12251265>. L’utilizzo del *Content-Type* “*multipart/form-data”* ha richiesto la dipendenza org.glassfish.jersey.media:jersey-media-multipart. Il client *REST* invia i dati in formato *multipart/form-data* (codice adattato da <https://stackoverflow.com/q/24637038>). Il codice per il download di un documento tramite *JavaScript* è tratto (ed opportunamente adattato) da <https://stackoverflow.com/q/33247716>, quello per l’upload in formato *multipart/form-data* da <https://stackoverflow.com/a/43014086>. Tutti i link indicati risultano funzionanti al 10 aprile 2021. [↑](#footnote-ref-1)
2. *Jersey* è anche usato per rispondere alle richieste della *SPA*. [↑](#footnote-ref-2)