Applicazioni Internet 2018-19

Esercitazione 3

Con riferimento all'esercitazione precedente, si implementi la componente di sicurezza associata al servizio web REST, utilizzando la tecnologia JWT.

L'applicazione dovrà esporre i seguenti end-point non protetti:

- POST /login – invia un oggetto JSON contenente e-mail e password. Se la coppia è riconosciuta e l'utente è attivo, restituisce un JWT valido, altrimenti restituisce 401 - Unauthorized
- POST /register – invia un oggetto JSON contenente e-mail, password, password di verifica. Controlla che l'utente con l'indirizzo di posta indicato non sia già presente nella base dati degli utenti, controlla che le due password combacino e siano sufficientemente sicure, crea un record con i dati dell'utente e ne fissa lo stato alla condizione di attesa di verifica. Invia all'indirizzo di posta un link random per l'abilitazione dell'account.
- GET /confirm/{randomUUID} – verifica che il codice random corrisponda ad uno degli utenti in corso di verifica, controlla che tale registrazione non sia scaduta e, nel caso, porta l'utente allo stato attivo e restituisce 200 – Ok, altrimenti restituisce 404 – Not found
- POST /recover – invia un'indirizzo di posta elettronica di cui si vuole ricuperare la password. Se l'indirizzo corrisponde a quello di un utente registrato, invia un messaggio di posta elettronica all'utente contenente un link random per la modifica della password. Risponde sempre 200 - Ok
- GET /recover/{randomUUID} – Restituisce una pagina HTML contente una form per la sostituzione della password
- POST /recover/{radomUUID} – Verifica che il codice random corrisponda ad uno di quelli che sono stati generati da una richiesta di recovery e che tale codice non sia scaduto. Verifica inoltre che le due password inviate corrispondano e che abbiano i necessari criteri di robustezza. In caso positivo aggiorna la base dati degli utenti con la nuova password e restituisce 200 – Ok, in caso negativo restituisce 404 – Not found

Tutti gli end-point precedentemente esistenti dovranno essere configurati per essere accessibili solo se viene passato, come intestazione della richiesta, il campo "Authorization: bearer <JWT>" e che il JWT sia valido e non scaduto. In caso contrario risponderanno 401 – Unauthorized. Se dal JWT risulta che l'utente corrente ha un ruolo non consono con la richiesta in corso, risponderà 403 – Forbidden.

All'atto della creazione, tutti gli utenti hanno il ruolo "user", tranno uno, preconfigurato dal sistema, che ha ruolo "system-admin". Costui avrà il permesso di modificare il ruolo degli altri per renderli "admin" di una particolare linea. Un utente "admin" di una linea potrà rendere

“admin” altri utenti o revocare tale permesso per la propria linea. A tale scopo si aggiungano gli end-point seguenti:

- GET /users, disponibile solo a chi ha il ruolo system-admin o admin di una specifica linea, che restituisce l’elenco di tutti gli utenti del sistema, eventualmente paginandoli
- PUT /users/{userID}, disponibile solo a chi ha il ruolo di system-admin o admin di una specifica linea che permette di rendere una persona admin della linea indicata o di rimuovere tale diritto. Se l’utente è system-admin, qualunque richiesta è lecita, altrimenti la linea indicata deve coincidere con quella a cui è associato il ruolo di admin. Una singola utenza può essere admin di più linee.