Features Modul 183

Sichere Passwordspeicherung

Die Sichere Passwortspeicherung wird über bcrypt gewährleistet.
Der Algorithmus generiert automatisch einen Salt, der zusammen mit dem Plaintext-Passwort über den bcrypt-hash Algorithmus gehasht.

Login über http-Post

Das Login wird über http ausgeführt, der Post schickt das E-Mail und Passwort der Login-Maske ans Backend, wo es mit dem bcrypt-Package überprüft wird. Wenn das Password stimmt wird ein JsonWebToken(JWT) zurückgeschickt.

Session Handling

Das Session Handling wird über ein JWT gewährleistet. Dieses hat ein Ablaufdatum, welches dem Benutzer erlaubt, für eine gewisse Zeit auf der App zu verweilen, bevor das Token durch erneutes Einloggen erneuert werden muss.

Log-Datei

Wir schreiben vom Backend aus, alle Zugriffe mit dem NPM-Package «fs-extra» in eine .log Datei.

Registration über http-Post

Die Registration wird über http ausgeführt, der Post schickt die Daten der Registrations-Maske ans Backend, wo der Benutzer in die Datenbank gespeichert wird. Der Benutzer wird danach automatisch eingeloggt.

Rollenkonzept

Dem Benutzer können über eine Zwischentabelle, Rollen zugewiesen werden. Diese Rollen ermöglichen dem Benutzer verschiedene gesicherte Ressourcen einzusehen, oder auf API-Endpoints mit Rollenbasierter Sicherung zuzugreifen.

Bruteforce

Bruteforce wird verhindert durch das Verfolgen von Login Versuchen auf eine bestimmte E-Mail. Nach 3 fehlerhaften Login Versuchen wird der Account für 1h gesperrt.