Projektdokumentation SecJSFApp

Paul Stonjek

Inhalt

Einrichtung in Eclipse unter Verwendung von MySQL und Tomcat

Das Projekt ist in einer .ZIP file enthalten. Diese muss entpackt und im Eclipse workspace geöffnet werden. Danach muss Eclipse auf die „Java EE“ Perspektive eingestellt werden.

Zusätzlich zum Projekt liegt eine .SQL datei vor, welche das Datenbankschema und alle zugehörigen Tabellen enthält. Dies wird benötigt, um die Kollation der Tabellen auf „utf8mb4_unicode_ci“ zu stellen, da alles weitere Probleme mit dem Hashing der Passwörter verursachen kann.

Es ist zu beachten, dass die META-INF/persistence.xml gültige Zugangsdaten mit Administrator-Berechtigung zur Datenbank enthält. Diese können vom Anwender beliebig gesetzt werden.

Verwendung und Funktionen

Registrierung und Login

Sowohl Registrierung als auch Login erfolgen über eine Email-Adresse und ein Passwort. Nach der Registrierung wird man sofort eingeloggt. Ausloggen erfolgt manuell über eine Schaltfläche oben rechts.

Nach einmaliger Registrierung kann man sich unter Angabe der verwendeten Email-Adresse und des Passworts einloggen.

Einziger existierender Benutzer ist Admin (Username: „admin“, Passwort: „admin“).

Anlegen und Managen von Geheimnissen

Das Anlegen und Managen von Geheimnissen wurde nicht implementiert.

Abdeckung von Kriterien

Allgemein

- Es sind ausschließlich die Registrierung und das Login von Benutzern implementiert.
- Das Anlegen und Managen von Geheimnissen wurde nicht implementiert.
- Ebenfalls wurde die Verwaltung von Nutzern als Admin weggelassen.

Sicheres Sessionhandling

- „Protected“ Seiten auf dem Server sind geschützt und können nicht ohne Anmeldung aufgerufen werden.
- Passwörter werden im Klartext übertragen, serverseitig gehasht und gesalzen unter Verwendung eines 16 Zeichen langen Salt und einer SHA256-Hashfunktion.
- Session Fixation wurde nicht berücksichtigt, und keine Gegenmaßnahme wurde implementiert.

Absicherung Standardangriffe

- Injections werden durch die Verwendung von Named Queries verhindert.
- XSS-Angriffe werden nicht aktiv verhindert.

Errorhandling, Logging

- Die Fälle, dass ein falsches Passwort zum Login oder ein existierender Nutzer zur Registrierung verwendet werden, sind abgesichert und mit speziellen Warnmeldungen versehen.
- Eine 404-Seite existiert nicht.
- Logging von Fehlern wird nicht durchgeführt.

CSRF-Absicherung

- CSRF-Angriffe wurden nicht abgesichert.