Pflichtenheft zur "Authentication and Authorisation" von inspectIT

Maximillian Rösch, Lucca Hellriegel, Thomas Sachs, Mario Rose,
Andreas Herzog, Clemens Geibel, Joshua Hartmann und Phil Szalay

16. August 2015

Inhaltsverzeichnis

0.1 Passwortspeicherung

Da unserem System mehrere Benutzer mit verschiedenen Rechten handhaben können soll, müssen wir die einzelnen Benutzer mit einem Passwort sichern. Zur Speicherung der Passwörter eignet sich eine Datenbank wohl am besten, weitere Aspekte sind unten beschrieben.

0.1.1 Passwort vergessen

Sollte ein Benutzer sein Passwort vergessen haben, soll es möglich sein, sich ein neues Passwort an seine E-Mail-Adresse schicken zu lassen.
Dadurch besteht die Möglichkeit, wieder Zugriff auf den Benutzer erhalten zu können, sollte man sein Passwort vergessen haben.

0.1.2 Passwortsicherheit

Wir nehmen nicht an, dass beim Betrieb des System eine sehr große Zahl an Benutzern aufkommen wird.
Deshalb haben wir uns dazu entschieden, nicht die aufwändigste Art der Passwortspeicherung zu nutzen, die uns davor schützen würde, dass im Fall von gestohlenen Daten die Passwörter von allen Nutzern schnell bekannt werden würde.
Entschieden haben wir uns für einen guten Mittelweg aus Sicherheit und Performance sowie Einfachheit.
Wir speichern die Passwörter als gesalzene Hash-Werte ab und prüfen bei der Anmeldung entsprechend nach, ob der Hash-Wert des eingegebenen Passworts mit dem gespeicherten Wert übereinstimmt.

0.2 Benutzermanagement

0.2.1 Benutzer anlegen

Mit entsprechenden Rechten ist es möglich, neue Benutzer in dem System anzulegen. Für einen Benutzer speichern wir dabei folgende Informationen:

1. Benutzername
   Ein eindeutiger Benutzername, mit dem ein einzelner Benutzer im System identifiziert werden kann.

2. Passwort-Hash
   Zur Sicherheit speichern wir das Passwort der Benutzer nicht im Klartext ab, sondern nur als Hash. Näheres dazu im Abschnitt über die Passwortsicherheit.

3. E-Mail Adresse
   Falls der Benutzer benachrichtigt werden muss, zum Beispiel falls er sein Passwort vergessen haben sollte. [Nice-To-Have: vielleicht auch, falls z.B. seine Rolle geändert wurde?]

4. Rolle
   Jeder Benutzer hat intern eine Rolle zugewiesen, die jeweils bestimmte Berechtigungen zusammenfasst.

0.2.2 Rollen anlegen

Mit entsprechenden Rechten ist es möglich, neue Rollen in dem System anzulegen. Für eine Rolle speichern wir dabei folgende Informationen:

1. Identifikationsnummer
   Eine eindeutige Identifikationsnummer, mit der eine Rolle im System gekennzeichnet ist.

2. Titel
   Ein kurzer Titel, der die Rolle beschreibt.

3. Berechtigungen
   Eine Liste mit allen Berechtigungen, die einer Rolle zugewiesen wurde.

0.2.3 Berechtigungen anlegen

Mit entsprechenden Rechten ist es möglich, neue Berechtigung in dem System anzulegen. Für eine Berechtigung speichern wir dabei folgende Informationen:

1. Id
   Eine eindeutiger Identifikationsnummer, mit der eine Berechtigung im System gekennzeichnet ist.

2. Titel
   Ein kurzer Titel, der die Rolle beschreibt.

3. Beschreibung
   Eine detailliertere Beschreibung, was die Berechtigung für einen Zweck hat.

0.2.4 Benutzern neue Rolle zuweisen

Mit entsprechenden Rechten ist es möglich, einem Benutzer eine neue Rolle zuzuweisen.

0.2.5 Rollen bearbeiten

Mit entsprechenden Rechten ist es möglich, einzelnen Rollen weitere Berechtigungen zuzuweisen oder zu entziehen.