HOCHSCHULE
HANNOVER
UNIVERSITY OF
APPLIED SCIENCES
AND ARTS
–
Fakultät IV
Wirtschaft und
Informatik

Anforderungsbeschreibung der von uns implementierten Zusatzfunktionalitäten

Dennis Grabowski, Julius Zint, Philip Matesanz, Torben Voltmer

Masterprojekt „Entwicklung und Analyse einer sicheren Web-Anwendung“
Wintersemester 18/19

9. Dezember 2018

Inhaltsverzeichnis

1 Benutzerverwaltung

1.1 Zwei-Faktor Authentisierung

1. Ein angemeldeter Nutzer kann die Zwei-Faktor Authentisierung aktivieren.
2. Ein angemeldeter Nutzer, der zuvor die Zwei-Faktor Authentisierung aktiviert hat, kann diese auch wieder deaktivieren.
3. Hat ein angemeldeter Nutzer die Zwei-Faktor Authentisierung aktiviert, so muss er diese bei jedem Login-Versuch verwenden.
4. Sollte ein Nutzer seinen zweiten Faktor verlieren, muss er einem Administrator Bescheid geben, so dass dieser die Zwei-Faktor Authentisierung deaktiviert, sofern dieser den Akteur für vertrauenswürdig hält.
5. Die Zwei-Faktor Authentisierung ist so implementiert, dass es keinem statistisch möglich sein sollte, das Shared Secret zu erraten.
    - Wir nutzen hierfür eine Implementation basierend auf einem Time-Based-One-Time-Password.
6. Administratoren haben eine neue Administratorfunktion, mit welcher sie die Zwei-Faktor-Authentisierung eines anderen Nutzerkontos deaktivieren können. Diese Funktion wurde hinzugefügt für den Fall, dass ein Nutzer seinen zweiten Faktor verloren hat, da er sonst nicht mehr einloggen kann.

1.2 Passwort ändern

1. Ein angemeldeter Nutzer soll in der Lage sein, sein Passwort ändern zu können.
2. Für eine Passwortänderung muss ein angemeldeter Nutzer folgende Daten angeben:
    2.1. Aktuelles Passwort.
    2.2. Neues Passwort.
    2.3. Erneute Eingabe des neuen Passworts zur Bestätigung dieses Passworts.

2 Sessions verwalten

1. Ein angemeldeter Nutzer kann seine eigenen, aktiven Sessions betrachten.

2. Ein angemeldeter Nutzer kann seine eigenen, aktiven Sessions invalidieren.
3. Ein angemeldeter Nutzer kann zusätzlich alle bisherigen Logins betrachten.
4. Ein angemeldeter Nutzer kann seinen Session-Timeout einstellen:
   4.1. Der Session-Timeout soll in Minuten angegeben werden.
   4.2. Die absolute Mindestdauer einer Session beträgt 5 Minuten. Das ist auch der voreingestellte Wert.
   4.3. Die absolute Maximaldauer einer Session beträgt einen Tag (1440 Minuten).

3 Datei-Austausch

1. Ein angemeldeter Nutzer kann zusätzlich zu einer Datei, auf die er Zugriff hat, sehen, welcher Nutzer die Datei als letztes überschrieben hat.
2. Dateien sollen visuell hervorgehoben werden, um die Vertrauenswürdigkeit besser darstellen zu können:
   2.1. Eine Datei soll grün hinterlegt werden, wenn Diese Datei zuletzt durch den Nutzer beschrieben wurde.
   2.2. Eine Datei soll rot hinterlegt werden, wenn diese Datei zuletzt durch einen **anderen** Nutzer beschrieben wurde.
3. Ein angemeldeter Nutzer kann nach Dateien suchen:
   3.1. Diese Suchfunktion soll einem Nutzer in jeder Ansicht bereit stehen.
   3.2. Er kann nur nach Dateien suchen, auf die er durch eine Nutzer- oder Gruppenberechtigung Zugriff hat. Andere Dateien darf er nicht durch die Suche finden.

Appendix