Sharebucket Technische Projektdokumentation	
Author	Linus Degen, Noah Grun
Version	1.0
Datum	07.01.2019

Dieses Dokument beschreibt die Umsetzung der verlangten Kompetenzen aus den Modulen M133 und M151 in unserem Projekt.

Kompetenz A1 - Validierung des HTML und CSS Codes

Für die Validierung haben wir das Online-Tool von W3C verwendet.
Link HTML: https://validator.w3.org
Link CSS: https://jigsaw.w3.org/css-validator/
Dazu haben wir mit direktem Text-Input den CSS und HTML-Code in das Textfeld kopiert und wo nötig, die Errors und Warnings behoben.

Kompetenz B2 - Validierung & Speicherung der Informationen

Validierung: Clientseitig
Die clientseitige Validierung wird mit dem HTML5-Mechanismus für die Validierung realisiert. Jeder User-Input wird sowohl Client- als auch Serverseitig validiert. Clientseitig überprüfen wir unter anderem den Type, die maximale Länge und ob es sich um ein Pflichtfeld handelt oder nicht. Bei einer Passworteingabe prüfen wir mit einem Regulären Ausdruck, ob das Passwort mit dem gegebenen Format übereinstimmt (Gross- & Kleinbuchstaben, Zahlen, Sonderzeichen, min. 8 Zeichen, keine Umlaute).

Validierung: Serverseitig
Ist die clientseitige Validierung erfolgreich gewesen, so beginnt nun die serverseitige Validierung. Serverseitig wird hauptsächlich geprüft, ob ein Eintrag überhaupt vorhanden ist und ob die Länge dem Format des Datentyps in der Datenbank gerecht wird. Bei der serverseitigen Validierung des Passworts wird ebenfalls nochmals nach dem Regulären Ausdruck abgefragt. Die E-Mail-Adresse, welche bei der Registrierung angegeben werden muss, wird mit *FILTER-VALIDATE_EMAIL* auf ihre Gültigkeit überprüft. Schlägt die Validierung fehl, so wird eine Error-Meldung per Alert ausgegeben und die Registrierung ist fehlgeschlagen. Ist die Validierung erfolgreich, so werden die Daten im korrekten Format in die Datenbank geschrieben.

Kompetenz B3 - Speicherung von schutzwürdigen Informationen & Datenbankberechtigungen

Die einzige wirklich schutzwürdige Information, welche in der MySQL-Datenbank eingetragen werden muss, ist das Passwort eines Benutzers. Dieses wird nach neusten Technologien gehasht und mit einem zusätzlichen Salt versehen. Der Datenbankbenutzer von welchem aus die Applikation Werte in die Datenbank speichert ist nur mit Insert, Update, Delete, Select

Kompetenz B4 - Registrierung und Login

Bei der Registrierung werden folgende Daten vom User erfasst: Username, Vorname, Nachname, E-Mail und Passwort. Die Daten werden client- und serverseitig validiert und je nach Vertraulichkeit der Daten auch gehasht und mit einem Salt versehen.

Kompetenz B5 - Quellcode Strukturierung

Die Php Dateien in unserem Projekt sind in 3 verschiedene Ordner und somit Kategorien unterteilt: Views, Templates und Actions. Views sind die Hauptseiten, also verschiedene Unterseiten der Applikation welche aufgerufen werden können. Um diese möglichst klein zu halten und Wiederholung zu vermeiden, haben wir viele Teile in Templates exportiert welche dann in den einzelnen Views mit includes importiert haben. Die Actions haben keine Darstellung und sind ausschliesslich dazu da, etwas auszuführen. Meistens werden dabei Datenbankzugriffe gemacht. In jeder View werden alle benötigten Aktionen oben eingebunden und können dann gebraucht werden.
Das System wurde dadurch sehr erweiterbar und mit nur wenig Aufwand könnte jetzt eine neue View mit neuen Funktionen und Templates erstellt werden und anschließend verknüpft.

Kompetenz C1 - Usability

In unserem Programm achten wir besonders auf die Usability mit verschiedenen Meldungen, welche den User über Veränderungen informieren. Zusätzlich verwenden wir Icons und Fülltext für die Eingabefelder in den Formularen, dies ist nicht nur designtechnisch ansprechbar, sondern auch sehr nützlich für den Benutzer. Der Benutzer kann bei unserer Web-Applikation kaum etwas falsch machen.

Kompetenz C2 - Session-Handling, Funktionen autorisierter Benutzer

Wir speichern Informationen in Cookies, um die aktuelle Sitzung eines Users nicht zu beenden, wenn dieser die Seite in der selben Browser-Session erneut aufrufen möchte. So bleibt der User während der gesamten Sitzung eingeloggt, und ist nicht ständig verpflichtet, seine Benutzerdaten neu einzutragen. Im Userprofil, welches man durch einen Klick auf den Button in der Navigation aufrufen kann, findet der angemeldete Benutzer die Möglichkeit, sein Passwort zu ändern. Dort befindet sich auch die Funktion, um sich wieder auszuloggen. Angemeldete Benutzer können Projekte dem Board hinzufügen. Der erste Benutzer, welcher sich registriert, erhält zudem Administrations-Rechte. Ihm wird ein zusätzliches

Administrationsmenu im Dort ist es möglich ganze Projekte auf dem Board zu entfernen und Kategorien für die Projekte hinzuzufügen.

Kompetenz C3 - SQL-Injection, Script-Injection, Session-Hijacking

SQL-Injections werden in unserem Programmcode durch Prepared Statements für jeden Datenbank-Eintrag (User, Projekt, Kategorie) verhindert.

Script-Injections werden verhindert, indem man mit dem Befehl htmlspecialchars(trim(input)) spezielle Zeichen escaped.

Session-Hijacking wird verhindert, indem wir die Session-ID nach dem Login neu generieren lassen.

Kompetenz C4 - Erfassen, Ändern, Löschen zusätzlicher Daten in der Datenbank

Unsere Web-Applikation ermöglicht das **Erfassen** von Benutzern, Projekten und (im Admin-Bereich) Kategorien. **Verändern** lässt sich das Passwort jedes Benutzers, solche können ihr Passwort mit Eingabe des alten Passworts und des neuen Passworts wechseln. Admin-Benutzer haben die Möglichkeit, Projektideen zu **entfernen**. Jeder Benutzer hat Einsicht über seine Nutzerdaten im Userprofil und über die ganzen Projektideen auf dem Board. Es wird auch angezeigt, von welchem User die Projektidee gepostet wurde.