Entwicklung eines webbasierten ePortfolios

im Rahmen einer Umschulung zum Fachinformatiker - Anwendungsentwicklung

Moritz Mandler & Didier Zielke

5. Juni 2020

Ausbildungsbetrieb:
BFW Berufsförderungswerk Hamburg
Marie-Bautz-Weg ???
22159 Hamburg

Ausbilder:
Petra Treubel
Dr. Olaf Kubillus

Inhaltsverzeichnis

1 Einführung

Die IT-Solution & Design GmbH ist eine Lernfirma innerhalb des Berufsförderungswerks Hamburg GmbH (BFW). Als norddeutsches Zentrum für berufliche Rehabilitation und Integration ist das BFW Hamburg kompetenter Partner für Unternehmen, Träger der beruflichen Rehabilitation und Versicherungen und vor allem für Menschen, die aus gesundheitlichen Gründen ihre bisherige Tätigkeit nicht mehr ausüben können. Es soll eine einfache Plattform zur Veröffentlichung einer 'Mappe' der eigenen Arbeitsergebnisse geboten werden. Benutzer müssen sich authentifizieren und können dann die eigene Mappe bearbeiten. Innerhalb dieser Mappe, die hier nur eine Webseite darstellt, können beliebige Download-Dateien, Texte und Bilder eingefügt werden. So soll den Benutzern auch die Möglichkeit gegeben werden Lebensläufe, Arbeitsproben oder Zertifikate auf der eigenen Seite abzulegen. Die IT-Solutions & Design hat vom BFW Hamburg den Auftrag erhalten diese Webanwendung zu erstellen.

2 Projektdefinition

2.1 Ist-Analyse

Die Teilnehmer*innen des BFW müssen sich während ihrer Ausbildung auf einen Praktikums- und einen Arbeitsplatz bewerben. Viele Bewerbungen werden dabei per E-Mail versendet. Um eine E-Mail nicht zu groß werden zu lassen, werden dabei manchmal Arbeitsergebnisse, Zertifikate o. ä. nicht mit gesendet. Das könnte den Gesamteindruck im Bewerbungsprozess verschlechtern. Außerdem müssen die Teilnehmer*innen entscheiden, auf welche Unterlagen, Arbeitsproben und Bilder sie verzichten wollen.

2.2 Anforderungsdefinition (Soll-Konzept

Wie im Pflichtenheft angegeben (siehe Anhang) sollen folgende Anforderungen erfüllt werden:

i. Musskriterien

- Neuanlegen, Ändern und Löschen von Benutzern durch den Admin
- Jedem Benutzer ist eine Benutzerseite zugeordnet, die nur von dem jeweiligen Benutzer bearbeitet werden darf
- Neuanlegen, Ändern und Löschen von Texten (auch Links) auf der jeweiligen Benutzerseite
- Hochladen von Bildern und Pdf-Dateien innerhalb der Benutzerseite
- Berücksichtigung verschiedener Berechtigungsstufen (Admin, Benutzer, Gast)
- Nur registrierte Gäste dürfen die Inhalte der Benutzer einsehen. Anlegen eines Gasts über Formular mit Überprüfung der E-Mailadresse (Freischaltung des Gastaccounts über E-Mail-Link) und Versenden eines generierten Kennworts

ii. Wunschkriterien

- Gäste dürfen nur die Portfolios sehen, welche ihnen über eine Freigabe zugeordnet wurden.

iii. Abgrenzungskriterien

- Keine Überprüfung auf Verletzung von Urheberrechten oder Verstöße gegen das Datenschutzgesetz

3 Projektplanung

3.1 Ressourcenplanung

Als Ressource sollen ein PC mit der im Pflichtenheft angegebenen technischen Produktumgebung zur Verfügung gestellt werden. Für die Kalkulation wurde eine Stundenplanung gemacht. Zwei Personen sollen dem Projekt für die folgenden Arbeitsschritte zur Verfügung stehen.

Software-Entwurf	
Use-Case-Diagramm	4h
Klassenmodell	4h
Datenmodell	4h
Summe:	12h
Realisierung	
Entwurf der Testfälle	4h
Programmierung Geschäftslogik	24h
Programmierung Datenzugriffsklassen	10h
Programmierung Controller-Klassen	24h
Programmierung View-Klassen	20h
Summe:	82h
Tests	
Testfälle programmieren und durchführen	10h
Eventuelle Fehlerbeseitigung	4h
Summe:	
Abschluss	
Soll-Ist-Vergleich	6h
Dokumentation	25h
Übergabe	1h
Summe:	32h
Gesamtsumme:	**140h**

3.2 Kosten

Die Kosten für dieses Projekt belaufen sich bei einem Stundensatz von 35,00€ und einem Gesamteinsatz von 140Std. pro Person, wie aus der Ressourcenplanung hervorgeht, auf:

2 Personen * 140Std * 35,00€ = **9800€**

4 Projektdurchführung

4.1 Softwareentwurf

Zuerst werden die Anwendungsfälle ermittelt. Es wird drei Hauptanwendungsfälle geben. Die Nutzung als Administrator, als Benutzer und als Gast. Wir entscheiden uns für eine zentrale Login-Oberfläche und danach zu einer strikten Trennung der Hauptanwendungsfälle.

Aus Gründen der Einfachheit wird im Klassenmodell und im Datenmodell zwischen den Benutzergruppen Administrator, Benutzer und Gast über eine Eigenschaft „status“ unterschieden, ansonsten jedoch das gleiche Model genutzt. Es ist darauf zu achten, dass eine mögliche Doppelbelegung der Kombination E-Mail und Passwort vorkommen könnte. In diesem Fall kann das Login System keine eindeutige Zuordnung durchführen. Dieser Fall ist sehr unwahrscheinlich und wird daher nur für den Fall das ein Gast von mehreren Portfolios Berechtigungen mit dem gleichen Passwort erhalten hat, behandelt.

Für die Umsetzung der Wunschkriterien wird die **Benutzeroberfläche** unterteilt in:

- Ansichten aller Seiten des eigenen Portfolios mit Bearbeitungsmöglichkeit
- Möglichkeit zum erstellen und löschen neuer Seiten innerhalb des eigenen Portfolios
- Gästeverwaltung zum erstellen und löschen von Gästen des eigenen Portfolios und setzten derer Berechtigungen

Für die Umsetzung der Wunschkriterien wird die **Gastoberfläche** unterteilt in:

- Ansicht aller freigegebenen Seiten eines Gastes
- Downloadmöglichkeit der hinterlegten Dateien auf freigegebenen Seiten

Für die Umsetzung der Wunschkriterien wird die **Adminoberfläche** unterteilt in:

- Möglichkeit zum erstellen neuer Benutzer
- Übersicht aller existierenden Benutzer und Gäste mit Lösch-Option
- Möglichkeit zum erstellen neuer Administratoren
- Übersicht aller existierenden Administratoren mit Lösch-Option

All diese Hauptanwendungen sind über eine Navigationsleiste verfügbar.

Damit keine Karteileichen in der Datenbank entstehen, wird beim Löschen eines Gastes stets auch jede seiner Berechtigungen aus der Datenbank entfernt. Beim Löschen eines Users werden automatisch auch all seine Berechtigungen, seine Gäste und die Berechtigungen derer aus der Datenbank entfernt.

Bei allen Formularen wurde aus Sicherheitsgründen darauf geachtet keine Datenbank Id oder Ähnliches zur Identifizierung auf der Serverseite zu übergeben. Stattdessen wird ein Index in ein Array übergeben, welches lediglich erlaubte Aktionen zulässt. So ist keine Form-Manipulation bei beispielsweise dem löschen von Gästen möglich.

Ein weiterer Schwerpunkt ist die Sicherheit der Daten eines jeden Benutzers. Wir entschieden uns aus Gründen der performance nicht für die Speicherung von Dateien in der Datenbank.

Wenn bei dem Prinzip der Objektorientierung eine strikte Trennung der Zuständigkeiten von Klassen und Methoden beachtet wird, ist die Wartbarkeit des Codes einfacher. Hier ist ein einfaches MVCModell geplant, bei welchem die Model-Klassen die Geschäftslogik implementieren, die View-Klassen die Ein- und Ausgaben darstellen und die Controller-Klassen für die Verbindung dazwischen eingesetzt werden sollen.

Für jeden Anwendungsfall soll es mindestens eine Controller-Klasse geben, die über den Frontcontroller aufgerufen wird. Außerdem soll es Klassen geben, die für die Schnittstelle der ankommenden HTTP-Anfragen zuständig sind (Request) und Klassen, die für die Antwort benutzt werden (Response). Neben den reinen Modelklassen wird geplant, Datenzugriffsklassen zu implementieren, die für die Datenbankzugriffe (CRUD) verwendet werden sollen. Durch die Verwendung eines DAO-Interfaces könnte man schnell die Datenzugriffsklassen für andere Datenbanksysteme erweitert werden. Aus Zeitgründen wurde aber hierauf verzichtet.

4.2 Daten- und Klassenentwurf

Das Klassenmodell (Abbildung 2) und das Datenmodell (Abbildung 1) befindet sich im Anhang auf den Seiten 9 und 8.

Da ein Benutzer mehrere Seiten in seinem Portfolio haben kann, wurde hier eine 1:n Beziehung im Datenmodell genutzt. Da eine Seite sich aus mehreren Inhalten zusammensetzen kann, wird auch hier eine 1:n Beziehung im Datenmodell genutzt. Da ein Gast keine eigenen Seiten hat, wird eine Berechtigungs-Tabelle für Seiten der Benutzer genutzt. Ein Gast kann mehrere Berechtigungen haben, aber jede Berechtigung muss eindeutig einer Person zugeordnet sein. Daher wird hier eine 1:n Beziehung im Datenmodell genutzt.

Im Klassenmodell wird festgelegt, dass jeder User eine Liste von Seiten beinhaltet. Jede Seite beinhaltet wiederum eine Liste von Inhalten.

Jeder User wird definiert über eine eindeutige Id (Primärschlüssel), vorname, nachname , E-Mail und Passwort, sowie einen status der entweder admin, user oder guest heisst. Jeder User enthält zudem eine Liste von Seiten, welche, wenn vorhanden, definiert werden über eine eindeutige Id (Primärschlüssel), die Id des Seitenerstellers und den Titel der Seite. Jede dieser Seiten enthält zudem eine Liste von Inhalten, welche jeweils Dateinamen und/oder html/text enthalten.

Die Liste an Seiten eines jeden Users wird anhand der Berechtigungstabelle der Datenbank initialisiert. Bei einem Admin wird diese Liste also leer sein.

Damit für einen existierenden Gast oder Benutzer immer mindestens eine Seite mit Inhalt existiert, die nach dem Login angezeigt werden kann, entscheiden wir uns für eine Standard „Home“ Seite. Diese Seite kann jeder Benutzer selbst verändern und gestalten, jedoch nicht löschen. Diese Seite wird außerdem all seinen Gästen zur Begrüßung angezeigt, sprich die Berechtigungen werden automatisch jedem Gast gewährt und können nicht entzogen werden.

4.3 Realisierung

4.3.1 Übersicht

4.3.2 Programmierung der Geschäftslogik und der Datenzugriffsklassen

4.3.3 Programmierung der Controllerklassen

4.3.4 Programmierung der Viewklassen

4.3.5 Dateiverwaltung

Dateiupload Beim Upload von Dateien durch den Benutzer wird zunächst geprüft, ob es sich auch tatsächlich und eine hochgeladene Datei handelt. Aus Sicherheitsgründen werden danach die MIME-Types der Dateien geprüft und mit einem Array zulässiger Typen verglichen. So wird vermieden, dass der Benutzer Shell-Scripts, php-Scripts usw. hochlädt, selbst wenn er die Dateiendung ändert. Sollte die Datei zulässig sein, wird geprüft, ob bereits eine Datei mit gewählten Namen existiert und ggf. eine Meldung ausgegeben und der Upload abgebrochen. Ist diese Prüfung negativ wird geprüft, ob der Dateiname zulässig ist. Nach aktuellem Stand ist nur der Dateiname "defaultContentünzulässig. Wenn der Name zulässig ist, wird die Datei in den Ordner des Users verschoben und der Dateiname in der Tabelle *content* eingetragen.

Benutzerordner Jeder Bentuzer erhält beim Anlegen einen eigenen Ordner, der nach seiner ID benannt wird. In diesem werden seine Uploads gespeichert. Aus Sicherheitsgründen befindet sich der Benutzerordner außerhalb des Webroots um einen ungewollten Zugriff von Außen zu verhindern.

> **Alternative:**
>
> Es kann auch in den Tabellen *user*, *content* und *page* jeweils eine weitere Spalte hinzugefügt werden mit einer zufälligen Folge aus Buchstaben und Zahlen, die eine externe ID darstellen sollen. Dies erhöht nochmals die Sicherheit, da manche Daten über GET in der URL übermittelt werden.

Löschen von Dateien Will der Benutzer seinen Content löschen, so wird nicht nur der Datesatz aus der Datenbank gelöscht, sonder auch die Datei. Der Benutzer kann somit sicher sein, dass seine Dateien nicht auf ungewollt versteckt verbleiben. Hierzu wird zunächst ermittelt welches Betriebssystem auf dem Server läuft um mit dem korrekten Befehl die Datei zu entfernen:

```
53  if(strtoupper(substr(PHP_OS, 0, 3)) === 'WIN') {
54      unlink(USERS_DIR . $currentUser->getId() . '/' . $file);
55  } else {
56      shell_exec('rm ' . USERS_DIR . $currentUser->getId() . '/' . $file);
57  }
```

Verhalten bei Accountlöschung Möchte der Benutzer seinen Account vollständig löschen, so werden alle seine Dateien sowie sein Benutzerordner vom System gelöscht. Um dies sicherzustellen wird auch hier zuerst das Betriebssystem ermittelt. Bei Windows wird zunächst jede Datei einzeln gelöscht um anschließend den Ordner zu entfernen. Bei Linux Systemen sowie BSD und anderen unixoiden System kann der Ordner samt Inhalt mit einem an die Shell übergebenem Befehl gelöscht werden:

```
31  if(strtoupper(substr(PHP_OS, 0, 3)) === 'WIN') {
32      foreach (glob(USERS_DIR . $userId . "/*.*") as $filename) {
33          unlink($filename);
34      }
35      rmdir(USERS_DIR . $userId);
36  } else {
37      shell_exec('rm -rf ' . USERS_DIR . $userId);
38  }
```

Als Beispiel befindet sich der vollständige Code zur Accountlöschung durch den Admin im Anhang (Listing 1, Seite 7).

4.4 Tests

Test	Ziel	Ergebnis	Maßnahmen
Testname	Testziel, kurz beschrieben	Ergebnis	Maßnahmen, falls der Test nicht ausgefallen ist wie erwartet

5 Soll-/Ist-Vergleich

6 Fazit

Die Entwicklung des ePortfolios ermöglicht einen ersten Einblick in den Aufbau und Struktur von Social Media Seiten. Einer der wichtigsten Aspekte bei der Entwicklung stellt die Sicherheit dar und die jeweiligen Tests um diese zu erhöhen. Bei der Entwicklung ist uns aufgefallen, dass man sehr viele Optionen implementieren kann um den User größtmögliche Individualität zu ermöglichen. Auch beim Design gibt es sehr viel Spielraum, der ein erfahrener Webdesign nutzen kann um den Benutzer ein optisch ansprechendes Portfolio zu bieten, mit welchem er sich bei Kunden und potenziellen Arbeitgeber präsentieren kann.

7 Anhang

7.1 Code Listings

Listing 1: RemoveUserCommand.php

```
1  <?php
2      namespace classes\commands;
3
4      use classes\request\Request;
5      use classes\response\Response;
6      use classes\template\HtmlTemplateView;
7      use classes\mapper\UserDAO;
8      use classes\model\User;
9
10     class RemoveUserCommand implements Command{
11         public function execute(Request $request, Response $response) {
12
13             if (isset($_SESSION['admin'])){
14                 $currentUser = unserialize($_SESSION['admin']);
15             }
16             else{
17                 header('location: index.php');
18             }
19             if (!($currentUser instanceof User)){
20                 header('location: index.php');
21             }
22             if ($currentUser->getStatus() != "admin"){
23                 header('location: index.php');
24             }
25             $userDAO = new UserDAO;
26
27             if($request->issetParameter('deleteUser')){
28                 $userId = $request->getParameter('deleteUser');
29                 $userDAO->deleteUser($userId);
30
31                 if(strtoupper(substr(PHP_OS, 0, 3)) === 'WIN') {
32                     foreach (glob(USERS_DIR . $userId . "/*.*") as $filename) {
33                         unlink($filename);
34                     }
35                     rmdir(USERS_DIR . $userId);
36                 } else {
37                     shell_exec('rm -rf ' . USERS_DIR . $userId);
38                 }
39             }
40
41             $listOfAllUsers = $userDAO->readAllUsersWithPages("user");
42             $multiListArray = array();
```

```
43              for($i = 0; $i < count($listOfAllUsers); $i++){
44                  $multiListArray[$i][] = $listOfAllUsers[$i];
45                  $multiListArray[$i][] = $userDAO->readGuestListOfUser($listOfAllUsers
                        [$i]->getId());
46              }
47
48              $view = 'RemoveUser';
49
50              $template = new HtmlTemplateView($view);
51              $style = "default"; // provisorisch
52              $template->assign('style', $style);
53              $template->assign('userList', $multiListArray);
54              $template->render( $request, $response);
55          }
56      }
57  ?>
```

7.2 Abbildungen

Abbildung 1: Datenmodell

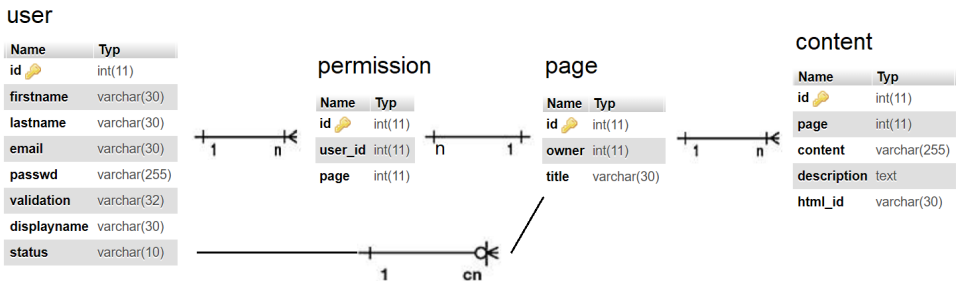

Abbildung 2: Klassendiagramm

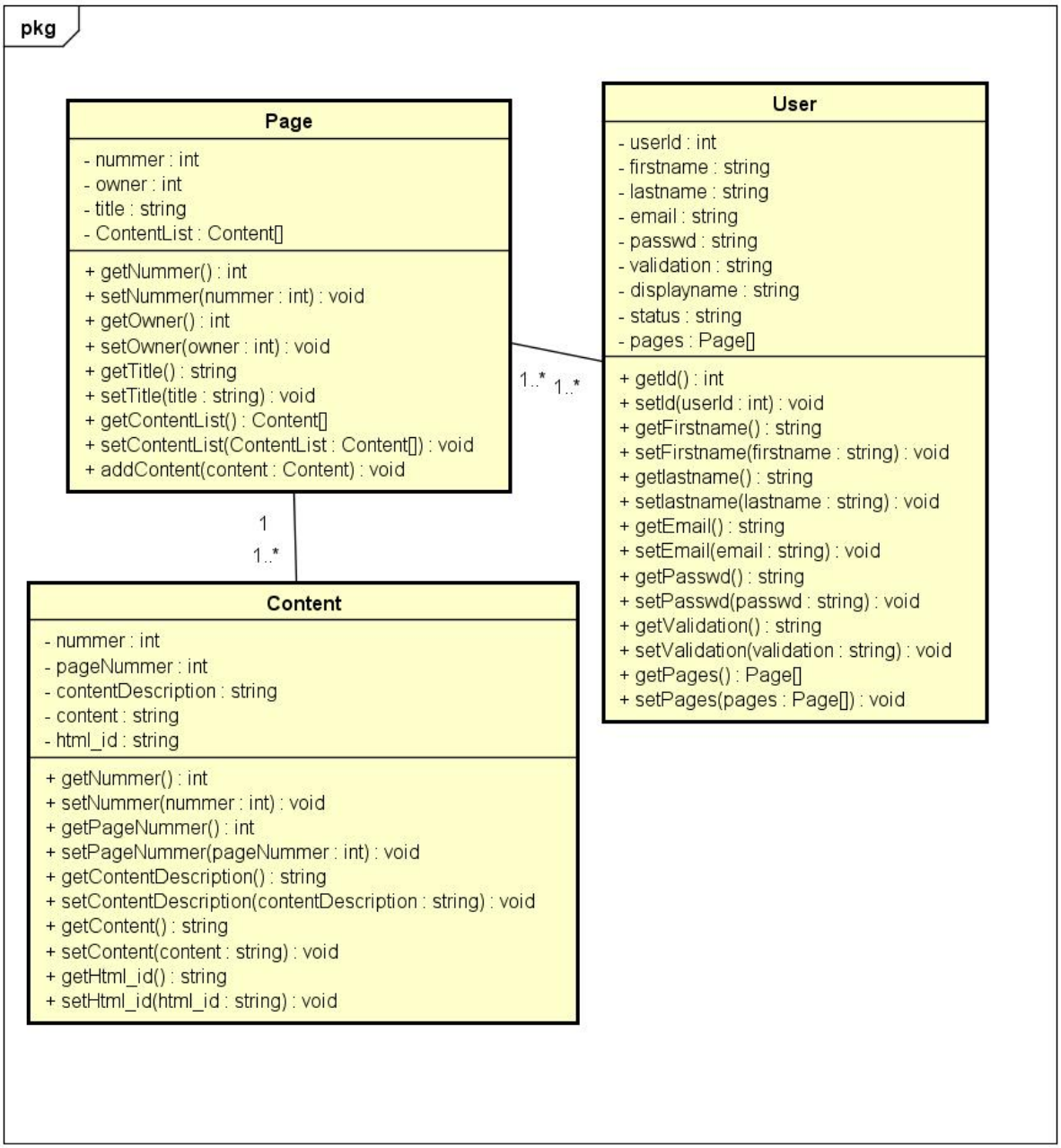

Abbildung 3: Use Case Diagram