Dokumentation: Weblog/Board-Projekt für das Fach 'Einführung in das Programmieren'

Christopher von Bargen (2239427)

Abgabe: 15. März 2017

1 Aufgaben der Software

1.1 Projektidee

Als Projektidee stand zunächst ein einfaches Weblog im Raum. Nutzer sollen sich mit Nutzerkonten registrieren können, Artikel verfassen und Artikel anderer Nutzer lesen können. Diese Einträge sollen dann kategorisiert werden können, beispielsweise in Kategorien wie Sport, Alltag, Filme, Musik etc.. Zusätzlich zu den Kategorien waren sogenannte Tags vorgesehen, mit denen Artikel noch genauer bezeichnet werden können. So ließe sich ein Artikel der Kategorie Filme eventuell mit Filmtitel, Darstellern, Genre und vielem mehr 'taggen', also markieren. Mit Hilfe der geplanten Suchfunktionm ergibt sich dann der Sinn dieser Tags ist es. Zum Einen können Suchen nach Artikeln, die sehr viele Resultate liefern, eingegrenzt werden, außerdem aber auch kategorieübergreifend zusammenhängende Artikel leichter mit der Suchfunktion gefunden werden.
Für die Hauptseite des Weblogs sollten die neusten Artikel aus allen Bereichen zusammengefasst werden, so dass der Nutzer einfach und vermeindlich ziellos in den Artikeln stöbern kann. Zum Zurechtfinden auf der Seite war außerdem noch eine Navigation geplant, welche anfangs nur die Bedingung 'sinnvoll hatte, allerdings ohne zu wissen, was in diesem Zusammenhang eigentlich sinnvoll ist. Weiter stand von Anfang an auf der Todo-Liste die Findung eines Designkonzepts mit Farben, Schriftarten und Seitenaufbau sowie das Erarbeiten eines Datenbank-Konzepts.
Aus Zeit- und Arbeitskraftmangel wurden nicht alle Vorhaben umgesetzt, dazu mehr im Fazit. Besonders im Design-Bereich wäre noch viel machbar gewesen.

1.2 Anwendung

Dieser Abschnitt geht auf die Aufgaben der Software im aktuellen Entwicklungsstand ein, berücksichtigt also nicht die nicht umgesetzten Aufgaben, welche bereits im vorherigen Abschnitt erwähnt wurden. Anwendungen einer möglichen Weiterentwicklung finden sich im Abschnitt 'Fazit und Auswertung'. Wichtige Anwendungsfälle sind beispielsweise: Registrierung und Anmeldung eines Nutzers an ein Nutzerkonto: Die Nutzer sind an Konten gebunden, so dass Artikel immer einem Benutzer zugeordnet werden können. In der Suchfunktion kann nach Autoren, also nach Beiträgen die von diesem Nutzerkonto aus verfasst wurden, gesucht werden. Es gibt auch schon ein Nutzerprofil, das bis dato allerdings nur die Beiträge des Nutzers zusammenfasst. Die Datenbank sieht neben Nutzernamen und Kennwort außerdem noch einen Beschreibungstext vor, der noch nicht genutzt werden kann. Lesen von Beiträgen: Die Softwäre ermöglicht durch Darstellung der zuvor geschriebenen Beiträge einem Nutzer das Lesen eben dieser. Auch wenn das vielleicht zu offensichtlich ist, handelt es sich bei der Darstellung der Texte dennoch um eine Aufgabe der Software. Auf der Hauptseite sind die Texte mit Titel, Text, Beitragsnummer, Datum und Autor vermerkt vorzufinden. Die Anzahl der angezeigten Beiträge ist zunächst begrenzt, doch der Nutzer kann selbstständig ältere Beiträge hinzuladen. Verfassen von

Beiträgen unbestimmten Inhalts: Nutzer schreiben unter ihrem Nutzernamen einen Beitrag mit Titel und Text von maximal eintausend Zeichen, der dann für alle - auch nicht angemeldete Nutzer - sichtbar ist. Diese werden dann zusammen mit allen anderen und geordnet nach Datum angezeigt und können im Nachhinein vom Autor - oder einem Administrator - gelöscht werden. Suchen von bestimmten Beiträgen: Nutzer können Beiträge in Titel oder Text nach bestimmten Inhalten durchsuchen, nach Beiträgen von bestimmten Autoren suchen, sowie beide Suchoptionen vereinen. Hier gibt es die Option, sich, anstatt der neusten, die ältesten Beiträge zuerst anzeigen zu lassen.

2 Installationsanleitung

2.1 Webserver

Zur Installation dieser als Internetanwendung konzipierten Software wird ein Webserver benötigt, um die HTML-Dokumente einem Client zur Verfügung zu stellen. Da die Anwendung mit PHP programmiert ist, muss PHP auf diesem Server installiert sein. Der Client auf der anderen Seite braucht dafür lediglich einen Webbrowser und keine virtuelle Laufzeitumgebungen oder Umgebungsvariablen, die konfiguriert werden müssen. Wärend der Umsetzung des Projekts wurde ein Apache Webserver benutzt, welcher über die Adresszeile unter 'localhost/' lokal erreichbar war. Eine einfache Möglichkeit, einen Webserver zu installieren, bietet das Bitnami-Stack WAMP[1], eine ausführbares Programm, welches Server automatisch einrichtet und laufen lässt.

2.2 Datenbank

Neben dem Webserver wird für die Software außerdem ein Datenbank-Server benötigt, der über die selbe IP erreichbar ist und auf dem das Datenbankverwaltungssystem MySQL installiert ist. Der Client kommuniziert nicht direkt mit der Datenbank, sondern ausschließlich über den Webserver, daher ist hier auch keine clientseitige Vorkehrung zu treffen. Desweiteren muss die Datenbank korrekt initialisiert werden, das heißt, dass Datenbankmanagementsystem muss über die benötigten Tabellen mit den zugehörigen Feldern und Attributen verfügen. Um das zu realisieren, gibt es die Möglichkeit, mit der bestehenden Datenbank eine Migration durchzuführen, oder mittels 'reverse Engineering' SQL-Skripte zu erstellen, welche man auf dem neuen Server laufen lässt, um die Datenbank einzurichten. Die während der Entwicklung genutzte Datenbanksoftware MySQL Workbench bietet beide Möglichkeiten und ist frei verfügbar. [2] Solche SQL-Skripte finden sich im Anhang dieses Dokuments.

[1] https://bitnami.com/stack/wamp
[2] https://www.mysql.de/products/workbench/

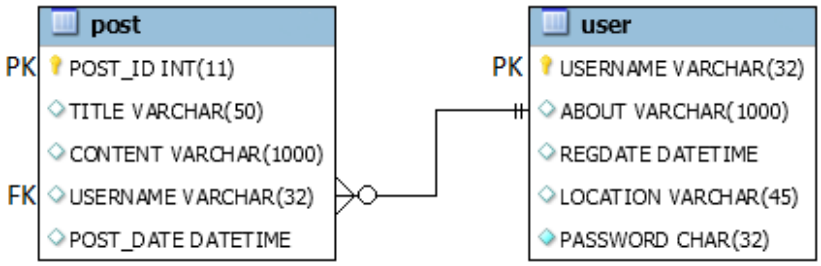

Figure 1: Crow's Foot-Diagramm der Datenbankstruktur. Jeder Beitrag hat einen Autor, Autoren können mehrere Beiträge verfassen.

2.3 Online-Demo

Momentan ist das Weblog online erreichbar auf dem Server der HAW. Die URL dazu lautet:

`http://abx427.pstud0.mt.haw-hamburg.de/`

Sämtliche Nutzer können getestet werden, die Kennwörter sind gleich der Nutzernamen, auch bei 'admin'. Natürlich können auch neue Nutzer registriert werden.

3 Bedienungsanleitung

Die bis dato noch sehr einfach gestaltete Webseite lässt sich in wenigen Schritten erklären. Öffnet man die Webseite, sieht man zunächst die Navigationsleiste und darunter die Blog-Ansicht. Die Navigationsleiste ist in jeder Ansicht der Seite sichtbar und ermöglicht die direkte Weiterleitung zu einer anderen Ansicht. Lediglich die Nutzerprofil-Seiten sind nicht direkt erreichbar. Links ist der Titel der Seite, der momentan einfach 'weblog' lautet, mittig die Hauptnavigation mit Blog, Write und Search, rechts befinden sich Register-, Login- oder Logout-Funktionen.

- Blog-Ansicht:
  In dieser Ansicht können auch ohne Anmeldung die letzten fünf Beiträge aller Autoren gelesen werden. Finden sich in der Datenbank mehr als fünf Beiträge, so erscheint unter dem letzten Beitrag ein Button, der es ermöglicht weitere Beiträge zu laden und zwar wieder fünf. Das kann solange wiederholt werden, bis alle Beiträge sichtbar sind. Der Wert 'fünf' ist übrigens zu Testzwecken gewählt, ein höherer Wert wäre an sich sinnvoll.

- Register-Ansicht: Ein Nutzerkonto anlegen
  Wird die Seite vom Nutzer zum ersten Mal geöffnet, hat dieser wahrscheinlich noch kein Nutzerkonto. In der Register-Ansicht kann er eins anlegen.

Hierzu wählt er einen Benutzernamen, welcher aus alphanumerischen Zeichen und dem Unterstrich bestehen darf. Dieser Name sollte noch nicht vergeben sein, anderenfalls, oder auch bei Verwendung eines unzulässigen Zeichen im Namen, wird einen Fehlernachricht dargestellt. Zum Nutzernamen wählt der Nutzer noch ein Kennwort und wiederholt dies einmal, um eine korrekte Eingabe zu verifizieren. Im Falle der Ungleichheit beider Eingaben, gibt es ebenso eine Fehlermeldung. Alle drei Felder müssen ausgefüllt werden. Das Abschicken des Formulars geschieht über den Button 'register'. Eine weitere Verifikation - beispielsweise über ein E-Mail-Konto - ist nicht umgesetzt. Die Register-Ansicht kann nur dann von der Navigation aus erreicht werden, wenn der Nutzer nicht bereits eingeloggt ist.

- Login-Ansicht: Anmelden in ein Nutzerkonto
  Ist ein Nutzerkonto angelegt, kann sich mit Nutzername und Kennwort eingeloggt werden. Falsche Eingaben werden erkannt und erzeugen eine Fehlermeldung. Ein Hinweis über das erfolgreiche Anmelden erfolgt. Als Angemeldeter Nutzer sieht man innerhalb der Navigation außerdem den Hinweis, unter welchem Namen man angemeldet ist. Ein Klick auf diesen Namen leitet den Nutzer zu seinem Nutzerprofil weiter.

- Logout-Button:
  Ist ein Nutzer bereits angemeldet, wird ihm in der Navigationsleiste statt des Logins die Möglichkeit zum Logout angeboten. Nach dem Abmelden kann der Nutzer sich wieder anmelden oder ein neues Konto registrieren.

- Write-Ansicht: Verfassen von Beiträgen
  Diese Ansicht enthält ein einfaches Formular, mit dem Beiträge verfasst werden können. Im ersten Feld, wird ein Titel eingegeben, darunter ein beliebiger Text. Mit einem Klick auf 'publish' wird dieser Beitrag dann veröffentlicht. Ein Auslassen eines der Felder ist nicht möglich. Die Titelzeile ist begrenzt auf 50, der Text auf 1000 Zeichen. Die Veröffentlichungen werden mit einer fortlaufenden Beitragsnummer sowie einem Zeistempel versehen. Eigens verfasste Beiträge können außerdem vom Autor gelöscht werden. Dies geschieht in einer beliebigen Ansicht, in der die Beiträge dargestellt werden. Unten rechts im Beitragsfenster findet sich dann ein Button mit einem 'X' darin. Falls ein Nutzer nicht angemeldet ist, wird er mit einem Hinweis auf die Login-Ansicht weitergeleitet.

- Search-Ansicht: Durchsuchen von Beiträgen
  Die Suchfunktion ermöglicht es, Beiträge nach einem bestimmten Inhalt zu durchsuchen, mit der Option, ausschließlich den Titel der Beiträge zu berücksichtigen ("only titles"). Außerdem kann man nach Beiträgen eines bestimmten Autoren suchen und beide Möglichkeiten kombinieren um Beiträge bestimmter Autoren mit bestimmten Inhalten zu finden. Standardmäßig werden diese nach zunehmendem Alter geordnet, beim setzen des Hakens 'oldest post first' wird diese Reihenfolge umgekehrt. Die Suchergebnisse werden sofort darunter angezeigt.

- Profile-Ansicht: Nutzerprofile.
  Klickt man auf einen Autorennamen unter einem Beitrag, so gelangt man zu dessen Profil. Diese Profile beinhalten jedoch momentan nicht mehr, als eine Ausgabe aller Beiträge des jeweiligen Nutzers. Um in das eigene Nutzerprofil zu kommen, befindet sich bei angemeldeten Nutzern innerhalb der Navigation ein Link dahin, der sich hinter dem Nutzernamen versteckt.

- Administration:
  Ein einziger Nutzer, nämlich der mit dem Nutzernamen 'admin' hat im Gegensatz zu anderen Nutzern die möglichkeit, Beiträge zu löschen, die er nicht selbst verfasst hat.

4 Systemarchitektur

Die Software wird von einem Webserver mit laufendem PHP zur Verfügung gestellt, welcher die Kommunikation mit den Clients regelt. Kommt eine Anfrage eines Clients, stellt der Webserver das angeforderte Dokument zusammen. In vielen Fällen werden dafür Daten aus der Datenbank benötigt, welche über sogenannte Queries, also Anfragen, vom Webserver angefordert werden. Die Verarbeitung des in SQL geschriebenen Querys übernimmt dann das Datenbankmanagementsystem. Queries können Daten zurückfordern, oder aber nur die Datenbank aktualisieren. Mit dem Rückgabewert wird dann das HTML-Dokument vom Webserver zusammengesetzt und an den Client weitergeleitet.

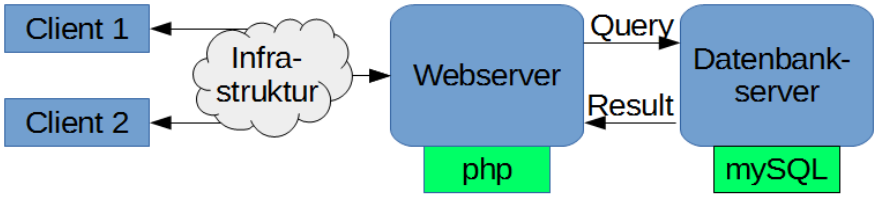

Figure 2: Schematische Darstellung einer Kommuikation zwischen Webserver, Datenbank und Client

5 Beschreibung eines technischen Teilaspektes

Mit Hilfe eines erfahrenen Testers wurden einige Sicherheitslücken aufgedeckt, mit denen ein Anwender potentiellen Schaden anrichten könnte. Da sie auch für unerfahrene Entwickler von Bedeutung sind, seien sie hier kurz erklärt.

5.1 Injektion durch HTML oder SQL

Durch die Formulare ist es möglich, Code an die Datenbank oder den Webserver zu schicken, welcher dann ausgeführt wird. Bezogen auf die Datenbank ließen sich also mit SQL-Injektion beispielsweise Passwörter auslesen. Diese sind zwar MD5-codiert, allerdings können sie mit einer Brute-Force-Methode geknackt werden. Wenn HTML-Code nicht richtig abgefangen wird, wird dieser vom Server dann in HTML-Elemente übersetzt. Anstatt Beiträgen, die dann nur aus Zeichen bestehen, sind nun auch beispielsweise Buttons mit Links zu anderen Webseiten etc. darin möglich. Sogar JavaScript lässt sich über das ¡script¿-Tag ausführen. Um solche Injektionen zu vermeiden, müssen Zeichenketten vor einem Übermitteln an die Datenbank mit der Funktion 'real_escape_string()' der Klasse mysqli gesäubert werden. Für HTML gibt es eine vergleichbare Funktion namens 'htmlspecialchars()'. Diese wird immer dann benötigt, wenn ein Nutzer Text eingibt, der an einer anderen Stelle wieder veröffentlicht wird.

5.2 Modifizierte Werte beim Abschicken von Formularen

Lässt sich ein Anwender Beiträge anzeigen, sieht er nur dann einen Löschen-Button, wenn dieser Beitrag von ihm selbst ist. Die Werte, die der Löschen-Button übergibt, identifizieren den dazugehörigen Beitrag anhand seiner POST_ID. Dieser Wert lässt sich allerdings von einem Anwender modifizieren und abschicken, wodurch Beiträge mit einer anderen ID gelöscht werden können, also auch solche, die derjenige gar nicht löschen darf. Hier wurde eine nachträgliche Verifikation nötig und eingebaut, die die ID des Beitrags und den Namen des angemeldeten Nutzers in der Datenbank abgleicht.

6 Fazit und Auswertung

Leider sind die Entwickler in puncto Gruppenarbeit nicht über die Konzeptionsphase herausgekommen. Die Umsetzung wurde dann nur noch von einem Entwickler durchgeführt. Dadurch sind viele Ziele auf der Strecke geblieben. Kategorien und Tags wurden nicht eingeführt, das Designaspekte (CSS) wurden minimal gehalten. Da es sich um das allererste PHP/Webseiten-Projekt des Entwicklers handelt, wurde außerdem viel Zeit in die Erarbeitung der Eigenheiten von HTML und PHP investiert. Nichtsdestotrotz gibt es einen funktionierenden und erweiterbaren Prototyp. Mögliche Erweiterungen neben den oben genannten Kategorien wären beispielsweise eine Kommentarfunktion für Beiträge, direkte, verborgene Nutzerkommunikation und ganz besonders mehr Kennwortsicherheit. Eine echte Administrator bzw. Moderatorfunktion wäre auch wünscheswert und die optische Darstellung hat noch viel Luft nach oben.

7 Anhang

1. github: https://github.com/zevau/weblog
2. SQL-Script zur Datenbankinitialsierung

```
CREATE TABLE IF NOT EXISTS `abx427_prg`.`user` (
  `USERNAME` VARCHAR(32) NOT NULL,
  `ABOUT` VARCHAR(1000) NULL DEFAULT NULL,
  `REGDATE` DATETIME NULL DEFAULT CURRENT_TIMESTAMP,
  `LOCATION` VARCHAR(45) NULL DEFAULT NULL,
  `PASSWORD` CHAR(32) NOT NULL,
  PRIMARY KEY (`USERNAME`))
ENGINE = InnoDB
DEFAULT CHARACTER SET = utf8;

CREATE TABLE IF NOT EXISTS `abx427_prg`.`post` (
  `POST_ID` INT(11) NOT NULL AUTO_INCREMENT,
  `TITLE` VARCHAR(50) NULL DEFAULT NULL,
  `CONTENT` VARCHAR(1000) NULL DEFAULT NULL,
  `USERNAME` VARCHAR(32) NULL DEFAULT NULL,
  `POST_DATE` DATETIME NULL DEFAULT CURRENT_TIMESTAMP ON UPDATE CURRENT_TIMESTAMP,
  PRIMARY KEY (`POST_ID`))
ENGINE = InnoDB
AUTO_INCREMENT = 20
DEFAULT CHARACTER SET = utf8;
```

   Findet sich außerdem im Projektordner unter /sql/

3. Server-URL zum Ausprobieren: http://abx427.pstud0.mt.haw-hamburg.de/
4. Externer Link: Bitnami Stack WAMP:https://bitnami.com/stack/wamp
5. Externer Link: MySQL Workbench: https://www.mysql.de/products/workbench/