Meilenstein 4 – E-Mensa

Abgabe: 8.12.2023

Ziel ist der Abschluss und die Fertigstellung der E-Mensa Werbeseite, deren Quelltext wir in Form eines Reviews überprüfen, für eine Sicherheitsprüfung vorbereiten und einreichen.
Zudem beginnen wir mit der Entwicklung der E-Mensa selbst, die wir auf der Werbeseite beworben haben. Dafür verwenden wir eine neue Architektur, das MVC-Muster, das uns eine bessere Organisation und Aufteilung des Quelltextes ermöglicht.

Empfehlung VL: Security

Aufgabe 1

Werbeseite: Wunschgericht. Die Werbeseite soll vor der geplanten Veröffentlichung durch die E-Mensa GmbH noch eine letzte Erweiterung erhalten: Besucher:innen der Werbeseite sollen die Möglichkeit haben, Wunschgerichte über die Werbeseite zu melden.

Sie erhalten folgende Beschreibung:
Ein Wunschgericht besitzt einen Namen, eine Beschreibung (z.B. Hinweise für die Zubereitung), ein Erstellungsdatum sowie eine eindeutige automatisch berechnete Nummer. Das Wunschgericht besitzt eine(n) Ersteller:in, zu welchem/r ein Name und eine E-Mail gespeichert wird. Ein(e) Ersteller:in kann viele Wunschgerichte eintragen. Gibt der/die Ersteller:in keinen Namen ein, soll als Name „anonym“ gespeichert werden.

1) Entwerfen Sie zur Beschreibung ein ERD und anschließend einen Datenbankentwurf in Relationenschreibweise.
2) Erzeugen Sie die Struktur mit SQL in der Datenbank.
3) Erweitern Sie die Werbeseite unter **/werbeseite/wunschgericht.php** um das notwendige Eingabeformular. Speichern Sie die Eingaben nach Betätigen der Schaltfläche „Wunsch abschicken“ in der Datenbank ab.
4) Fügen Sie einen Link auf der Hauptseite zur Erfassung eines Wunschgerichts ein.
5) Erstellen Sie mindestens 5 Testeinträge über die neue geschaffene Oberfläche.
6) Erstellen Sie eine SQL-Abfrage a), welche die neuesten 5 Einträge vollständig darstellt. Erstellen Sie eine weitere Abfrage b), die die Anzahl der Wünsche pro Ersteller:in zeigt.
   Zur Darstellung der Ergebnisse müssen Sie keine extra Webseite konstruieren. Eine Abfrage über ein Datenbankwerkzeug Ihrer Wahl ist ausreichend.

Aufgabe 2

Werbeseite: Security. Die E-Mensa GmbH möchte die Werbeseite online schalten. Bevor dies geschehen kann, müssen wir mögliche Schwachstellen wie XSS, SQL-Injection und CSRF beseitigen.

1) Sichten Sie Ihren vollständigen Quelltext der Werbeseite und beheben Sie sicherheitskritische Schwachstellen bzgl. XSS und SQL-Injection.
2) (Optional) Beheben Sie Schwachstellen bzgl. CSRF.
3) Dokumentieren Sie Ihre Fundstücke (und die Verbesserung) im Dossier.

*Hinweis: Einige **Abgaben** werden **zufällig ausgesucht** und anschließend durch Studierende höheren Semesters des Moduls „Development, Security and Operations“ von Prof. Dr. Georg Neugebauer auf **Schwachstellen hin überprüft**. Wurde Ihre Abgabe ausgewählt, so erhalten Sie voraussichtlich Mitte Januar den Prüfbericht und Sie erfahren, welche Schwachstellen beanstandet wurden und welche Gegenmaßnahmen wirksam sind.*
Das Ergebnis hat keine Auswirkungen auf Ihr Testat.
Sollten Sie im Team an der Security-Prüfung auf jeden Fall teilnehmen wollen, so tragen Sie Ihre Teamnummer sowie eine E-Mail-Adresse bitte ein unter:
Praktikum > Anmeldung Security-Check

Aufgabe 3 (optional)

Review durchführen. Im Rahmen dieser Aufgabe erhalten Sie die Möglichkeit zu Ihren bisherigen Arbeitsergebnissen weitere Rückmeldungen von einem anderen Team zu erhalten. (Zusätzlich haben Sie auch die Chance weitere Kommilitonen kennen zu lernen).

1) Sie erhalten die Kontaktdaten des anderen Teams via E-Mail in den kommenden Tagen.
2) Kontaktieren Sie das Ihnen zugewiesene andere Team und vereinbaren Sie einen Zeitpunkt für den gegenseitigen Reviewtermin in der nächsten Woche. Der Reviewtermin soll maximal 60 Minuten dauern. Bitten Sie das jeweils andere Team um die Zusendung der letzten Abgabe via E-Mail.
3) Führen Sie das Review des Quelltexts durch und achten Sie unter anderem auf die folgenden Aspekte:
   - Sind Dateien, Variablen, Funktionen, usw. zweckdienlich benannt?
   - Existieren Fehler im Quelltext?
   - Was würden Sie anders strukturieren?
   - Existieren Sicherheitsprobleme?
   - Was fällt Ihnen sonst am Quelltext auf?
   - Was haben Sie selbst durch das Lesen des anderen Quelltexts gelernt? Was würden Sie jetzt bei Ihrem Quelltext anpassen?

Verbringen Sie nicht mehr als 45 Minuten mit dem Review. Dokumentieren Sie Ihre Fundstücke für den Bericht im Dossier und den gegenseitigen Austausch mit dem anderen Team.

4) Führen Sie den Reviewtermin durch und stellen Sie sich Ihre Untersuchungsergebnisse (jeweils 30 Minuten) höflich und respektvoll gegenseitig vor. Organisieren Sie die Terminfindung mit dem anderen Team sowie die Durchführung selbst (z.B. mit einer Bildtelefonie-Software Ihrer Wahl).
5) Halten Sie neue Erkenntnisse im Dossier fest.
6) Teilnehmende Teams am Review können im letzten Meilenstein 6 eine von mehreren gekennzeichneten Pflicht-Aufgaben einsparen.

Hinweis: Als Hilfestellung zur Durchführung des Termins können Sie sich vorab https://phauer.com/2018/code-review-guidelines/ anschauen. Dort sind Tipps für die Durchführung eines Reviews beschrieben.

Aufgabe 4

E-Mensa: Nebenbedingungen in Datenbank. Zur weiteren Absicherung der Konsistenz der Daten und Erhöhung der Performanz sollen Erweiterungen in der Datenbank eingefügt werden. Verändern Sie die bestehende Datenstruktur um die folgenden Punkte, wobei Sie ALTER Statements verwenden und die verwendeten SQL-Abfragen in Ihr Dossier schreiben:

1) In Tabelle *gericht_hat_kategorie* soll eine Kombination aus Gericht und Kategorie einzigartig sein.
2) In der Tabelle *gericht* soll eine Abfrage nach Name beschleunigt werden.
3) Bei Löschung eines Gerichts sollen 1) die zugehörigen Zuordnungen zu einer Kategorie sowie 2) die zugehörigen Zuordnungen zu Allergenen automatisch mit gelöscht werden.
4) Eine Kategorie kann nur dann gelöscht werden, wenn 1) dieser keine Gerichte zugeordnet sind und 2) diese keine Kindkategorien besitzt.
5) Wird der Code eines Allergens verändert, so ändert sich dieser Code automatisch in den referenzierenden Datensätzen.
6) Eine Kombination aus *gericht_id* und *kategorie_id* in *gericht_hat_kategorie* soll als Primärschlüssel dienen.

Empfehlung VL: PHP Objekte Patterns, Templatesprache

Aufgabe 5

Übung PHP. Zur Einübung der neuen Sprachkonstrukte in PHP wollen wir zunächst den grundlegenden Umgang mit diesen erlernen. Dazu steht für Sie in ILIAS ein Test mit Fragen zum Thema Klassen und Muster bereit unter:

Praktikum > M4 > PHP Klassen und Muster Quiz

Führen Sie den Test so lange durch, bis Sie mit über 80% erreichten Punkten bestehen. Jede/r Einzelne von Ihnen muss den Test bestehen. Eine Abgabe eines einzelnen Teammitglieds reicht nicht aus. Sie können den Test beliebig oft wiederholen. Sie müssen den Test bestanden haben, bevor die Abgabefrist des Meilensteins endet.

Aufgabe 6

E-Mensa: Projektbeginn. Wir beginnen mit einem neuen Projekt, der E-Mensa, wozu wir die Grundsteine in einer neuen Architektur legen.

1) Legen Sie in Ihrer Entwicklungsumgebung ein neues Verzeichnis mit dem Namen **emensa** (neben den Verzeichnissen **beispiele** und **werbeseite**) an.
2) Sie erhalten die Datei **emensa.zip**. Die Datei beinhaltet bereits eine Grundstruktur für das Projekt „E-Mensa“.
3) Entpacken Sie die emensa.zip und kopieren Sie alle Inhalte in Ihren neuen Ordner **emensa**.
4) Wir verwenden die bestehende Datenbank ***emensawerbeseite*** weiter. Konfigurieren Sie Ihre Datenbank unter **/emensa/config/db.php**.
5) Starten Sie Ihren PHP-Built-In-Server mit dem Zielpfad (Dokumentenpfad) **/emensa/public**, öffnen Sie die Seite mit dem Webbrowser (z.B. http://localhost:9000) und lesen Sie die Informationen unter „Demo“.

*Hinweis: Sollten Sie bereits Erfahrungen mit dem **Framework Laravel** besitzen (oder einfach Lust haben es bereits jetzt kennenzulernen), so können Sie ab hier auch direkt mit Laravel in Eigenregie beginnen. Selbstverständlich sind alle folgenden Aufgaben auch mit Laravel sehr gut lösbar. Der Support leistet jedoch nur Unterstützung für die Lösung ohne den Einsatz von Laravel.*

Aufgabe 7

Übung. Die folgenden Übungsaufgaben verfolgen das Ziel den Umgang mit der Templatesprache Blade einzuüben, damit wir diese Templatesprache in den nachfolgenden Aufgaben besser beherrschen und sicherer einsetzen können.

Erweitern Sie für jede der folgenden Aufgaben im Projekt E-Mensa

- den gegebenen ExampleController (unter /controller) um eine Methode
- den Ordner /views um eine View und
- die web.php um eine Route,

so dass jede Aufgabe durch genau einen Pfad und eine Methode im ExampleController umsetzt ist. Verwenden Sie die Templatesprache Blade in den Views.

Schreiben Sie den mit dem Webbrowser erreichbaren Endpunkt …

a) `/m4_7a_queryparameter`, der einen Abfrage-Parameter *name* über eine URL (*?name=…*) in einem Controller empfängt und diesen an eine View weitergibt. Die View zeigt den Satz „Der Wert von name lautet: <name>“.
Der Name der verwendeten View soll sein:
views/examples/m4_7a_queryparameter.blade.php

b) `/m4_7b_kategorie`, der alle Namen der Kategorien der Gerichte in der Datenbank aufsteigend sortiert ausgibt. Jeder zweite Name soll (über CSS) fett ausgegeben werden.
Der Name der verwendeten View soll sein:
views/examples/m4_7b_kategorie.blade.php

c) `/m4_7c_gerichte`, der alle Namen und internen Preise von Gerichten, die intern mehr als 2€ kosten sortiert nach Name absteigend darstellt. Sind keine Gerichte zu finden, so soll der Text „Es sind keine Gerichte vorhanden“ dargestellt werden.
Der Name der verwendeten View soll sein:
views/examples/m4_7c_gerichte.blade.php

d) `/m4_7d_layout`, der die Anwendung eines Layouts in Blade demonstriert.
Schreiben Sie ein Layout unter
views/examples/layout/m4_7d_layout.blade.php mit drei unterschiedlichen Bereichen mit den Namen: *header*, *main*, *footer* sowie einer Variablen *title*, die den Titel der Seite im Layout setzt.
Schreiben Sie zwei Seiten, die das Layout mit unterschiedlichen Inhalten verwenden:
views/examples/pages/m4_7d_page_1.blade.php und
views/examples/pages/m4_7d_page_2.blade.php
Steuern Sie über den Controller über einen Abfrageparameter *no* in der URL, welche Seite der Controller laden soll (*?no=1* für m4_7d_page_1.blade.php und *?no=2* für m4_7d_page_2.blade.php). Ohne Parameter wird no=1 angenommen.

Aufgabe 8

E-Mensa: Hauptseite. Gestalten Sie im neu eingerichteten Projekt E-Mensa die Hauptseite unter / (Wurzelverzeichnis), wobei Sie das MVC-Muster verwenden.

1) Übernehmen Sie die bestehende Werbeseite als Hauptseite der E-Mensa, wobei Sie mindestens die folgenden Komponenten der Hauptseite wieder darstellen:
    a) Kopfbereich & Navigation
    b) Fußbereich & Copyright
    c) Begrüßungstext
    d) Gerichteübersicht

    … wobei Sie …
    a) CSS-Anweisungen in eine eigene Datei auslagern
    b) die übernommenen Quelltexte entsprechend der Belange von MVC aufteilen
    c) ein Layout für die Hauptseite verwenden (Blade: @extends).
2) Stellen Sie sicher, dass das ausgelieferte HTML-Dokument valide ist.

Aufgabe

Abgabe. Sie geben Ihre erarbeiteten Ergebnisse des Meilensteins ab.

1) Aktualisieren Sie Ihr Dossier.
2) Prüfen Sie im PTV, ob Ihre vorherige erfolgreiche Abnahme eingetragen ist.
3) Laden Sie Ihre Ergebnisse als ZIP in ILIAS hoch.
   Bennen Sie das ZIP, das Sie *zweimal zippen*, nach dem folgenden Muster:

   <TeamNr>.zip

   Die TeamNr (bzw. Team ID) finden Sie bei der Teamzuordnung in ILIAS unter Praktikum.