Dokumentation Projekt Ikarus

Prüft Benutzereingaben

Wir validieren sämtliche Benutzereingaben auf den Seiten userlogin, createuser, changePassword, BlackJack und Roulette.
Diese Eingaben validieren wir sowohl clientseitig als auch serverseitig. Clientseitig validieren wir mithilfe von input type, max/min und required.
Serverseitig überprüfen wir ob einen Wert gesetzt wurde, die max länge nicht überschritten wurde, ob die Passwörter dem Pattern entsprechen und ob angegebene Emailadressen einem vordefinierten Filter einhaltet.

Speicherung und Datenbankkommunikation

Die Daten werden alle in sinnvollen Grössen und Datentypen abgespeichert. Zudem wird das Passwort mit dem md5 Hash Algorithmus gehasht in die Datenbank geschrieben.
Die Webseite hat für die Kommunikation mit der Datenbank einen eigenen User. Dieser User ist so stark wie möglich eingeschränkt. Er hat nur Rechte auf diese eine Datenbank und ist nur berechtigt Select, Insert, Delete und Update Befehle auszuführen.

Registrierung und Login mit sinnvollen Daten

Um unsere Seite nutzen zu können ist eine Registrierung notwendig, da man Geld braucht, um die Spiele zu spielen, welches man nur mit einem User hat.
Zur Registrierung gibt man den Namen, den Vornamen, den Usernamen, die E-Mail-Adresse. Zudem gibt man zweimal das Passwort, zur Sicherstellung, dass man sich nicht vertippt hat, an. Dabei ist es nicht möglich zwei User mit dem gleichen Usernamen zu erstellen.
Wenn man sich anmelden will, muss man den Usernamen, sowie das Passwort eingeben.

Projektplanung

Am Anfang des Projektes haben wir ein neues Board auf Trello erstellt. Danach haben wir folgende Listen hinzugefügt: "Über Thema informieren", "Dinge, die erledigt werden müssen", "Im Gange" und "Fertig".
Daraufhin haben wir begonnen Karten zu definieren. Im verlauf des Projektes sind jedoch immer wieder neue Karten dazugekommen.
Die Funktionen Kommentare schreiben und Checklisten haben wir 1 – 2 Mal ausprobiert, jedoch nicht weiterverwendet.
Die Karten haben wir aktiv geführt, das heisst die Karten wurden immer in der richtigen Liste geführt.

Usability

Die Bedienung unserer Webseite ist simpel und leicht verständlich gestaltet. Der User wird bei wichtigen Ereignissen mit den notwendigen Informationen versorgt. Zum Beispiel beim Ändern des Newsletterabos wird der User über den neuen Status informiert.

Sessionhandling, Passwortänderung und zusätzliche Funktionen

Wie zuvor schon erwähnt, ist es notwendig sich auf der Seit zu einzuloggen, um sie nutzen zu können. Wenn man nicht eingeloggt ist, kommt man nur auf die Login und Registrierungsseite.
Sobald man sich eingeloggt oder registriert hat, wird eine Session erstellt und ein Login Parameter hinzugefügt. Sobald dieser Parameter gesetzt ist, hat man Zugriff auf alle Seiten.
Normale Benutzer können auf der Home Seite beim User Icon den Newsletter abonniere/deabonnieren und das Passwort ändern.
Der Admin User hat nicht die Möglichkeit seinen User zu löschen und den Newsletter zu abonnieren. Dafür hat er Zugriff auf eine zusätzliche Seite (Statistik Seite). Auf der Statistikseite kann er sämtliche Daten, welche von den Usern gesammelt wurden, sehen.

SQL-, Script-Injection und Session-Hijacking

SQL-Injection verhindern wir mit dem Nutzen von prepared statements bei den Datenbankabfragen.
Script-Injection verhindern wir einerseits mir der Validierung der Eingaben. Andererseits entfernen wir nach dem Validieren mit htmlspecialchar alle html tags.
Session-Hijacking verhindern wir durch das ständige Wechseln der Session ID.

Erfassen, ändern und löschen von Daten, welche Admin ansehen kann.

Auf der Home Seite kann man entscheiden ob man zusätzlich den Newsletter abonnieren will oder nicht.
Die IkarusCoins werden bei jedem Spiel, abhängig von dem was der User setzt, geändert.
Zudem kann man sein Passwort ändern.
Wenn man den Account nicht mehr möchte, kann der Benutzer sich selbst löschen.
Dementsprechend löscht er damit auch die Daten von ihm von der Datenbank.

Wie schon vorhin erwähnt hat der Admin eine Statistik Seite auf der er einige Daten sehen kann.
Folgende Daten werden angezeigt:

- Anzahl gespielte Black Jack spiele
- Anzahl gespielte Roulette spiele
- Black Jack Gewinne
- Roulette Gewinne
- Gewonnenes Geld im Black Jack
- Gewonnenes Geld im Roulette
- Ausgegebenes Geld im Black Jack
- Gewonnenes Geld im Roulette

Diese Daten können normale Benutzer nicht ansehen.
Der normale User kann stattdessen einfach sein Vermögen an Ikaruscoins sehen und ob er den Newsletter abonniert hat oder nicht.

Strukturierung Quellcode

Durch das Einrücken des Codes ist er schön übersichtlich und gut strukturiert. Ordner machen die Strukturierung der Files ebenfalls ordentlicher.
Der Code wurde wie vorgegeben Kommentiert, sodass es einfacher ist ihn zu lesen.