Dokumentation Projekt LB3 Modul 183

Übersicht

Das Projekt wurde mit php, Javascript, HTML5 CSS 3 und Bootstrap erstellt. Verwendet wurde ein schlankes MCV Framework welches Sascha Blank in früheren Projekten erstellt hatte.

Im folgendem eine Liste der Klassen welche aus dem Framework stammen:

- BaseModel
- Dispatcher
- SessionManager
- View

Login

Für das Login werden die Klassen LoginController und UserModel verwendet. Die Felder aus der Anfrage wird per htmlspecialchar escaped. Die Anfrage wird an den LoginController geleitet. Dieser liest die Anfrage aus und fürt über die UserModel Klasse den Datenbankzugriff aus. Im UserModel wird nur der Passwordhash, aus der Datenbank, angefragt. Zu diesem ZWeck wurden Preparedstatements verwendet(Verhindern von SQL Injections). Der Rückgabewert aus der getPasswordHashByUserName Methode im UserModel liefert das Password zurück, sofern der Eintrag für diesen Benutzer vorhanden ist. Das Passwort aus der Anfrage wird anschlissend mit der password_verify Methode(PhP Funktion) verifiziert.

Neuer Benutzer Registrieren

Um einen neuen Benutzer anzulegen, wird die Klasse Logincontroller mit der Methode newUser verwendet. Die Felder aus der Anfrage wird per htmlspecialchar escaped. Diese Methode prüft, mit Hilfe der UserModel Klasse ob ein Benutzer mit dem Namen schon vorhanden ist und zeigt gegebenfalls im RegisterView ein Fehler an. Falls der Benutzer erfolgreich angelegt wurde, wird wieder das Login angezeigt. Um das Passwort des Benutzers in der Datenbank zu hinterlegen wird die Php Funktion password_hash mit dem Parameter PASSWORD_BCRYPT verwendet. Diese Methode generiert einen Hash aus dem Passwort. Ein Salt für den Hash zu erstellen ist nicht nötig da die password_hash Funktion dies standardmässig erledigt. Deshalb ist auch eine “Salt” Spalte in der Datenbank nicht notwendig.

Session Handling

Die Session wird über die SessionManager Klasse verwaltet. Diese Klasse stellt einen Wrapper um die PhP Session dar. Gestartet wird die Session über session_start() Methode. Der SessionManager setzt einen bool Wert, in die Session, wenn sich ein Benutzer erfolgreich angeldet hat. So kann festgestellt werden ob ein Benutzer eingelogt ist und kriegt, in diesem Falle, den MainView, in welchem die Systemkommandos ausgeführt werden können, präsentiert.

Sichere persistente Passwortspeicherung, gegen Wörterbuchangriffe

Um sich gegen Wörterbuchangriffe zu schützen wurden folgende Massnahmen ergriffen:

- Passwort wird mit Salt gehasht (siehe Abschnitt Neuer Benutzer registrieren).
- Das Passwort muss 8 oder mehr Zeichnen enthalten.
- Das Passwort muss Gross-und Kleinbuchstaben enthalten
- Das Passwort muss Zahlen enthalten.

Für die Validierung des Passworts werden 3 Regex im LoginController verwendet(LoginController Zeile 69 -71). Erst nach der Validierung des Passwortes wird eine neues Record in der Datenbank mit den Benutzerdaten angelegt. So sollte sichergestellt werden das ein ausreichend sichers Passwort gesetzt wird, welches schwer mit einem Wörterbuchangriff geknackt werden kann.

SSL/TLS

Der Server läuft in einer geschlossenen Umgebung, die über einen Gateway im Netz verfügbar ist. Dieser Gateway holt bei https://letsencrypt.org ein offiziell gesigntes Zertifikat um https für alle Server der Umgebung zu ermöglichen. Dieses Zertifikat wird automatisch erneuert und von den gängigen Browsern erkannt.

Logs

Es wird pro Tag ein Logfile erstellt. Diese Logs werden in eine Datei mit dem Namen yyyy.mm.dd.log unter dem Ordner php/logs gespeichert. Es werden die Schritte Anmelden, Registrieren und das Ausführen der Systemkommandos gelogt. Beim Anmelden wird der anmeldende Benutzer geloggt, beim Registrieren den neuen Benutzer und bei den Systemkommandos das Kommando mit Optionen und dem Ausführenden Benutzer.

Systemkommando absetzen

Um ein Systemkommando abzusetzen, wird die Klasse SystemCommandController mit der Mehtode executeSystemCommand verwendet. Die eingegeben Optionen des Users werden anhand einer Whitelist überprüft. Diese Whitelist enthält alle erlaubten Eingaben. Sind die Eingaben des Users valid, so werden diese an das Kommando angehängt. Anschliessend wird das Kommando abgesetzt und die Ausgabe an die View übergeben. Die Whitelist, sowie auch das Kommando sind systemspezifisch. Läuft der Server unter Windows, wird das Kommando “ipconfig” ausgeführt. Unter Linux wird “ls” ausgeführt.