**Reflexion**

Ich hatte es mir zur Aufgabe gemacht das Frontend für den Login- und Registrationsbereich zu programmieren und zu gestalten. Hier für musste ich genau wissen, wie das geschriebene Backend von Fabian genau funktioniert; sowohl was sein Backend von mir an Eingaben erwartet als auch was ich für Informationen erhalte. Da ich recht wenig von Backend-Programmierung verstehe, musste Fabian sehr viel Geduld mit mir haben. Er hat mir alles hervorragend erklärt, ging auf sämtliche meiner Fragen ein und bewies sehr viel Geduld.   
Schließlich war ich in der Lage die Usereingaben ans Backend zu übergeben, ein Token zu erhalten und mit dem Erhalt das Spiel zu starten.  
Des Weiteren hat Fabian mich darin unterrichtet, wie man eine SSL-Zertifizierung einrichtet.

**Frontend Login**

Die Eingaben des Nutzers werden sowohl bei der Registrierung als auch beim Login in Variablen gespeichert („username“ und „password“). Diese werden dann ans Backend übergeben und entweder im Falle der Registrierung wird ein neuer Nutzer angelegt oder im Falle eines Logins erhält der Nutzer ein Token. Dieses Token wird im Session Storage gespeichert, damit der Nutzer eingeloggt bleibt, solange er sich auf der Seite befindet.  
Besitzt der Nutzer ein Token, so ist es ihm gestattet weiter als bis zum Login oder zur Registration zu gehen und ist in der Lage das Spiel zu starten.

**SSL-Zertifizierung**

Eine SSL-Zertifizierung ist essenziell erforderlich für Seiten, auf denen ein Login stattfindet, wie bspw. bei Banken, Online Shops oder eben unserem Spiel.  
Ist eine Seite SSL geschützt, so ist es Hackern deutlich erschwert die Eingaben des Nutzers abzufangen und für sich zu benutzen. Die Verschlüsselung dient dazu die Kommunikation zwischen Datenbank und Login sicher zu stellen und sicher zu stellen, dass kein Dritter an diese Daten kommt. Das schafft das Protokoll, indem es immer wieder in regelmäßigen Abständen Prüfziffern an beide Kommunikationspartner schickt und diese abgleicht. Im Grund ist SSL ein reines Aufzeichnungsprotokoll. Aber auch schon bevor Daten ausgetauscht werden, sorgt SSL für die Übermittlung persönlicher Identifikationsdaten der Teilnehmer. Es sorgt dafür, dass beide Teilnehmer sich auf eine Art der Fragmentierung und Kodierung einigen und nur diese verwenden.  
Man sollte bei der Eingabe von persönlichen Daten immer darauf achten, dass die Website „https“ enthält, denn nur so kann man relativ sicher gehen, dass man an der Stelle in keine Phishing-Falle läuft.