**Pflichtenheft (Sicherheit)**Gruppe: Timo Schmahl, Kevin Graß, Fritz Sengelmann, Fabian Brinkmann, Tom Stich und David Loos  
Ziel: Sicherheitskonzept in ein Browsergame implementieren.

|  |  |
| --- | --- |
| Zielbestimmung, Funktionen und Leistungsumfang | |
| Musskriterien | * Registrierfunktion * Login-Funktion   + Passwörter in der Datenbank nicht in Klartext speichern (“hashen“) * SSL-Verschlüsselung |
| Wunschkriterien | * IP-Firewall * Email-Verifikation   + Validierung * Passwörter „salten“ |
| Abgrenzungskriterien | * Passwort-Reset |

|  |  |
| --- | --- |
| Zielbestimmung, Funktionen und Leistungsumfang | |
| Musskriterien | * Der User kann sich mit einem Usernamen und einem Passwort registrieren * Der User kann sich mit seinem Usernamen und seinem Passwort anmelden * Dem Passwort wird eine zufällig generierte Zeichenfolge angefügt und mittels SHA256 gehasht. Dieser Hash wird anstelle des Passworts in der Datenbank gespeichert * Sämtliche Kommunikation zwischen Client und Server wird mittels SSL verschlüsselt |
| Wunschkriterien | * IP-Firewall * Email-Verifikation. Bei der Registrierung wird an die vom User angegebene Email-Adresse ein Bestätigungslink verschickt. Solange der User seinen Account nicht bestätigt hat, kann er sich nicht anmelden |
| Abgrenzungskriterien | * Der User soll sich nicht über einen Button („Passwort vergessen“) ein neues Passwort oder einen Link zur Änderung zuschicken lassen können |